**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського**

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 11 (листопад)

Київ – 2021

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №11 (листопад) . – 327 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2021
© Національна бібліотека України імені В.І. Вернадського, 2021

ЗМІСТ

Стан кібербезпеки в Україні 4
Національна система кібербезпеки 4
Кібервійна проти України 5
Боротьба з кіберзлочинністю в Україні 9
Міжнародне співробітництво у галузі кібербезпеки 19
Коронавірус COVID-19 та питання кібербезпеки 31
Світові тенденції в галузі кібербезпеки 42
Сполучені Штати Америки та Канада 75
Країни ЄС та Великобританія 94
Китай 97
Російська Федерація та країни ЄАЕС 98
Інші країни 102
Кібервійни та протидія зовнішній кібернетичній агресії 108
Створення та функціонування кібервійськ 111
Захист персональних даних 112
Кібербезпека Інтернету речей 147
Кіберзлочинність та кібертероризм 148
Діяльність хакерів та хакерські угруповування 204
Вірусне та інше шкідливе програмне забезпечення 219
Програми-вимагачі 236
Операції правоохоронних органів та судові справи проти кіберзлочинців 285
Технічні аспекти кібербезпеки 293
Виявлені вразливості технічних засобів та програмного забезпечення 293
Технічні та програмні рішення для протидії кібернетичним загрозам 318

«З 15 по 19 листопада в Києві проходив Національний хакатон із кіберзахисту. Під час заходу команда кіберполіції розробила нове технічне рішення для боротьби із фішинговими та фейковими ресурсами у мережі Інтернет.

У заході взяли участь 16 команд з сектору безпеки та оборони, освітніх та наукових закладів України.

Змагалися команди за трьома напрямками:

• кіберзахист об'єктів критичної інфраструктури;

• виявлення, реагування та запобігання кібератакам на об'єкти кіберзахисту;

• добування (збір), оброблення, аналіз і відображення інформації з відкритих джерел (OSINT) для виявлення та запобігання кібератакам і кіберінцидентам.

Під час хакатону, виконуючи одне із завдань, команда кіберполіції розробила рішення AntiPhish. Ціль проєкту - створення механізму протидії фішинговим та фейковим ресурсам у мережі Інтернет та захист громадян від фішингових атак.

Концептуально рішення передбачає встановлення додатку у браузер. При відвідуванні фішингових ресурсів додаток порівняє його з інформацією, що є у кіберполіції щодо шахрайських сайтів. У разі встановлення збігу користувача буде поінформовано відповідним повідомленням.

Подальший розвиток цього проєкту та його широке впровадження дозволить значно зменшити кількість фішингових атак, а також злочинів, пов'язаних із шахрайством.

За результатами змагань команда кіберполіції одержала перемогу.

Кіберхакатон організовано Державною службою спеціального зв'язку та захисту інформації України, а співорганізатор – Центр стратегічних комунікацій «СтратКом Україна».

Під час підбиття підсумків т.в.о. начальника Департаменту кіберполіції Сергій Кропива зауважив:

«Такі змагання допомагають ключовим гравцям, які забезпечують безпеку у кіберпросторі, вдосконалити співпрацю, покращити професійні навички та обмінятися досвідом. Головне завдання кіберполіції – створити максимально безпечне кіберсередовище для користувачів онлайн простору. Тільки спільними зусиллями ми досягнемо успіху». ***(Команда кіберполіції перемогла у Національному хакатоні з кіберзахисту // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/komanda-kiberpolicziji-peremogla-u-naczionalnomu-xakatoni-z-kiberzaxistu/). 19.11.2021).***

***

Національна система кібербезпеки

«Національний координаційний центр кібербезпеки запустив проєкт подкастів Qwerty.

У випусках фахівці розповідають про кейси світових кібератак, кібергігієну, блокчейн та хакерів, а також про те, що qwerty — пароль, яким користуються приблизно 18 мільйонів людей в усьому світі.

Подкаст може бути корисним як тим, хто користується лише онлайн-банкінгом та соцмережами, так і людям, які працюють у фаховій сфері.

Нові епізоди виходитимуть щочетверга». ***(Центр кібербезпеки при РНБО запустив проєкт подкастів Qwerty // Інтернет-видання «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/28444/2021-11-04-tsentr-kiberbezpeky-pry-rnbo-zapustyv-proiekt-podkastiv-qwerty/). 04.11.2021).***

***

Кібервійна проти України

«Фахівці Ситуаційного центру забезпечення кібербезпеки СБУ у жовтні 2021 року припинили та нейтралізували 57 кібератак на інформаційні системи органів державної влади.

Це відбулося через безпосередній аналіз понад 28 000 критичних подій інформаційної безпеки, виявлених у поточному місяці.

Довідка:

Виявлена кібератака є результатом безпосереднього аналізу критичних подій інформаційної безпеки.

Здебільшого основними типами виявлених кіберзагроз (хакерських атак) були:

З'єднання з командно-контрольними серверами (C&C Server);

Спроби отримання несанкціонованого доступу (Brute Force Attack);

Атаки на веб-додатки (Web App Attack);

Шкідливе програмне забезпечення (Malware);

та інші.

Нагадаємо, що на базі Ситуаційного центру забезпечення кібербезпеки СБУ функціонує система управління подіями інформаційної безпеки (SIEM), яка моніторить події в режимі реального часу і дозволяє аналізувати стан інформаційної безпеки. Потенційно критичні події безпосередньо обробляються аналітиками безпеки, що дає змогу оперативно виявляти, реагувати і попереджувати загрози в національному кіберпросторі…» ***(У жовтні поточного року СБУ заблокувала понад 50 кібератак на українські органи влади // Служба безпеки України (https://ssu.gov.ua/novyny/u-zhovtni-potochnoho-roku-sbu-zablokuvala-ponad-50-kiberatak-na-ukrainski-orhany-vlady). 01.11.2021).***

***

«Немає жодних сумнівів у тому, що саме Росія організувала кібероперації проти України та США, які відбувалися в останні роки, вважає Лора Галанте, американська фахівчиня з кібербезпеки.

В інтерв'ю журналу НВ вона констатувала, що з часу президентських виборів у США 2016 року російських кібероперацій проти Америки поменшало, але це сталося не через брак ресурсів у Росії для такої ворожої діяльності.

«Путін бачить, наскільки поляризованим є внутрішньополітичний діалог у США, тому розуміє, що йому й не потрібно зайвий раз втручатися, щоб посіяти чергову порцію хаосу. Якщо ж відносини США та Росії погіршаться, Кремль буде активно використовувати об'єкти американської критичної інфраструктури для кібероперацій», — попереджає Лора Галанте, яка в США є визнаним фахівцем у сфері протидії кіберзагрозам, заснувала власну компанію Galante Strategies та консультує уряди західних країн і НАТО.

Коментуючи думку про те, що Росія тестує в Україні свої агресивні кібертехнології, аби потім застосовувати їх на Заході, Галанте відзначила: «Так, у цьому немає жодних сумнівів. За кіберопераціями проти України, які відбувалися з 2014 року, стоїть російська держава. Це й атаки на електромережу в 2015—2016 роках, і, звісно, атака з використанням вірусу Not Petya у 2017-му. Моя команда вже чотири роки аналізує ту атаку».

Розповідаючи, як організовані російські кібератаки, вона підтвердила, що «ці операції реально дуже складні, вони базуються на серйозних ресурсах, плануванні та мають чіткий перелік результатів, яких бажано досягти».

«ГРУ, тобто російська військова розвідка, це одна з найбільш активних хакерських груп у Росії. Вони вміють робити буквально все: від втручання в американські вибори до атак на українські обленерго. Вірус Not Petya — це теж справа їхніх рук, а в 2014-му вони атакували французьке інформаційне середовище», — констатує Галанте.

За її словами, методи й цілі операцій ГРУ щоразу різні, але мета одна — підтримка російських державних та військових інтересів.

«Ми не можемо собі дозволити бути беззахисними, ми не можемо лише спостерігати за діями Путіна. Це не може собі дозволити Захід, це не може собі дозволити Україна», — резюмувала експертка». ***(«Це дуже складні операції». Провідна експертка США з кібербезпеки розкрила НВ деталі хакерських атак РФ в Україні та Америці // НВ (https://nv.ua/ukr/world/geopolitics/rosiyski-hakeri-yak-voni-organizuvali-kiberataki-v-ssha-ta-ukrajini-ostanni-novini-50193729.html). 13.11.2021).***

***

«Кіберфахівці СБУ встановили хакерів всесвітньо відомого угруповання «ARMAGEDON», яке здійснило понад 5 тис. кібератак на державні органи та об’єкти критичної інфраструктури України. Ними виявилися офіцери «Кримського» ФСБ, а також зрадники, які перейшли на бік ворога під час окупації півострова у 2014 році.

Українській спецслужбі вдалося поіменно встановити зловмисників, перехопити їхні розмови, а також отримати беззаперечні докази їх причетності до атак. І це при тому, що вони використовували власні вірусні програми ФСБ, а також засоби анонімізації та «прикриття» у мережі Інтернет.

Наразі 5 учасникам хакерської групи оголошено про підозру за ст. 111 (державна зрада) Кримінального кодексу України.

За наявною інформацією, хакерське угруповання «ARMAGEDON» - це спеціальний проект ФСБ РФ, який прицільно «працював» по Україні. Цей «напрям

роботи» координує 18-й Центр ФСБ РФ (Центр інформаційної безпеки) з дислокацією в Москві.

З моменту російської агресії у 2014 році цей підрозділ ФСБ здійснив понад 5 тис. кібератак і намагався «заразити» понад півтори тисячі урядових комп'ютерних систем. Основними цілями зловмисників були:

контроль над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання);

викрадення та збір розвідувальних даних, у тому числі інформації з обмеженим доступом (сектор безпеки та оборони; державні установи);

проведення акцій інформаційно-психологічного впливу;

блокування інформаційних систем.

Наразі проводяться слідчі дії та експертні дослідження для притягнення співробітників ФСБ РФ до відповідальності за такими статтями Кримінального кодексу України:

ст. 114 (шпигунство);

ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин);

ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів).

Вживаються заходи з локалізації та нейтралізації кіберагресії РФ проти України.

Заходи із викриття зловмисників проводили співробітники Департаменту кібербезпеки та слідчі СБУ у взаємодії з Головним Управлінням розвідки Міністерства оборони України та за процесуального керівництва Офісу Генерального прокурора України». ***(СБУ встановила хакерів ФСБ, які здійснили понад 5 тис. кібератак на державні органи України (відео) // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy). 04.11.2021).***

***

«Заступник міністра охорони здоров'я Марія Карчевич повідомила, що СБУ зафіксувала ознаки старту нової атаки проросійської сторони на систему охорони здоров'я України. Про це вона сказала під час брифінгу 19 листопада.

– В останні дні в інформаційному просторі спостерігається поява нових, відверто неправдивих статей, які стосуються реформи е-лікарняних та загалом роботи електронної системи охорони здоров'я, – наголосила Карчевич.

Вона додала, що пропагандистські матеріали використовують давно відомі наративи телебачення РФ про те, що система нібито не витримує, а люди – нібито відмовляються від отримання послуг.

– Методами російської пропаганди в Україні намагаються посіяти недовіру до державних медичних послуг та дестабілізувати ситуацію у системі охорони здоров'я, – заявила заступник міністра». ***(Анастасія Гевко. РФ проводить інформатаки на українську систему охорони здоров'я – МОЗ // ФАКТИ ICTV (https://fakty.com.ua/ua/ukraine/20211119-rf-provodyt-informataky-na-ukrayinsku-systemu-ohorony-zdorov-ya-moz/). 19.11.2021).***

***

«СБУ проводить комплексні заходи щодо запобігання та нейтралізації загроз гібридної агресії РФ. У ході слідчо-оперативних дій у Херсонській області викрито потужну ботоферму, яка діяла в інтересах російських спецслужб.

Зловмисники проводили спеціальні інформаційні операції для розхитування суспільно-політичної обстановки в Україні.

Для реалізації підривної діяльності вони створили понад 20 тисяч фейкових акаунтів у соцмережах, форумах та популярних месенджерах.

Через анонімні профілі поширювали дезінформацію про внутрішню ситуацію у нашій країні. Крім того, зловмисники розсилали неправдиві повідомлення щодо «мінування» інфраструктурних об'єктів на території регіону.

За даними слідства, до організації ботоферми причетні декілька місцевих жителів. Технологічне обладнання встановили за адресами свого проживання. Для маскування акаунтів зловмисники використовували спеціальні телекомунікаційні пристрої.

Оплату від своїх «кураторів» вони отримували через заборонені російські платіжні системи.

Під час обшуків за адресами перебування організаторів протиправної діяльності у Херсонській області правоохоронці виявили:

понад 3 тисячі сім-карток,

комп'ютерну техніку із доказами незаконних дій.

Наразі вирішується питання щодо повідомлення зловмисникам про підозру у вчиненні злочину та обрання судом мір запобіжних заходів.

У межах кримінального провадження за ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України триває досудове розслідування.

Правоохоронці встановлюють всі обставини правопорушень для притягнення до відповідальності осіб, причетних до злочинів проти державної безпеки України.

Заходи з викриття протиправної діяльності проводили кіберфахівці Управління СБУ в Херсонській області спільно з Головним слідчим управлінням Національної поліції та за процесуального керівництва Офісу Генерального прокурора». ***(СБУ знешкодила потужну ботоферму спецслужб РФ: понад 20 тисяч акаунтів здійснювали інформаційні диверсії проти України // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-zneshkodyla-potuzhnu-botofermu-spetssluzhb-rf-ponad-20-tysiach-akauntiv-zdiisniuvaly-informatsiini-dyversii-proty-ukrainy). 25.11.2021).***

***

«Служба безпеки України встановила хакерів угрупування Armagedon, які здійснили понад 5 тис. кібератак на державні органи України. Ними виявилися офіцери «кримського» ФСБ…

Цитата:

«Кіберфахівці СБУ встановили хакерів всесвітньо відомого угруповання Armagedon, яке здійснило понад 5 тис. кібератак на державні органи та об'єкти критичної інфраструктури України. Ними виявилися офіцери «Кримського» ФСБ, а також зрадники, які перейшли на бік ворога під час окупації півострова у 2014 році», — йдеться в повідомленні.

Деталі

Повідомляється, що українській спецслужбі вдалося поіменно встановити зловмисників, перехопити їхні розмови, а також отримати беззаперечні докази їх причетності до атак. І це при тому, що вони використовували власні вірусні програми ФСБ, а також засоби анонімізації та «прикриття» у мережі Інтернет.

«Наразі 5 учасникам хакерської групи оголошено про підозру за. 111 (державна зрада) Кримінального кодексу України», — зазначається в повідомленні.

У СБУ повідомляють, що за наявною інформацією, хакерське угруповання «Armagedon» — це спеціальний проект ФСБ РФ, який прицільно «працював» по Україні. Цей «напрям роботи» координує 18-й Центр ФСБ РФ (Центр інформаційної безпеки) з дислокацією в Москві.

З моменту російської агресії у 2014 році, як вказали у СБУ, цей підрозділ ФСБ здійснив понад 5 тис. кібератак і намагався «заразити» понад півтори тисячі урядових комп'ютерних систем. Основними цілями зловмисників були:

контроль над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання);

викрадення та збір розвідувальних даних, у тому числі інформації з обмеженим доступом (сектор безпеки та оборони; державні установи);

проведення акцій інформаційно-психологічного впливу;

блокування інформаційних систем.

Наразі проводяться слідчі дії та експертні дослідження для притягнення співробітників ФСБ РФ до відповідальності за такими статтями Кримінального кодексу України:

ст. 114 (шпигунство);

ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин);

ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів).

Окрім того, вживаються заходи з локалізації та нейтралізації кіберагресії РФ проти України…» ***(Анна Мурашко. Понад 5 тис. кібератак на сайти влади: СБУ викрила хакерів з російського Armagedon // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1950980-ponad-5-tis-kiberatak-na-sayti-vladi-sbu-vikrila-khakeriv-z-rosiyskogo-armagedon). 04.11.2021).***

***

«Вісьмом колишнім співробітникам Служби безпеки України – нині офіцерам ФСБ РФ заочно повідомлено про підозру в організації хакерських атак на державні органи України…

Цитата

«За процесуального керівництва прокурорів Офісу Генерального прокурора заочно повідомлено про підозру 8 колишнім співробітникам Служби безпеки України – нині офіцерам ФСБ РФ у вчиненні державної зради (ч. 1 ст. 111 КК України)», - йдеться в повідомленні.

Деталі

Повідомляється, що за даними слідства, злочинна організація, створена спеціальними та розвідувальними органами іноземних спецслужб, вчиняла несанкціоноване втручання до комп'ютерів, комп'ютерних мереж, інформаційно-телекомунікаційних систем органів державної влади, підприємств установ та організацій України, а також інших країн з метою збору розвідувальних даних, вчинення диверсій та інших злочинів.

«У ході розслідування викрито підрозділ Федеральної служби безпеки Російської Федерації, співробітники якого з використанням хакерського угруповання «Armageddon» здійснюють атаки на об'єкти критичної інформаційної інфраструктури установ, що забезпечують належне функціонування економічної і правоохоронної систем України, а також її обороноздатності», - зазначається в повідомленні.

В ОГП повідомляють, що правоохоронці встановили причетність до вчинення таких протиправних дій колишніх співробітників Головного управління Служби безпеки України в Автономній Республіці Крим. Під час проходження служби в органах Служби безпеки України до їх службових обов'язків входило забезпечення контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, а після вчинення зради вони забезпечували проведення розвідувально-підривної діяльності проти України саме у цій сфері.

У ході слідства здобуто докази, що колишні співробітники української спецслужби з використанням завербованих хакерів здійснювали кібератаки, направлені на несанкціоноване втручання в роботу комп'ютерів, телекомунікаційних мереж України, створення прихованих технічних каналів витоку інформації, збір конфіденційної інформації, в тому числі інформації з обмеженим доступом, викрадення ідентифікаторів доступу та персональних даних насамперед співробітників правоохоронних органів, військових підрозділів, блокування роботи державних та корпоративних електронних ресурсів, проведення акцій кібернетичного впливу в інтересах спеціальних та розвідувальних органів Російської Федерації…». ***(Анна Мурашко. Співробітникам ФСБ РФ заочно повідомлено про підозру в організації хакерських атак на сайти влади // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1952006-spivrobitnikam-fsb-rf-zaochno-povidomleno-pro-pidozru-v-organizatsiyi-khakerskikh-atak-na-sayti-vladi). 11.11.2021).***

***

«Правоохоронці припинили роботу одного з найбільших вебресурсів, де незаконно розповсюджували персональні дані громадян України, Молдови, Білорусі, Казахстану та інших країн СНД.

Працівники Департаменту кіберполіції спільно з працівниками дізнання Дарницького управління поліції Києва та у співпраці з представниками уповноваженого Верховної Ради України з прав людини та міжнародними партнерами із США, Молдови та Німеччини припинили факти порушення захисту персональних даних з використанням автоматизованих систем та мережі Інтернет.

Профілактичні заходи були спрямовані на виявлення окремих осіб та злочинних груп, які займаються незаконним отриманням та розповсюдженням персональних даних громадян, баз даних, а також встановлення підприємств, установ та організацій, які можуть бути причетні до порушення законодавства України в сфері обігу персональних даних.

У результаті спільних дій локалізовано та припинено діяльність одного з найбільших вебресурсів, де незаконно розповсюджувалися персональні дані близько 200 мільйонів осіб, зокрема громадян України, Молдови, Білорусі, Казахстану та інших країн СНД.

На сайті містилися відомості щодо номера телефону, прізвища, ім'я та по батькові громадян, їхнього місця реєстрації, а в окремих випадках й інформацію про надані адмінпослуги, пов'язані з використанням транспортних засобів.

За даним фактом відкрито кримінальне провадження за ст. 182 (Порушення недоторканності приватного життя) Кримінального кодексу України. Досудове розслідування наразі триває.

Процесуальне керівництво здійснює Дарницька окружна прокуратура Києва». ***(Кіберполіцейські припинили незаконне розповсюдження персональних даних близько 200 мільйонів осіб // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-prypynyly-nezakonne-rozpovsyudzhennya-personalnyx-danyx-blyzko--miljoniv-osib-8998/). 08.11.2021).***

***

«Використовуючи вразливості вебсайту турагентства, фігурант заволодів базою даних клієнтів. За скоєне правопорушнику загрожує до трьох років ув'язнення.

Протиправну діяльність 26-річного місцевого мешканця викрили співробітники кіберполіції Вінниччини спільно зі слідчим відділом Вінницького районного управління поліції області.

Чоловік, використовуючи вразливості вебсайту місцевого туристичного агентства, несанкціоновано скопіював клієнтську базу. На сайті компанії містилися відомості щодо номерів телефонів, ПІБ громадян, місця реєстрації, посилання на облікові записи у соцмережах, а в окремих випадках — копії документів, що посвідчують особу.

База даних містила інформацію про близько 100 тисяч осіб. Відомості з незаконно отриманої бази правопорушник розповсюджував третім особам.

Правоохоронці провели обшуки за місцем проживання та реєстрації фігуранта. За результатами яких вилучили комп’ютерну техніку, мобільні телефони та накопичувачі даних. Вилучене буде направлено на проведення відповідних експертиз.

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає до трьох років позбавлення волі. Вирішується питання щодо оголошення фігуранту про підозру. Слідчі дії тривають». ***(Кіберполіція Вінниччини викрила чоловіка у несанкціонованому доступі до персональних даних 100 тисяч осіб // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vinnychchyny-vykryla-cholovika-u-nesankczionovanomu-dostupi-do-personalnyx-danyx--tysyach-osib-1112/). 12.11.2021).***

***

«После ареста подозреваемых участников операции по вымогательству Clop на Украине, в красных уведомлениях Интерпола содержится требование об аресте еще шести членов русскоязычной преступной группировки в рамках того, что правоохранительные органы окрестили операцией «Циклон».

Агентство выпустило два красных уведомления в пятницу, уведомив свои 194 страны-члена по запросу южнокорейского отдела расследования киберпреступлений через Национальное центральное бюро Интерпола в Сеуле.

По данным Интерпола, «красное уведомление» - это запрос к правоохранительным органам по всему миру с целью найти и временно арестовать лицо, ожидающее экстрадиции, выдачи или аналогичного судебного иска.

Уведомления были выпущены после ареста в Украине шести членов печально известного семейства вымогателей Clop в ходе глобальной операции, которую координировал Интерпол и в которой также участвовали правоохранительные органы Южной Кореи, США и Национальная полиция Украины в июне.

Интерпол не сразу ответил на запрос о комментарии.

Операция Циклон

Во время операции в июне украинская полиция сообщила, что сотрудники милиции провели 21 обыск в столице Украины Киеве и окрестностях, обыскивая дома и автомобили обвиняемых, изъяв компьютерное оборудование, автомобили и около 185 000 долларов наличными.

Полиция также сообщила, что они нарушили инфраструктуру, используемую при атаках.

Новости об арестах поступили всего за несколько часов до того, как президент США Джо Байден должен был встретиться с президентом России Владимиром Путиным на саммите в Женеве.

Байден подтолкнул Путина сделать больше для пресечения глобальных кибератак, предпринимаемых отдельными лицами изнутри России. Ведущие промышленно развитые страны на встрече в Англии также призвали «все штаты срочно выявлять и разрушать преступные сети вымогателей, действующие в пределах их границ, и привлекать эти сети к ответственности за свои действия».

Операция Cyclone следует за международными правоохранительными органами, расследующими атаки на корейские компании и академические учреждения США, совершенные группой вымогателей Clop.

Операцию координировал центр киберфузии Интерпола в Сингапуре.

В июне власти заявили, что обвиняемые участвовали в нападениях на организации в Южной Корее и США, включая медицинскую школу Стэнфордского университета, Мэрилендский университет и Калифорнийский университет.

Полиция сообщает, что в результате атак в 2019 году всего четыре неназванных южнокорейских фирмы вымогатель Clop заблокировал 810 серверов и компьютеров.

В рамках этих атак, как сообщает полиция, операция Clop использовала различные инструменты, в том числе установку FlawedAmmyy RAT в системы для обеспечения удаленного доступа и запуск программного обеспечения для тестирования на проникновение Cobalt Strike для поиска уязвимостей, которые могли бы использовать злоумышленники для перемещения по сети и заразить больше систем.

Операторы вредоносного ПО Clop в Украине якобы атаковали частные и бизнес-объекты в Корее и США, заблокировав доступ к их компьютерным файлам и сетям, а затем потребовали вымогательский выкуп за восстановление доступа. Предполагается, что подозреваемые способствовали передаче и обналичиванию активов от имени группы программ-вымогателей, при этом угрожая обнародовать конфиденциальные данные, если не будут произведены дополнительные платежи», - заявляет Интерпол.

Если подозреваемым будет предъявлено обвинение в хакерских атаках и отмывании денег, им грозит до восьми лет лишения свободы.

Clop выполняет операцию «программа-вымогатель как услуга». Он предлагает портал, который аффилированные лица могут использовать для создания вредоносных программ для криптоблокировки и последующего заражения жертв. Каждый раз, когда жертва платит, оператор и партнер делят прибыль.

Скоординированные усилия

Интерпол сообщает, что он развернул Operation Cyclone при помощи своих частных партнеров Trend Micro, CDI, Kaspersky Lab, Palo Alto Networks, Fortinet и Group-IB через Project Gateway, который делится важной информацией с агентством.

Project Gateway помогает правоохранительным органам генерировать данные об угрозах из нескольких источников и позволяет полиции предотвращать атаки.

«Несмотря на нарастание глобальных атак программ-вымогателей, эта коалиция полиции и частного сектора стала свидетелем одного из первых арестов преступных группировок в мире правоохранительных органов, который посылает мощный сигнал преступникам-вымогателям, что независимо от того, где они прячутся в киберпространстве, мы будем их неустанно преследовать», - говорит Крейг Джонс, директор по киберпреступности Интерпола.

Интерпол также сообщает, что две южнокорейские компании по борьбе с киберугрозами, S2W LAB и KFSI, предоставили ему ценный анализ данных в темной сети на протяжении всей операции.

«Операция «Циклон» продолжает предоставлять доказательства, которые используются в дальнейших расследованиях киберпреступлений и позволяют международному полицейскому сообществу нарушать работу многочисленных каналов, используемых киберпреступниками для отмывания криптовалюты», - заявляет Интерпол». ***(Prajeet Nair. Law Enforcement Operation Targets Clop Ransomware // Information Security Media Group, Corp. (https://www.govinfosecurity.com/law-enforcement-operation-targets-clop-ransomware-a-17858). 07.11.2021).***

***

«Використовуючи вразливості вебсайту турагентства, фігурант заволодів базою даних клієнтів. За скоєне правопорушнику загрожує до трьох років ув'язнення.

Протиправну діяльність 26-річного місцевого мешканця викрили співробітники кіберполіції Вінниччини спільно зі слідчим відділом Вінницького районного управління поліції області.

Чоловік, використовуючи вразливості вебсайту місцевого туристичного агентства, несанкціоновано скопіював клієнтську базу. На сайті компанії містилися відомості щодо номерів телефонів, ПІБ громадян, місця реєстрації, посилання на облікові записи у соцмережах, а в окремих випадках — копії документів, що посвідчують особу.

База даних містила інформацію про близько 100 тисяч осіб. Відомості з незаконно отриманої бази правопорушник розповсюджував третім особам.

Правоохоронці провели обшуки за місцем проживання та реєстрації фігуранта. За результатами яких вилучили комп'ютерну техніку, мобільні телефони та накопичувачі даних. Вилучене буде направлено на проведення відповідних експертиз.

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає до трьох років позбавлення волі. Вирішується питання щодо оголошення фігуранту про підозру. Слідчі дії тривають». ***(Кіберполіція Вінниччини викрила чоловіка у несанкціонованому доступі до персональних даних 100 тисяч осіб // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vinnichchini-vikrila-cholovika-u-nesankczionovanomu-dostupi-do-personalnix-danix-100-tisyach-osib/). 12.11.2021).***

***

«На спеціалізованих хакерських форумах фігурант за 300-400 доларів збував персональні дані громадян. Бази даних налічували персональну інформацію відносно пів мільйона осіб. За скоєне фігуранту загрожує до 5 років ув'язнення.

Правопорушення задокументували слідчі Головного слідчого управління Нацполіції за інформацією Департаменту кіберполіції.

До кіберполіції звернувся представник приватної компанії, бази даних якої розповсюджувались у мережі Інтернет. Завдяки вчасному інформуванню та взаємодії з приватним сектором правоохоронці припинили злочинну діяльність 23-річного мешканця Київської області.

Фігурант в мережі Інтернет на спеціалізованих хакерських форумах розміщував пропозиції щодо збуту конфіденційної інформації. Вартість коливалась від 300 до 400 доларів залежно від кількості даних.

Також фігурант надавав послуги так званого "пробиву", які полягали в збуті персональних даних на вимогу третіх осіб.

Правоохоронці провели обшуки за місцем мешкання фігуранта. За результатами вилучили комп'ютерну техніку та мобільні термінали, які використовувалися для вчинення злочину.

Під час попереднього огляду вилученої техніки кіберполіцейські виявили чисельні бази даних комерційних установ України. Бази даних налічували персональну інформацію відносно пів мільйона клієнтів. У них містились відомості щодо дати народження, прізвища, ім’я та по батькові громадян, серій та номерів паспортів, індивідуальних податкових номерів платників податків та номерів телефонів.

Наразі бази персональних даних вилучено з незаконного обігу. Облікові записи, які використовувались для злочинної діяльності, заблоковано.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк від двох до п'яти років. Слідчі дії тривають.

Процесуальне керівництво здійснює Офіс Генерального прокурора України». ***(Кіберполіція викрила чоловіка у збуті баз персональних даних комерційних установ // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-cholovika-u-zbuti-baz-personalnix-danix-komerczijnix-ustanov/). 17.11.2021).***

***

«Фігуранти на спеціалізованих форумах купували авторизаційні дані користувачів Інтернет-магазинів. З облікованих записів, які мали позитивний баланс, купували товари. Також один із правопорушників у месенджері розповсюджував базу 792 тисяч авторизаційних даних облікових записів користувачів мережі.

Злочинну діяльність двох 32-річних місцевих мешканців викрили співробітники кіберполіції Хмельниччини спільно зі слідчим управлінням поліції області.

На спеціалізованих форумах зловмисники купували логіни та паролі доступу до облікових записів користувачів Інтернет-магазинів. Далі перевіряли їх на валідність. Потім здійснювали вхід до облікового запису та відшукували ті, які мають позитивний фінансовий баланс. В подальшому купували товари за гроші користувачів Інтернет-магазинів.

Крім цього, перевірені бази даних один із фігурантів збував в одному із месенджерів. Встановлено факт розповсюдження бази даних, яка містить відомості щодо 792 тисяч авторизаційних даних облікових записів користувачів мережі Інтернет.

Правоохоронці провели обшуки за місцями мешкання фігурантів. Вилучили комп'ютерну техніку, мобільні телефони, накопичувачі даних.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Фігурантам загрожує до 6 років ув'язнення. Слідчі дії тривають.

Процесуальне керівництво здійснює Хмельницька обласна прокуратура». ***(Кіберполіція Хмельниччини викрила двох чоловіків у несанкціонованому втручанні в роботу облікових записів користувачів Інтернет-магазинів // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-xmelnichchini-vikrila-dvox-cholovikiv-u-nesankczionovanomu-vtruchanni-v-robotu-oblikovix-zapisiv-koristuvachiv-Internet-magaziniv/). 18.11.2021).***

***

«Кіберфахівці Служби безпеки України припинили протиправну діяльність групи хакерів. Зловмисники позиціонували себе як учасники міжнародного хакерського угруповання «Phoenix». «Спеціалізувалися» на дистанційному зламуванні мобільних пристроїв та незаконному збиранні персональних даних.

За даними слідства, до складу угруповання входило 5 громадян України, мешканців Києва та Харкова. Всі мали вищу технічну освіту.

У своїй діяльності зловмисники використовували спеціально розроблене програмне забезпечення і технічні засоби.

Для отримання доступу до облікових записів користувачів мобільних пристроїв хакери використовували «фішингові» ресурси – копії сайтів відомих виробників мобільних пристроїв «Apple», «Samsung» та ін.

Користувач мобільного пристрою, завантажуючи застосунок чи програму на такому «псевдоофіційному» сайті, надавав зловмисникам пароль до свого облікового запису. Потім зловмисники копіювали інформацію, що зберігалася на зламаному телефоні.

Отримані у такий спосіб дані дозволяли зловмисникам знімати кошти з рахунків громадян та продавати третім особам інформацію про їхнє приватне життя.

Середня «вартість» за несанкціонований доступ до облікового запису власника мобільного телефону становив $200.

Також задокументовано, що ще одним видом «діяльності» зловмисників було розблокування викрадених та загублених гаджетів виробництва «Apple». Згодом їх продавали через мережу підконтрольних магазинів у Києві та Харкові.

За оперативними даними, хакери вели свою «діяльність» понад 2 роки, а їх жертвами за цей час стали кілька сотень осіб.

У ході 5 обшуків, проведених за адресами розташування офісів, підпільних технічних центрів, які функціонували під виглядом магазинів з продажу телефонів, та фактичного мешкання зловмисників у Києві та Харкові, правоохоронці вилучили:

• комп'ютерну техніку та мобільні телефони із доказами злочинної діяльності;

• програмне забезпечення і технічні засоби для несанкціонованого втручання в облікові записи;

• викрадені мобільні телефони, які під виглядом нових готували до збуту.

Наразі вирішується питання щодо оголошення про підозру учасникам угруповання за ст. 361 (незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж) Кримінального кодексу України.

Тривають слідчі дії для встановлення та притягнення до відповідальності всіх причетних до протиправної діяльності осіб.

Заходи із викриття діяльності хакерського угруповання проводили співробітники СБУ за процесуального керівництва Дніпровської окружної прокуратури Києва». ***(СБУ викрила міжнародну хакерську групу: «зламували» мобільні телефони, крали паролі та продавали конфіденційну інформацію громадян (відео) // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-vykryla-mizhnarodnu-khakersku-hrupu-zlamuvaly-mobilni-telefony-kraly-paroli-ta-prodavaly-konfidentsiinu-informatsiiu-hromadian). 24.11.2021).***

***

«15-річний миколаївець на платній основі створював для громадян будь-який документ - від ID-паспорта до Covid-сертифіката. За попередніми даними до нього звернулись близько 30 клієнтів, що встигли придбати підроблену «Дію». Наразі всіх їх встановлюють правоохоронці.

Протиправну діяльність юнака викрили слідчі Миколаївського районного управління поліції та кіберполіцейські Миколаївської області під процесуальним керівництвом окружної прокуратури м. Миколаєва.

Правоохоронці встановили, що на базі міжплатформенного середовища розробки мобільних застосунків хлопець створював фейковий мобільний додаток, що повністю ззовні копіював мобільний додаток офіційного Єдиного порталу державних послуг «Дія». У фейковій програмі користувачам надавалась можливість створити собі будь-який документ із представлених в «Дії», на якому генерувався QR-код, але не зчитувався офіційним застосунком. Зокрема, користувачі могли змінити свій вік, додати будь-яке фото або підробити сертифікат про вакцинацію від коронавірусної хвороби.

Фейковий додаток юнак продавав у месенджері за суму від 250 до 650 гривень. Різниця в сумі залежала від функціоналу та повноти дозволених змін у додатку. Рекламуючи свою розробку, він зазначав, що будь-хто може оформити собі сертифікат про вакцинацію від Covid-19 та інший офіційний документ. Підліток працював лише за умови повної передплати на його електронний гаманець одного з платіжних сервісів країни-агресора, з якого потім виводив кошти на картковий рахунок. Після оплати підліток надсилав замовнику архів з програмним забезпеченням, клієнту лише залишалось його інсталювати на власний смартфон.

У результаті санкціонованого обшуку поліцейські знайшли на комп’ютерній техніці та смартфоні юнака вихідні файли фейкового мобільного додатку «Дія», листування з покупцями та відомості про його продаж і отримані кошти. Речові докази (комп’ютерна техніка, смартфон, накопичувачі інформації та програмне забезпечення) слідчі вилучили і направили на експертизу.

За вказаним фактом слідчі відкрили кримінальне провадження за ч. 1 ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», санкція статті передбачає позбавлення волі на строк до трьох років.

У результаті санкціонованого обшуку поліцейські знайшли на комп’ютерній техніці та смартфоні юнака вихідні файли фейкового мобільного додатку «Дія», листування з покупцями та відомості про його продаж і отримані кошти. Речові докази (комп’ютерна техніка, смартфон, накопичувачі інформації та програмне забезпечення) слідчі вилучили і направили на експертизу.

За вказаним фактом слідчі відкрили кримінальне провадження за ч. 1 ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», санкція статті передбачає позбавлення волі на строк до трьох років.

Також кіберполіцейськими вживаються заходи для блокування усіх каналів розповсюдження фейкового додатку». ***(Кіберполіція викрила у Миколаєві розповсюджувача фейкового застосунку, що повністю копіював дизайн державного додатку "Дія" // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-u-mikolajevi-rozpovsyudzhuvacha-fejkovogo-zastosunku-shho-povnistyu-kopiyuvav-dizajn-derzhavnogo-dodatku-diya/). 22.11.2021).***

***

«Служба безпеки України викрила експравоохоронця з Полтавщини, який продавав інформацію з обмеженим доступом із закритих державних та комерційних баз даних.

Зловмисник торгував закритою інформацією, якою володіли правоохоронці та державні органи, а також банківські установи та оператори мобільного зв’язку. Зокрема, базами даних Міністерства внутрішніх справ, Державної податкової служби, Державної міграційної служби, Державної фіскальної служби, Міністерства юстиції України, Пенсійного фонду України.

«Клієнтів» він знаходив за оголошеннями в телеграм-каналах, а оплату, для уникнення відповідальності, отримував на банківські картки третіх осіб.

У ході слідства задокументовано збут зловмисником за 16 тисяч гривень інформації стосовно двох громадян України з баз, отриманих з:

«АРМОР» (інтегрована інформаційно-пошукова система Міністерства внутрішніх справ України, яка дає доступ до інформації про судимість, про нерозкриті злочини, дозволи на зброю тощо),

«РАЦС» (Державний реєстр актів цивільного стану громадян),

«ІТС ГАРТ» (інформаційно-телекомунікаційна система прикордонного контролю, яка дає доступ до бази даних Державної прикордонної служби України «Відомості про осіб, які перетнули державний кордон України»).

Також чоловік збирався продати інформацію, що містить банківську таємницю. Цю «послугу» він оцінив у 29 тисяч гривень. Правоохоронці затримали його «на гарячому» під час перемовин стосовно цієї «операції».

Наразі зловмиснику повідомлено про підозру за ч. 2 ст. 361-2 (несанкціонований збут та розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах) Кримінального кодексу України та вирішується питання щодо обрання йому запобіжного заходу.

Тривають слідчі дії для встановлення всіх причетних до схеми осіб.

Викриття протиправної діяльності проводив Департамент кібербезпеки СБУ спільно зі слідчими Національної поліції за процесуального керівництва Київської міської прокуратури». ***(СБУ викрила експравоохоронця, який продавав персональні дані українців // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-vykryla-ekspravookhrontsia-yakyi-prodavav-personalni-dani-ukraintsiv). 25.11.2021).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Европейский Союз, Соединенные Штаты и Япония организовали недельный онлайн-тренинг по кибербезопасности для кибербезопасности промышленных систем управления.

Тренинг по кибербезопасности проводился для экспертов из стран-партнеров Индо-Тихоокеанского региона с 25 по 29 октября. Тренинг является хорошим примером действий, предусмотренных новой Индо-Тихоокеанской стратегией ЕС, в соответствии с которой ЕС активизирует свой диалог с партнерами по вопросам безопасности и обороны, включая кибербезопасность, для укрепления потенциала партнеров по борьбе с киберпреступностью.

Обучение экспертов для 40 участников из Индо-Тихоокеанского региона является важным элементом партнерства ЕС-Япония в области взаимодействия, направленного на открытое, свободное, стабильное, доступное, функционально совместимое, надежное и безопасное киберпространство; В конечном итоге это будет способствовать будущему предлагаемому цифровому партнерству между ЕС и Японией. Кроме того, ЕС и Япония сотрудничают по другим вопросам, таким как продвижение ориентированной на человека цифровой трансформации и стандартов кибербезопасности на глобальном уровне.

Тренинг является частью Недели кибербезопасности, которая охватывает безопасность устройств, систем, сетей и средств контроля, используемых в промышленных процессах, а также состоялась сессия по политике и стандартизации.

Тренинг организован Министерством экономики, торговли и промышленности Японии (METI) и ICSCoE (Центр передового опыта в области промышленной кибербезопасности); правительство США (DHS / CISA, DOS и DOE). С европейской стороны в нем приняли участие эксперты из Генерального директората Европейской комиссии по сетям связи, контенту и технологиям (DG Connect), Генерального директората энергетики, Агентства ЕС по кибербезопасности (ENISA), а также промышленности…». ***(EU strengthens Indo-Pacific cybersecurity cooperation with week-long expert training // European Commission (https://digital-strategy.ec.europa.eu/en/news/eu-strengthens-indo-pacific-cybersecurity-cooperation-week-long-expert-training). 03.11.2021).***

***

«Сьогодні, 2 листопада, в рамках Місяця кібербезпеки вже вчетверте відбувся міжнародний форум, присвячений питанням державно-приватної взаємодії у розбудові безпечного кіберпростору в Україні.

Участь у заході взяв заступник начальника Департаменту кіберполіції Олег Заворотній. Він зазначив, що кіберполіція надає допомогу бізнесу у протидії кібератакам, а також здійснює постійне навчання та ділиться практичним досвідом, здобутим на реальних кейсах:

«У частині налагодження взаємодії з бізнесом ми ставимо перед собою завдання спростувати установлений стереотип каральності правоохоронних органів, оскільки, на сьогодні, бізнес часто намагається вирішувати питання кібербезпеки самостійно без залучення спеціалістів. Ми ламаємо стереотипи та показуємо свою відкритість до взаємодопомоги, формуємо поле взаємодовіри, на якому усі гравці – рівні».

Також він підкреслив, що для постійної комунікації з представниками бізнесу у кожному регіональному підрозділі кіберполіції є працівники, котрі відповідають за напрямок налагодження співпраці з партнерами.

Загалом участь у форумі взяли близько 50 спікерів. Представники державних структур, бізнесу і громадськості. Міжнародний форум «Кібербезпека - захистимо бізнес, захистимо Державу» відбувся за ініціативи Торгово-промислової палати України.

Крім цього, кіберполіція взяла участь у національній виставці з кібербезпеки та у кіберспортивних змаганнях по дисципліні CS:GO (Counter-Strike:Global Offensive) серед представників спільноти, студентства, приватного та державного секторів під назвою «Кібергерої».

Турнір проводився з метою знайомства суб'єктів кібербезпеки України (представники приватного та державних секторів) та тих, хто хоче бути її часткою (школярі та студенти).

Кіберполіція продемонструвала хорошу командну гру, тактичну грамотність та високий рівень готовності до участі у таких заходах». ***(Кіберполіція взяла участь у міжнародному форумі «Кібербезпека - захистимо бізнес, захистимо Державу» // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vzyala-uchast-u-mizhnarodnomu-forumi-kiberbezpeka---zaxystymo-biznes-zaxystymo-derzhavu-2246/). 02.11.2021).***

***

«Сообщество юристов, занимающихся киберпреступностью, со всего мира собирается под эгидой Совета Европы (COE), чтобы провести ежегодную конференцию по сотрудничеству в борьбе с киберпреступностью, получившую название Octopus 2021. Она также отмечает 20-ю годовщину соглашения о Конвенции о киберпреступности, подписанного в ноябре 2001 года в Будапешт.

Однако малоизвестный и малоизвестный Стэнфордский проект - предложение по международной конвенции о киберпреступности и терроризме - и инициатива, начатая в 1997 году, привела к появлению этого проекта договорного документа. Проект Стэнфорд был в некотором роде более технологически ориентированный и всеобъемлющий договор инструментом, который призвал к созданию международной договора на основе Агентства по информации защиты инфраструктуры.

Однако европейское сообщество по борьбе с киберпреступностью одновременно разработало свой собственный договорный инструмент, известный как проект COE ; и в суматохе после терактов 11 сентября администрация США решила поддержать этот инструмент. Четыре года спустя, в апреле 2005 года, некоторые из ключевых людей, которые сыграли важную роль в создании Стэнфордского проекта, собрались на семинаре Технологического института Джорджии, чтобы пересмотреть предмет и рекомендовать ряд инициатив в области кибербезопасности для США вместе с быстрой ратификацией Конвенция Совета Европы о киберпреступности, получившая название Атлантской декларации.

В этой статье рассказывается об истории этой основополагающей работы ведущих экспертов по кибербезопасности того периода, многие из которых имели большой опыт работы в сфере национальной безопасности и контроля над ядерными вооружениями. Это была пророческая работа, намного опередившая свое время.

Происхождение

В начале 1990-х годов несколько событий как в Соединенных Штатах, так и в Европе объединились, чтобы произвести параллельные усилия по сосредоточению внимания на новых механизмах и парадигмах кибербезопасности, включая международные договорные механизмы и институты. Годы сотрудничества между промышленностью и Агентством национальной безопасности на протяжении 1980-х годов по разработке и внедрению системы защищенных сетей передачи данных.(SDNS) глобальные платформы для обеспечения безопасности телекоммуникационной и информационной инфраструктуры не смогли масштабироваться на быстрорастущем и развивающемся рынке. Сетевая инфраструктура была существенно дерегулирована и удалена из-под государственного оперативного контроля во всем мире. Автономный, самоорганизующийся хаос архитектур возник как для мобильных, так и для фиксированных сетей. Атаки на сетевую инфраструктуру и всевозможные киберпреступления начали расти в геометрической прогрессии.

Основополагающее событие в США произошло в марте 1997 года, когда Центр международной безопасности и контроля над вооружениями в Стэнфордском университете и Центр исследований глобальной безопасности в LLNL принимали

членов недавно сформированной Президентской комиссии по защите критически важной инфраструктуры (PCCIP) и шестидесяти человек. представители промышленности, университетов и национальных лабораторий для оценки проблем. Обе площадки и многие участники были уважаемыми, давними лидерами в области национальной безопасности и контроля над ядерными вооружениями. Известный как семинар по защите и обеспечению критически важной национальной инфраструктуры, он ограничил свое внимание организованными угрозами, основанными на информационных технологиях, и необходимыми ответами. Эти угрозы включают терроризм, организованную преступность и нападения, спонсируемые государством.

Среди юридических рекомендаций семинара был призыв к «всестороннему использованию нормативных актов, новых законов и договоров, необходимых для решения этой проблемы». В связи с этим следует отметить следующие рекомендации: 1) распределение вины таким образом, чтобы обеспечить более надежную защиту активов в интересах общества, и 2) активные отношения между государством и частным сектором с учетом характера контроля над активами и дублирования ответственности за национальную безопасность и инфраструктуру. защита.

Проект CRISP

Основным результатом семинара стало создание в 1998 году нового проекта в Стэнфордском университете под названием Консорциум исследований в области информационной безопасности и политики (CRISP). В ответ на растущую обеспокоенность правительства угрозой кибератак, направленных против критически важных национальных инфраструктур, Агентство национальной безопасности (АНБ) заключило в 1998 году контракт со Стэнфордским университетом на реализацию многосторонней программы по обеспечению форума, сбора информации и проанализировать варианты устранения этой угрозы.

В CRISP участвовали несколько университетских организаций, Школа международных отношений Сэма Нанна и Компьютерный колледж, входящие в Технологический институт Джорджии; многие компании, занимающиеся разработкой информационных технологий и продуктов; несколько правительственных агентств США; и люди из других стран. Известными лидерами международных усилий были Абрахам Софаер, Сеймур Гудман, Стивен Лукасик и Прескотт Уинтер, который был высокопоставленным чиновником в АНБ, известным своим новаторским руководством. Все они сделали выдающуюся карьеру и объединились для решения проблем глобальной кибербезопасности. Работа представляет собой начало современного анализа кибербезопасности и породила множество основополагающих концепций и статей по кибербезопасности, которые остаются очень актуальными и сегодня. Софаер и Гудман впоследствии опубликовали сборник материалов в виде книги под названием «Транснациональное измерение киберпреступности и терроризма».

После того, как проект CRISP выявил и проанализировал то, что они описали как «уязвимости киберпространства», в декабре 1999 года они созвали конференцию по международному сотрудничеству в борьбе с киберпреступностью и терроризмом. Появился четкий консенсус в отношении необходимости более тесного

международного сотрудничества и значительное согласие с тем, что многосторонний договор, посвященный преступному злоупотреблению киберсистемами, поможет создать необходимую основу для сотрудничества.

Проекты Стэнфорда и COE

В следующем году, в августе 2000 года, девять главных экспертов опубликовали Стэнфордский проект - предложение по международной конвенции о киберпреступности и терроризме. Софаер, бывший федеральный судья и советник по правовым вопросам Государственного департамента США, серьезно участвовал в разработке проекта.

Комментарий к проекту описывает европейскую инициативу, именуемую Проектом COE, и противопоставляет их. Этот проект начался примерно в то же время, что и усилия США с Европейским комитетом по проблемам преступности (CDPC), рекомендовавшие в ноябре 1996 года, чтобы Совет Европы учредил комитет экспертов по киберпреступности, который независимо разработал договор о киберпреступности. Это та работа, которая в конечном итоге возобладала, превратившись в договорный инструмент, открытый для подписания в 2001 году, к которому присоединились США. Значительная связанная с этим работа также проводилась в то время среди агентств безопасности Великобритании.

В Стэнфордском проекте комментарияотмечает: «Стэнфордский проект в значительной степени соответствует проекту Конвенции Совета Европы о киберпреступности, но в некоторых отношениях отличается. Наиболее важно то, что Стэнфордский проект предусматривает учреждение международного агентства по образцу успешных специализированных учреждений Организации Объединенных Наций для подготовки и распространения - на основе рекомендаций неполитических экспертов - стандартов и рекомендуемых практик (SARPS) для повышения эффективности эффективность защитных и следственных мероприятий ». В частности, «Стэнфордский проект основан на шаблонах ИКАО и МСЭ при создании предлагаемого международного учреждения,« Агентства по защите информационной инфраструктуры »или« AIIP », для реализации целей государств-участников в отношении защиты информационной инфраструктуры от преступных и террористическая кибер-деятельность.

Технологический семинар Джорджии

В апреле 2005 года Технологический институт Джорджии вместе с Университетом Карнеги-Меллона, который является двумя ведущими центрами передового опыта в области кибербезопасности США, провел семинар по изучению международных аспектов кибербезопасности под руководством Сай Гудмана. В нем приняли участие многие из участников Стэнфордского проекта, а также широкий круг представителей частного сектора и правительства.

В итоговой декларации Атланты отмечается, что «инфраструктуры национальных сетей связи общего пользования в целом - и в США в частности - за последнее десятилетие стали значительно более уязвимыми и, вероятно, станут еще более уязвимыми, если не будут приняты срочные меры реагирования». Затем он описывает пять «причин» и описывает пять «корректирующих действий». Из этих пяти действий было принято только одно - ратифицировать Конвенцию о

киберпреступности и создать постоянный секретариат для реализации и развития его роли по защите глобальной инфраструктуры ».

Последующие проявления

Спустя годы после семинара 2005 года участники программы CRISP год за годом занимались подготовкой большего количества отчетов, проведением конференций и взаимодействием с последующими администрациями США и международными организациями с минимальным фактическим выполнением первоначальных рекомендаций.

Участники инициатив CRISP и Stanford Draft в течение ряда лет будут продолжать писать бесчисленные статьи и участвовать в американских и международных организациях и инициативах по киберзащите. Сеймур Гудман возглавил престижный Национальный исследовательский совет, результатом которого в 2007 году стал масштабный отчет об исследовании, в соавторстве с Хербом Лином - «На пути к более безопасному и безопасному киберпространству».

В октябре 2013 года один из основных участников проекта Стэнфордского проекта, Прескотт Винтер из NSA, оставил его в пользу частного сектора и охарактеризовал состояние безопасности предприятий как «ужасающее». Четыре года спустя он порекомендовал бы некоторые из тех же действий, что и член частного сектора в Президентском консультативном комитете по национальной безопасности и телекоммуникациям и в его отчете президенту об Интернете и устойчивости связи.

Лукасик скончался в 2019 году, несколько встревоженный упорной неспособностью правительства США осуществить практически любой из множества мер кибербезопасности и защиты инфраструктуры, неоднократно рекомендованных на протяжении многих лет, которые продолжали приводить к все более серьезным атакам и неблагоприятным последствиям с использованием инфраструктуры, которую он фасилитировал как директор DARPA. Одним из его последних мероприятий была подготовка для Агентства по уменьшению угроз обороны подробного анализа того, как социальные сети будут использоваться в качестве оружия и как уменьшить угрозы. Эйб Софаер и Сай Гудман по-прежнему занимают почетные должности в Стэнфордском университете и Технологическом институте Джорджии.

Положительным моментом является то, что значительная часть утешения в области кибербезопасности заключается в огромных совокупных знаниях и методах, разработанных настоящими экспертами по киберзащите сообщества национальной безопасности США, которые ушли на пенсию, чтобы создать некоммерческий Центр Интернет-безопасности и собрать глобальное сообщество, продвигающееся и реализация необходимых возможностей. Эти меры явно эффективны и широко применяются на международном уровне…». ***(Anthony Rutkowski. Remembering the Cybersecurity Treaty That Never Happened // CircleID (https://circleid.com/posts/20211115-remembering-the-cybersecurity-treaty-that-never-happened). 15.11.2021).***

***

«Соединенные Штаты и Европейский союз объявили о планах присоединиться к Парижскому призыву, международным усилиям по борьбе с киберугрозами, угрожающими гражданам и инфраструктуре.

Парижский призыв, учрежденный в ноябре 2018 года и поддержанный 80 международными государствами и более чем 700 частными предприятиями, основан на девяти общих принципах - от защиты Интернета до защиты избирательного процесса - для защиты киберпространства. Эти девять принципов служат областью для обсуждения и действий.

Лиза Плаггемье, временный исполнительный директор Национального альянса по кибербезопасности, заявила, что еще до широко распространенного цикла новостей о взломах в 2021 году кибербезопасность долгое время была взаимосвязанной и глобальной проблемой - просто она не получила особого признания как таковая.

«Дело в том, что весь наш деловой мир невероятно взаимосвязан, и в ближайшее время это не изменится», - сказала она. «Конечно, Берлин или Токио могут быть за тысячи миль, но прошли те времена, когда физическая безопасность была проблемой номер один».

Вместо этого она сказала, что из-за нашего взаимосвязанного образа жизни взлом критически важной инфраструктуры в Лос-Анджелесе может иметь далеко идущие последствия для всей деятельности бизнеса или правительства.

«Проще говоря, без глобального сотрудничества и четкой стратегии распутывание случаев взлома - не говоря уже о их полном предотвращении - становится намного, намного более сложной задачей», - сказал Плаггемьер.

Нет географических ограничений

Росс Рустичи, управляющий директор глобальной консалтинговой фирмы StoneTurn, согласился с этим, отметив, что кибербезопасность не может быть решена только внутри страны.

«Нет никаких географических ограничений для деятельности злоумышленника, что означает, что традиционный, географически ограниченный подход к правоохранительным органам просто не работает», - сказал он. «ФБР не имеет юрисдикции в отношении субъектов угроз в Канаде, Великобритании или России».

Рустичи сказал, что без сотрудничества со стороны этих правительств, законов, регулирующих то, из чего состоит незаконная онлайн-деятельность, и без надежной экстрадиции, киберпреступники могут осуществлять свою деятельность практически безнаказанно.

«Международному сообществу необходимо согласовать свои правовые интерпретации защищенных данных, какие типы доказательств и методы сбора допустимы в суде и что является нарушением уголовного законодательства в отношении онлайн-активности», - сказал он.

Плаггемье отметил, что девять общих принципов Парижского призыва служат хорошим обобщением тех областей, на которых международное сообщество должно в целом сосредоточиться.

«Приятно видеть, что оба« традиционных »приоритета, такие как общая интернет-безопасность, перечислены вместе с более новыми проблемами, такими

как безопасность выборов», - сказала она. «Но доказательством этого, конечно же, будет то, как мы на самом деле намеревались достичь этих целей и, в конечном итоге, насколько эффективно мы это делаем».

Плаггемье отметил, что существует множество более мелких международных организаций по кибербезопасности, которые уже сегодня делают большую работу, такие как OmniSOC, ISSA и многие другие.

Тем не менее, без крупномасштабной координации эти группы могут решить не так много, и, по ее словам, именно поэтому такие соглашения, как Парижский призыв, так важны.

«Конечно, есть здоровая доза цинизма по поводу того, чего в конечном итоге может достичь эта и другие подобные инициативы», - сказала она. «И хотя на самом деле здесь действительно важны действия, нам было бы упущением игнорировать кардинальные изменения, которые медленно происходят в глобальном сообществе по кибербезопасности, связанные с важностью сотрудничества, чего не хватало в прошлые годы».

Огромный шаг вперед

Она назвала это признание «огромным шагом вперед», который будет невероятно полезен в формировании общего ландшафта кибербезопасности, необходимого для решения стоящих перед нами проблем.

«Несмотря на опоздание на вечеринку, приятно видеть, что правительство США подписывается под Парижским призывом», - сказал Плаггемье. «США - один из крупнейших мировых рынков технологий и бизнеса, поэтому чем больше мы сможем взаимодействовать с« кибер-благодетелями »как в государственной, так и в частной сфере, тем лучше».

Она указала, что кибербезопасность - это проблема не только государственного или частного сектора, и поэтому для того, чтобы действительно реализовать наиболее всеобъемлющий план, необходимы постоянные усилия по наведению мостов между обоими мирами.

«Сфера кибербезопасности быстро меняется из-за множества факторов, поэтому у США есть возможность показать пример», - сказала она. «Продолжая налаживать партнерские отношения и модернизируя как нашу техническую инфраструктуру, так и инфраструктуру кибербезопасности человека, мы можем это сделать».

Рустичи добавил, что необходимо «значительно повысить уровень возможностей» для обнаружения, анализа и преследования киберпреступников.

«Существует значительный объем работы, которая потребует беспрецедентной координации и гармонизации между странами, и, как таковая, потребуется много времени, чтобы добраться до точки, в которой будут видны результаты», - сказал он. «Самая большая роль, которую США могут сыграть, - это техническая подготовка других правоохранительных органов».

Он объяснил, что правительство США отстает с точки зрения конфиденциальности, а характер его военных и шпионских программ также затрудняет моральное лидерство в инициативах по защите сети.

«Кроме того, большинство крупных успехов в борьбе с киберпреступностью было достигнуто через Интерпол из-за местонахождения преступников», - сказал он.

«Поддержка этого устоявшегося учреждения и предоставление технической помощи - лучшее краткосрочное решение для США обеспечить лидерство».

Помимо этого, Рустичи сказал, что использование его большой бюрократии для помощи персоналу, поддержки и продвижения дипломатических и регулирующих усилий также может значительно помочь атлантическому консенсусу по этой деятельности.

«США не могут сделать это в одиночку, и по репутационным причинам они не могут рассматриваться в качестве основной движущей силы во многих отношениях», - сказал он. «Это должно быть совместное усилие коллег для достижения реального, существенного прогресса». ***(Nathan Eddy. US, EU Join Paris Call for Cybersecurity // Techstrong Group Inc. (https://securityboulevard.com/2021/11/us-eu-join-paris-call-for-cybersecurity/). 16.11.2021).***

***

«14 ноября 2021 года Министерство финансов США объявило о двустороннем партнерстве в области кибербезопасности с Министерством финансов Израиля «для защиты критически важной финансовой инфраструктуры и новых технологий» и борьбы с использованием программ-вымогателей. Инициатива включает в себя создание американо-израильской целевой группы по финтех-инновациям и кибербезопасности («Целевая группа»), которая стремится продвигать двойную цель поощрения финтех-инноваций при одновременной защите от киберугроз со стороны национальных государств и криминальных субъектов.

Заместитель министра финансов Уолли Адейемо встретился с министром финансов Израиля Авигдором Либерманом и генеральным директором Национального управления кибербезопасности Игалом Унна, чтобы начать партнерство. Их объявление последовало за встречей по инициативе Counter-Ransomware Initiative, состоявшейся практически месяцем ранее с Европейским союзом и более чем 30 странами, включая Израиль, в ходе которой заместитель госсекретаря Адейемо подчеркнул важность международного сотрудничества для решения проблемы злоупотребления виртуальной валютой и подрыва бизнеса, связанного с программами-вымогателями. модель.

Недавно созданная целевая группа будет продвигать цели инициативы посредством различных усилий, включая серию экспертных технических обменов и немедленную разработку Меморандума о взаимопонимании, который будет поддерживать:

допустимый обмен информацией, относящейся к финансовому сектору, включая правила и рекомендации по кибербезопасности, инциденты кибербезопасности и сведения об угрозах кибербезопасности;

обучение персонала и ознакомительные поездки для развития сотрудничества в области кибербезопасности и финансовой системы; а также

мероприятия по повышению квалификации, такие как проведение трансграничных учений по кибербезопасности, связанных с финансовыми и инвестиционными потоками глобальных финансовых учреждений.

Экспертные технические обмены Целевой группы будут охватывать политику, регулирование и информационно-пропагандистскую деятельность для поощрения финтех-инноваций, которые включают надежные средства защиты кибербезопасности и могут способствовать соблюдению международных стандартов по борьбе с отмыванием денег и финансированием терроризма и распространения оружия массового уничтожения. Согласно объявлению, технические обмены будут изучать, как фирмы, занимающиеся кибер-аналитикой, и новаторы в сфере финансовых и регтех-технологий, разрабатывают новые подходы к снижению рисков незаконного финансирования и совершенствованию правительственной аналитической и правоприменительной деятельности. Министерство финансов США также примет участие в конференции CyberTech Global Tel Aviv в Израиле в январе 2022 года». ***(U.S. Department of the Treasury Announces Partnership with Israel to Combat Ransomware // Hunton Andrews Kurth LLP (https://www.huntonprivacyblog.com/2021/11/16/u-s-department-of-the-treasury-announces-partnership-with-israel-to-combat-ransomware/#page=1). 16.11.2021).***

***

«Генеральный прокурор Ирина Венедиктова открыла Международный форум по кибербезопасности, который пройдет 18-19 ноября в Киеве. Во время своего выступления она анонсировала создание платформы совместных действий для противодействия киберпреступлениям.

Об этом Венедиктова сообщила в Facebook.

По словам генпрокурора, форум собрал экспертов из разных уголков мира для того, чтобы сделать цифровой мир безопасным.

«Международный форум кибербезопасности объединил наших европейских коллег, специалистов из Японии, Аргентины, Марокко и представителей украинских правоохранительных и государственных органов», — отметила Венедиктова.

Генпрокурор отметила, что кибератаки в мире осуществляются каждые полминуты. В среднем ежедневно осуществляется более 2000 киберпреступлений. Поскольку кибератаки становятся все более интеллектуальными, опасными и не имеют географических границ, реакция на них должна быть молниеносной, законной и строгой.

«За последний год в три раза увеличилось количество запросов наших иностранных коллег о международной правовой помощи именно в сфере противодействия киберпреступлениям. Мы совместно с правоохранителями США, ФРГ, Южной Кореи, Франции и других стран провели успешный ряд спецопераций, в ходе которых была пресечена деятельность сверхмощных кибергруппировок. Это и операция «Emotet» в отношении группы преступников-хакеров, которая с помощью самого распространенного в мире вредоносного программного обеспечения нанесла общий ущерб физическим и юридическим лицам на 2,5 миллиарда долларов США. И обезвреживания кибергруппировки, которая осуществляла атаки вирусом-шифровальщиком "CLOP" на серверы американских и корейских компаний. Ущерб от противоправных действий составил более 500 млн долларов США», — сообщила генпрокурор.

Венедиктова также напомнила, что недавно впервые в истории Украины состоялся процесс передачи немецким компетентным органам автомобилей элит-класса, стоимостью более 1 млн евро, которые являются доказательствами в деле по международной мошеннической схеме.

Генпрокурор уверена, что в глобальном масштабе без скоординированных действий компетентных органов между собой эффективное противодействие и расследование преступлений этой категории не будут результативными. Однако Офис генпрокурора развивается в направлении расследования киберпреступлений. В ведомстве ввели новую киберспециализацию прокуроров и создали соответствующее подразделение, а Департамент международно-правового сотрудничества активно сотрудничает с иностранными коллегами.

Украинские IT-специалисты пользуются уважением и спросом на международном рынке, однако Украина сейчас стала и одним из мировых хабов киберпреступности. Наша цель, чтобы новые технологии меняли жизнь к лучшему, а не давали более широкие возможности для злоупотреблений, правонарушений и мошенничеств. Я надеюсь, что наш Международный форум по кибербезопасности и платформа действий, которую мы на нем создадим позволит нам направить синергию наших усилий на преодоление вызовов безопасности в цифровой сфере, - заключила Венедиктова.

Международный форум по кибербезопасности продлится 18-19 ноября в Киеве. Событие инициировал Офиса генерального прокурора для создания платформы активного диалога и взаимодействия для преодоления вызовов цифрового мира.

Мероприятие объединило более 80 экспертов из более 20 стран мира. Они встретились для обмена лучшими практиками в этой сфере и наработки совместных решений по противодействию киберпреступлениям и эффективному их расследованию…». ***(Венедиктова анонсировала запуск платформы совместных действий для противодействия киберпреступлениям // УНИАН (https://www.unian.net/science/venediktova-anonsirovala-zapusk-platformy-sovmestnyh-deystviy-dlya-protivodeystviya-kiberprestupleniyam-novosti-11614243.html). 18.11.2021).***

***

«Сьогодні, 18 листопада, заступник міністра внутрішніх справ України Ігор Бондаренко взяв участь у Міжнародному форумі з кібербезпеки, який проходить у столиці за ініціативи Офісу Генерального прокурора. Захід об’єднав експертів різних країн та міжнародних організацій.

Під час свого виступу він розповів про основні проблеми з якими стикається національна система кібербезпеки та окреслив шляхи їх вирішення. Заступник міністра підкреслив, що основними викликами на сьогодні є недосконаліть правової бази, недостатні технічні спроможності, погано розвинуті організаційні спроможності та нестача кваліфікованих кіберфахівців.

«Для впровадження ефективних заходів у протидії кіберзагрозам, зокрема кіберзлочинам, необхідно імплементувати у вітчизняне законодавство Конвенцію

про кіберзлочинність, зокрема, щодо збору електронних доказів», - зазначив Ігор Бондаренко.

Крім того, він розповів про ефективну модель національної системи кібербезпеки та шляхи подолання проблем. По завершенню виступу заступник міністра заявив, що МВС готове активно долучатися до розвитку сфери кібербезпеки в Україні.

Метою форуму є створення платформи для активного діалогу та взаємодії широкого кола національних та міжнародних експертів у сфері кібербезпеки, обговорення питань ефективної взаємодії під час розслідування кіберправопорушень та обміну найкращими практиками у цій сфері». ***(Для якісного та результативного розслідування кіберзлочинів необхідні законодавчі зміни, - Ігор Бондаренко // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/dlya-yakisnogo-ta-rezultativnogo-rozsliduvannya-kiberzlochiniv-neobxidni-zakonodavchi-zmini-Igor-bondarenko/). 18.11.2021).***

***

«Сьогодні, 19 листопада, т.в.о. начальника Департаменту кіберполіції Сергій Кропива взяв участь у Міжнародному форумі з кібербезпеки, який має стати платформою для діалогу між експертами з протидії та розслідування злочинів у віртуальному просторі.

Під час свого виступу Сергій Кропива зазначив, що підрозділ прагне створити максимально безпечне кіберсередовище для користувачів онлайн-простору.

«Ми розуміємо, що досягнення такої мети можливе лише за умови проактивного попередження та недопущення вчинення злочинів, надання кваліфікованої інформаційної та практичної допомоги, відповідальності перед суспільством і партнерами», – повідомив Сергій Кропива.

У цьому році кіберполіція провела результативні спецоперації загальнодержавного значення з викриття причетних до злочинів, пов’язаних із дитячою порнографією, хакерських угруповань, а також осіб, котрі причетні до онлайн-шахрайства. Зокрема кіберполіція виявила понад 2,5 тисячі злочинів у сфері високих інформаційних технологій, припинила діяльність 25 організованих злочинних груп і затримала 98 осіб безпосередньо під час вчинення злочинів, 24 із них – причетні до розбещення неповнолітніх та створення за їх участю протиправного контенту.

«Оскільки в епоху діджиталізації кіберзлочинність не має географічних кордонів, кіберполіція працює не лише на національній, а й на міжнародній арені. Ми робимо акцент на співпраці з іноземними колегами і цього року успішно провели 9 міжнародних операцій з викриття кіберзлочинів», – зазначив Сергій Кропива.

Також т.в.о. начальника Департаменту кіберполіції розповів, що підрозділ постійно працює над удосконаленням комунікації із населенням і є постійним ініціатором та учасником інформаційних кампаній з кібербезпеки. Крім цього він зазначив, що кіберполіція допомагає бізнес-середовищу у протидії кібератакам, проводить спеціальні навчання та ділиться досвідом, здобутим на реальних кейсах.

Міжнародний форум проходив у Києві 18-19 листопада за ініціативи Офісу Генпрокурора України. Окрім кіберполіції, участь у заході взяли понад 80 експертів з питань безпеки у цифровому середовищі з понад 20 країн світу». ***(Безпечне онлайн-середовище - найактуальніше питання в умовах стрімкої діджиталізації та всеосяжності Інтернету - Сергій Кропива // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/bezpechne-onlajn-seredovishhe-najaktualnishe-pitannya-v-umovax-strimkoji-didzhitalizacziji-ta-vseosyazhnosti-Internetu-sergij-kropiva/). 19.11.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Согласно новому изданию Оценки угроз организованной преступности в Интернете Европола, ускоренная цифровизация, связанная с пандемией COVID-19, существенно повлияла на развитие ряда киберугроз. Преступники быстро воспользовались текущими обстоятельствами, чтобы увеличить прибыль, распространив свои щупальца по различным областям и обнажая уязвимости, связанные с системами, больницами или отдельными лицами.

В то время как группы программ-вымогателей воспользовались широко распространенной удаленной работой, мошенники злоупотребляли опасениями по поводу COVID-19 и бесплодными поисками лекарств в Интернете, чтобы обмануть жертв или получить доступ к их банковским счетам. Увеличение количества покупок в Интернете в целом привлекло больше мошенников. В связи с тем, что дети проводят гораздо больше времени в Интернете, особенно во время изоляторов, значительно возросли объемы ухода за собой и распространение откровенных материалов собственного производства. Серая инфраструктура, включая услуги, предлагающие сквозное шифрование, виртуальные частные сети и криптовалюты, по-прежнему используются для облегчения и распространения широкого спектра преступной деятельности. Это привело к возникновению серьезных проблем при расследовании преступной деятельности и защите жертв преступлений.

Европол заявляет, что помимо расширения усилий по борьбе с этими угрозами с точки зрения правоохранительных органов, крайне важно добавить еще один уровень защиты с точки зрения кибербезопасности. Внедрение таких мер, как многофакторная аутентификация и управление уязвимостями, имеет первостепенное значение для снижения возможной подверженности киберугрозам. Повышение осведомленности и предотвращение являются ключевыми компонентами в снижении эффективности кибератак и другой преступной деятельности, связанной с киберпреступностью.

В отчете отмечается несколько ключевых угроз:

Партнерские программы программ-вымогателей позволяют большей группе преступников атаковать крупные корпорации и государственные учреждения, угрожая им многоуровневыми методами вымогательства, такими как DDoS-атаки.

Мобильные вредоносные программы развиваются, когда преступники пытаются обойти дополнительные меры безопасности, такие как двухфакторная аутентификация.

Интернет-магазины привели к резкому росту онлайн-мошенничества.

Явно созданный самим собой материал вызывает все большую озабоченность и также распространяется с целью получения прибыли.

Преступники продолжают злоупотреблять законными сервисами, такими как VPN, сервисы зашифрованной связи и криптовалюты.

Оценка угрозы организованной преступности в Интернете, проводимая Европолом, рассматривает развитие этих тенденций, вызванных расширением цифровизации в последние годы. Отчет был представлен на конференции Европола-Интерпола по киберпреступности, на которой собралось около 100 экспертов, чтобы поделиться своими взглядами на последние тенденции и угрозы киберпреступности и обсудить важность инноваций для противодействия ускорению киберпреступности.

Делегаты слышали, как, чтобы идти в ногу с технологическим развитием, правоохранительные органы должны обладать правильным набором навыков для борьбы с цифровой преступностью на национальном, региональном и международном уровнях, а также для целенаправленного и индивидуального наращивания потенциала с упором на инновации в полицейской деятельности.

Обсуждения показали, как социальные и технологические достижения могут позволить полиции бороться с киберпреступностью с помощью новаторских решений, таких как расшифровка доказательств, законно полученных в результате уголовных расследований, и роль лабораторий в инновациях правоохранительных органов.

Европол заявляет, что группы программ-вымогателей использовали пандемию в своих интересах для запуска более сложных и целенаправленных атак. В то время как массовое распространение программ-вымогателей, похоже, сокращается, киберпреступные группы и их филиалы предпочитают хорошо спланированные ручные атаки на крупные корпорации и правительственные учреждения. Всегда руководствуясь возможностями получения большей прибыли, в прошлом преступники нацелены на компании, у которых есть как финансовые возможности для выплаты крупных выкупов, так и необходимость быстрого возобновления операций в случае успешной кибератаки, что влияет на их основную деятельность. Атаки на Kaseya и SolarWinds показывают, как преступники осознали потенциал атаки на цифровые цепочки поставок, зачастую пытаясь найти «самое слабое звено». Тем не мение, многие из самых печально известных групп уменьшили количество атак на правительства и социальные службы, пытаясь ограничить внимание правоохранительных органов к ним. DDoS-атаки возобновились и нацелены на поставщиков услуг, финансовые учреждения и предприятия. Утверждая, что они являются частью двух известных групп угроз, они потребовали значительный выкуп. Пандемия также способствовала прорыву других угроз, которые уже предпринимали значительные попытки проникнуть в киберпространство. Мобильные вредоносные программы и, в частности, банковские трояны также были оснащены возможностями для перехвата текстовых сообщений на устройствах Android,

нарушая протоколы безопасности двухфакторной аутентификации. Утверждая, что они являются частью двух известных групп угроз, они потребовали значительный выкуп. Пандемия также способствовала прорыву других угроз, которые уже предпринимали значительные попытки проникнуть в киберпространство. Мобильные вредоносные программы и, в частности, банковские трояны также были оснащены возможностями для перехвата текстовых сообщений на устройствах Android, нарушая протоколы безопасности двухфакторной аутентификации. Утверждая, что они являются частью двух известных групп угроз, они потребовали значительный выкуп. Пандемия также способствовала прорыву других угроз, которые уже предпринимали значительные попытки проникнуть в киберпространство. Мобильные вредоносные программы и, в частности, банковские трояны также были оснащены возможностями для перехвата текстовых сообщений на устройствах Android, нарушая протоколы безопасности двухфакторной аутентификации.

В отчете также говорится, что жестокие обращения с детьми использовали увеличившееся бесконтрольное присутствие детей в сети во время пандемии, чтобы расширить свою деятельность по уходу за собой. Ускорению производства и распространения материалов о сексуальной эксплуатации детей также способствует распространение приложений для обмена зашифрованными сообщениями и платформ социальных сетей. Онлайн-игры и общение, сокращение реальной социальной активности и нормализация сексуального поведения в сети - это обстоятельства, которыми злоупотребляют хищники, чтобы нацелить большее количество жертв. Эти факторы создают условия для виктимизации детей в Интернете в течение более длительного периода. Ключевой угрозой является производство материалов, создаваемых самими людьми, тревожная тенденция, которой подвержены и дети младшего возраста. Заманиваемые преступниками, использующими вымышленные личности на игровых платформах и в социальных сетях, все больше и больше детей младшего возраста попадают в ловушку создания и распространения откровенных материалов. Запись без ведома жертв и дальнейшее распространение сексуальных материалов в прямом эфире - еще одна тревожная угроза, именуемая «улавливанием». Одноранговые сети остаются ключевым каналом для обмена материалами о жестоком обращении с детьми, наряду с Dark Web». ***(Europol's Threat Report Reveals Organized Cybercrime Has Benefited from the Pandemic // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/europols-threat-report-reveals-organized-cybercrime-has-benefited-from-the-pandemic/). 12.11.2021).***

***

«Отчеты показывают, что киберпреступность выросла на 600% из-за пандемии COVID-19. Этот процент в первую очередь связан с изощренными фишинговыми схемами электронной почты, совершаемыми киберпреступниками. Многие из них пришли в виде электронных писем CDC и ВОЗ, чтобы читатель мог щелкнуть ссылку, по которой вирус попадает на его компьютер.

Кибербезопасность стала важной вещью, о которой нужно думать в любом бизнесе. Существуют разные разделы кибербезопасности и то, что необходимо включить:

Безопасность приложений

Информация / Безопасность данных

Сетевая безопасность

Облачная безопасность

Операционная безопасность

Физическая охрана

Безопасность критически важной инфраструктуры

В вашем секторе кибербезопасности должно быть задействовано множество различных тактик и ресурсов, что требует, чтобы вы всегда были в курсе рисков безопасности. Что поможет вам определить, что лучше для вашего бизнеса: внутренняя или внешняя кибербезопасность?

Оперативный центр внутренней безопасности

Некоторые компании предпочитают иметь собственный центр безопасности со специальным специалистом по ИТ-безопасности. У кого-то, кто занимается вашими ИТ-операциями, есть свои плюсы и минусы, которые вы должны взвесить, прежде чем принимать окончательное решение.

Плюсы внутренней безопасности

Благодаря внутреннему операционному центру безопасности вы можете быть спокойны благодаря прозрачности операций. Вам также предоставляется беспрецедентная доступность с быстрым временем отклика, если что-то пойдет не так. Несмотря на то, что большинству предприятий хотелось бы иметь специального ИТ-специалиста, с экономической точки зрения более разумно иметь кого-то, кто может выполнять больше, чем просто ИТ-роль. Использование внутренней безопасности может позволить сделать самостоятельный подход к борьбе с киберугрозами и на практике.

Минусы внутренней безопасности

Самая большая претензия к выбору сотрудника службы безопасности - это невозможность его найти и цена, которую вы платите, когда все же найдете. Найти преданного своему делу сотрудника службы безопасности - непростая задача - вам нужен целеустремленный и образованный человек. Большинство предприятий обращаются к специалистам по ИТ-специалистам широкого профиля, когда хотят иметь собственного специалиста по безопасности, поскольку они могут выполнять более одной ИТ-роли.

Аутсорсинг центра безопасности

Вместо того, чтобы найти специальный внутренний центр безопасности, некоторые люди предпочитают использовать внешний подрядчик. Благодаря сторонним вариантам безопасности ничего не хранится на месте, и владелец бизнеса создает партнерские отношения с операциями по обеспечению безопасности.

Плюсы аутсорсинга центра безопасности

Поскольку все больше предприятий обращаются к облаку как к инфраструктуре, решения для ИТ-безопасности также с большей вероятностью будут отданы на аутсорсинг. С решениями, переданными на аутсорсинг, вам не

нужно работать, как решение для ИТ-безопасности на месте. Это также более доступные решения для предприятий, которые помогают малым предприятиям сократить расходы. Малые предприятия также являются наиболее подверженными угрозам кибербезопасности, поэтому необходимо иметь доступное решение.

Минусы аутсорсинга центра безопасности

Компании хотят, чтобы их процессы безопасности не попадали в руки других лиц, в том числе тех, кто может нанести вред бизнесу. Большинство из этих сторонних вариантов безопасности - универсальное решение. Когда вы решаете свои проблемы внутри компании, вам не нужно беспокоиться о такой же безопасности, как и у окружающих. Кроме того, компании часто становятся мишенью, когда они используют массовое решение для ИТ-безопасности.

Центр управления смешанной безопасностью

Пытаться выбрать, какой вариант (внутренний или внешний) лучше всего подходит для вашего бизнеса, может быть настолько трудным, что некоторые компании просто не выбирают. Большинство считает, что смешанная система помогает бизнесу более эффективно реагировать на угрозы и предоставляет больше возможностей. Чтобы быть рентабельным, внутренняя команда должна быть меньше и иметь масштабируемую аутсорсинговую операцию, а это означает, что оба варианта жизнеспособны для бизнеса, чтобы оставаться в безопасности от угроз кибербезопасности. Наличие внешнего варианта кибербезопасности может помочь развить навыки работы с внутренними инструментами, сделав их сильнее.

Что следует учитывать при выборе внутреннего или внешнего подряда

При выборе внутреннего или внешнего подряда следует учитывать несколько факторов: стоимость, временные затраты и обязанности руководства. Каждый из них требует от компаний взглянуть на то, что каждый из них предлагает, включая плюсы и минусы.

Расходы

Выбор собственного варианта обходится не всегда дешево. Вашему бизнесу необходимо покупать инструменты, программное обеспечение и все остальное, что необходимо для создания эффективного центра безопасности. Вы не можете оставить себя уязвимым, упустив важное оборудование или инструменты. Вы также должны иметь квалифицированный персонал для работы с такой системой. Аутсорсинг может быть более дешевым вариантом, но он может сделать вас уязвимыми. Знаете ли вы, есть ли у вас гарантия, что у вас не возникнет проблема с кибербезопасностью?

Обязательства по времени

Внедрение и обслуживание внутреннего решения по обеспечению безопасности отнимает много времени. Настолько, что для этого часто требуется команда людей. Дополнительные знания и сотрудники могут быть недешевым вложением, а поиск времени, чтобы постоянно заниматься этим, может создать ненужный стресс. При аутсорсинге все время, которое ваш бизнес тратит на работу над решениями безопасности, можно направить обратно в компанию.

Обязанности руководства

Как и в случае с затратами времени и средств, внутренние операции по обеспечению безопасности требуют тщательного контроля. У вас также должна

быть правильная цепочка команд, если вы хотите иметь решение безопасности, которое присутствует в вашем бизнесе. Попытка справиться со всем этим в качестве менеджера может быть сложной, особенно если у вас нет необходимых учетных данных или знаний в области ИТ. При аутсорсинге вы получаете помощь профессионалов, не пытаясь найти и нанять их для своего бизнеса.

Правильный выбор кибербезопасности

Выбор в пользу обеспечения кибербезопасности собственными силами или аутсорсингом лучше всего делать на бизнес-уровне. Не каждое решение подходит для каждого бизнеса. Некоторые будут лучше себя чувствовать с внутренними решениями по обеспечению безопасности, а другие лучше передадут свою охрану фирме. Правильный выбор - это то, что соответствует вашим расходам, тайм-менеджменту и обязанностям управленческой команды. В целом, если решение соответствует потребностям вашего бизнеса, вы делаете правильное решение». ***(Glenn Mabry. In-House vs. Outsourced Cybersecurity, Which is Better? // Emerald X, LLC (https://mytechdecisions.com/network-security/in-house-vs-outsourced-cybersecurity/). 15.11.2021).***

***

«Согласно исследованию SecureAge, восемьдесят пять процентов работодателей в США и Великобритании были вынуждены принять новые меры кибербезопасности из-за пандемии COVID-19 и перехода на удаленную работу.

На вопрос, какие типы инструментов они внедрили, 60% предприятий США и Великобритании ответили, что они приняли облачные решения, в то время как 45% ответили, что приняли шифрование на уровне файлов, а 41% установили полное шифрование диска для поддержки своей инфраструктуры кибербезопасности.

Однако это не всегда было легким переходом, и отчет показывает, что около 41% предприятий США и 38% предприятий Великобритании заявили, что « проблемы с технической реализацией » были основным препятствием на пути внедрения новых протоколов и стратегий кибербезопасности, основанных на COVID. место.

«Пандемия коренным образом изменила то, как мы работаем, - сказал Джерри Рэй, главный операционный директор SecureAge Technology. «И хотя многие компании хорошо адаптировались к средам удаленной работы, многие все еще пытаются понять, как их эффективно защитить. Это исследование проливает свет на то, как работодатели решают некоторые из этих возникающих проблем кибербезопасности, а также на болевые точки и препятствия, которые остаются на их пути ».

«Очевидно, что после пандемии у многих предприятий не было надлежащей защиты, и они были вынуждены изо всех сил стараться не отставать и преодолевать технические проблемы», - добавил Рэй.

«Современная кибербезопасность зависит от гибкости и сложных технологий, поэтому неудивительно, что компании внедряют инструменты, которые позволяют им оперативно реагировать на новые угрозы и блокировать все конфиденциальные данные. В конце концов, ничто так не расстраивает киберпреступников, как

получение бесполезных зашифрованных данных». ***(Businesses are forced to adopt new cybersecurity measures // Help Net Security (https://www.helpnetsecurity.com/2021/11/17/adopt-new-cybersecurity-measures/). 17.11.2021).***

***

«…В отчете Check Point Software's 2022 Cyber-security Predictions отмечается, что кампании по дезинформации возвращаются: на протяжении текущего года в сети распространялись фейковые новости о пандемии COVID-19 — и позднее о вакцинации. В 2022 году киберпреступники продолжат использовать такие новости для проведения фишинговых атак и мошенничества.

«Холодная кибервойна» будет усиливаться: улучшенная инфраструктура и технические возможности позволят террористическим группировкам и политическим активистам продвигать свои планы и идеи — и проводить изощренные атаки на более широкую аудиторию. Кибератаки будут все чаще использоваться как прокси-войны для дестабилизации деятельности во всем мире.

Утечки данных будут происходить чаще и в более крупных масштабах, организации и правительства будут тратить гораздо больше средств на восстановление. В мае 2021 года крупная страховая компания США заплатила хакерам выкуп в размере 40 млн долл. Это рекорд, крупнейший в истории выкуп - но дальше, скорее всего, крупные выкупы будут еще больше.

Число кибератак на цепочки поставок вырастет. Правительства начнут разрабатывать правила для защиты сетей и борьбы с такими атаками; и, скорее всего, начнут сотрудничать с частными организациями и другими странами для выявления подобных угроз и борьбы с ними на международном уровне.

Киберпреступники будут активнее использовать криптовалюту. Защитные решения должны будут учесть это, измениться и надежно защищать биткоины и прочие альткоины.

Мобильные устройства остаются самыми желанными целями. Так как электронные кошельки и сервисы мобильных платежей используются все чаще, киберпреступники будут адаптировать свои методы именно под смартфоны.

Злоумышленники будут использовать уязвимости микросервисов, которую чаще всего используют вендоры облачных услуг, поэтому киберпреступники будут искать в них уязвимости для запуска крупномасштабных атак на провайдеров.

Дипфейки станут настоящим оружием. Создание поддельных видео и аудио сейчас достаточно развито - гипотетически, такие фейки уже можно использовать для манипулирования мнениями, ценами на акции или чем-то еще. Также злоумышленники будут использовать дипфейки для атак методом социальной инженерии - например, чтобы обманом получить нужное разрешение от конкретного человека или доступ к конфиденциальным данным.

Использование инструментов проникновения увеличится: в 2021 году программы-вымогатели атаковали каждую 61 организацию в мире каждую неделю. Злоумышленники нацелены на компании, которые могут позволить себе уплату выкупа - и в 2022 году их атаки с вымогателями станут только изощреннее. Хакеры

будут все чаще использовать инструменты проникновения для настройки атак в реальном времени, а также для работы в сетях жертв.

Вот такая общая картина и компании должны действовать упреждающе, не оставляя ни одну точку, ни одно устройство незащищенным или неконтролируемым. В противном случае они могут стать следующей жертвой целевых атак». ***(Александр Савушкин. Прогнозы по кибербезопасности на 2022 г. // Компьютерное Обозрение (https://ko.com.ua/prognozy_po_kiberbezopasnosti_na_2022_g_139283). 05.11.2021).***

***

«Пандемия COVID-19 изменила многие аспекты работы предприятий, и удаленная работа стала одним из самых важных. На пике вспышки 71% американских рабочих работали на дому, по крайней мере, неполный рабочий день, 62% из которых раньше редко работали удаленно. Этот сдвиг затронул многие отрасли, но юридический сектор сталкивается с большими нарушениями, чем большинство других.

До пандемии COVID-19 юридическая работа над телекоммуникационными услугами проводилась редко. Сейчас более 80% юридических фирм частично или постоянно перешли на удаленную работу. Консультации и судебные слушания теперь регулярно проводятся по программному обеспечению для телеконференций, что дает неоднозначные результаты.

С одной стороны, удаленная работа облегчила доступ к юридическим услугам более широкому кругу людей. С другой стороны, этот переход обострил проблемы конфиденциальности в отрасли и породил новые.

Растущие опасения по поводу безопасности на фоне удаленной работы

Удаленная работа в юридической сфере представляет собой ряд серьезных проблем. Обеспечить адвокатскую / клиентскую тайну гораздо сложнее, когда вы не встречаетесь лично. Закрытая дверь может помешать другим подслушивать личный разговор, но виртуальные конференц-залы сталкиваются с гораздо большим количеством уязвимостей, многие из которых требуют высокотехнологичных решений.

Использование программного обеспечения для удаленной работы также может повлиять на юридическую ответственность фирмы. Все больше штатов вводят законы о конфиденциальности данных, которые могут повлиять на то, как организации используют инструменты цифровой связи. Такая конфиденциальная информация, как юридическая документация, скорее всего, будет подпадать под более высокие стандарты в соответствии с этими расширяющимися законами.

Как и в других отраслях, удаленная работа также затрудняет обеспечение кибербезопасности всей компании. Сотрудники, использующие собственные устройства в своих сетях, могут иметь недостаточное программное обеспечение для защиты от вредоносных программ или быть более уязвимыми для попыток фишинга. Нарушения в отрасли также обходятся дорого: одна компания подсчитала, что в 2017 году она потеряла миллионы долларов в бизнесе из-за атаки программы-вымогателя.

Как юридическая индустрия может оставаться в безопасности

В то время как удаленная работа делает кибербезопасность в юридической отрасли более сложной, это не делает его невозможным. Юридические фирмы могут предпринять несколько шагов, чтобы оставаться в безопасности при работе из дома. Вот несколько из самых важных.

1. Обучение сотрудников

Как и в других отраслях, возможно, наиболее важной мерой является создание и обеспечение соблюдения политики кибербезопасности. Сотрудники могут быть экспертами в законе, но могут не очень разбираться в вопросах безопасности, что приводит к внутренним угрозам из-за простого отсутствия знаний о кибербезопасности. Обучение сотрудников правилам кибергигиены предотвратит множество успешных атак.

Способность распознавать на фишинг попытки является важной областью, чтобы подчеркнуть в обучении персонала. Еще одна проблема - управление паролями, особенно потому, что сотрудники чаще используют их для удаленного доступа к конфиденциальным документам. Когда сотрудники поймут, как эти проблемы могут привести к таким разрушительным результатам, они с большей вероятностью будут следовать лучшим практикам.

2. Элементы управления аутентификацией пользователей

Еще один важный шаг к кибербезопасности в юридической отрасли - это использование более жестких мер аутентификации. В удаленной юридической работе решающее значение имеет обеспечение того, чтобы люди, пытающиеся получить доступ к конфиденциальным документам, были теми, кем они себя называют. Простая комбинация имени пользователя и пароля недостаточна при работе с конфиденциальной юридической информацией.

Фирмы должны использовать службы цифровой подписи, чтобы обеспечить безопасную удаленную подпись. Ищите инструменты, которые используют меры аутентификации на основе сертификатов, чтобы подтвердить, что люди являются тем, кем они себя называют. Когда юристы не могут физически присутствовать, чтобы проверить чью-либо личность, эти меры очень важны.

Точно так же юридические фирмы должны требовать многофакторную аутентификацию (MFA) для доступа к любым облачным серверам, которые они могут использовать. Исследование 2020 года показало, что менее 50% фирм используют MFA, что делает это необходимым улучшением для отрасли.

3. Шифрование

Шифрование - рекомендуемый шаг для любой отрасли, но он необходим для юридических фирм. Профессионалы в этой отрасли должны шифровать все свои документы при хранении и передаче, чтобы удовлетворить потребности отрасли в конфиденциальности. Точно так же зашифрованные электронные письма необходимы для сохранения конфиденциальности адвоката / клиента при удаленной работе.

Поскольку в настоящее время юридическая отрасль полагается на программное обеспечение для видеоконференцсвязи при проведении многих конфиденциальных разбирательств, она должна обеспечить надежное шифрование этих услуг. В разгар пандемии случаи «взрыва Zoom», когда актеры прерывают и

прерывают звонки Zoom, затронули как минимум одно дело в виртуальном суде, подчеркнув важность зашифрованных звонков.

Zoom с тех пор развернул сквозное шифрование после этих скандалов, но оно не включено по умолчанию. Юридические фирмы и суды должны помнить о включении этой функции для всех удаленных судебных разбирательств и встреч с клиентами. Подобные элементы управления, такие как добавление регистрации и требование аутентификации, также могут помочь сохранить конфиденциальность вызовов.

4. Планирование реагирования на инциденты.

Наконец, юридическая отрасль должна принять стандарт формирования планов реагирования на инциденты кибербезопасности. До преобладания удаленной работы в этом секторе эта проблема была менее актуальной или, по крайней мере, менее заметной. Теперь, когда они сталкиваются с новыми угрозами в условиях удаленной работы, жизненно необходимы планы реагирования на инциденты.

Наличие плана по уменьшению ущерба от кибератаки также может помочь минимизировать ответственность фирмы. Без письменного плана кибербезопасности клиенты, чьи данные были скомпрометированы в результате атаки, могут сказать, что фирма не предприняла надлежащих шагов для обеспечения их конфиденциальности.

Удаленная работа сопряжена с проблемами и возможностями

Удаленная работа может сделать юридические услуги более доступными для людей, которые могут испытывать трудности с посещением личных встреч. Это также может повысить производительность, и, учитывая эти преимущества, юридическая отрасль, вероятно, продолжит разрешать удаленную работу. Если это так, он должен принять более высокие стандарты кибербезопасности.

Какой бы полезной ни была удаленная работа, она сопряжена с рядом рисков для кибербезопасности. Юридические фирмы и государственные учреждения должны следовать этим шагам, чтобы оставаться в безопасности в условиях этого сдвига». ***(Devin Partida. Remote Work and Cybersecurity in the Legal Industry: What to Know // Tripwire, Inc. (https://www.tripwire.com/state-of-security/security-data-protection/remote-work-and-cybersecurity-in-the-legal-industry-what-to-know/). 16.11.2021).***

***

«…В результате ограничений, введенных правительствами в ответ на пандемию коронавируса, многие работодатели поощряют сотрудников работать из дома, и виртуальные конференц-связи начали заменять встречи, которые традиционно проводились лично. Как следствие, технологии становятся все более важными как в нашей работе, так и в личной жизни. Однако, несмотря на растущее распространение технологий, многие организации не могут обеспечить безопасную среду удаленной работы для своих сотрудников, работающих на дому. Тем не менее, очевидна потребность в надлежащей кибербезопасности для удаленного персонала. Более 50% удаленных сотрудников используют персональные устройства для доступа к рабочим данным, а 71% руководителей службы безопасности не имеют достаточной видимости домашних сетей удаленных

сотрудников. 1 Киберпреступники воспользовались этой возможностью: около 67% кибератак нацелены на удаленных сотрудников.

Увеличение удаленной работы требует большего внимания к кибербезопасности, чтобы компенсировать возросшую подверженность киберрискам. Например, сообщалось, что каждый третий сотрудник может стать жертвой фишингового мошенничества. Киберпреступники рассматривают пандемию как возможность использовать уязвимости такого типа. Еще один пример того, как преступники используют слабые места кибербезопасности при удаленной работе, можно увидеть в серии кибератак на сервисы видеоконференцсвязи. В период с февраля 2020 года по май 2020 года более полумиллиона человек пострадали от утечки данных, когда личные данные пользователей услуг видеоконференцсвязи были украдены и проданы в темной сети.

Домашняя рабочая среда не имеет сложных корпоративных мер предотвращения и обнаружения, а домашние сети Wi-Fi намного проще использовать. Более того, удаленные сотрудники больше подвержены кибератакам. Например, удаленные сотрудники могут с меньшей вероятностью регулярно запускать антивирусное сканирование или сканирование на наличие вредоносных программ. Кроме того, сотрудники, работающие из дома, могут быть более небрежными при обработке данных из-за того, что их отвлекают члены семьи или социальные посетители. ИТ-системам необходимо адаптироваться к этим изменениям в рабочей среде, чтобы снизить риски утечки данных и кибератак.

Как компании могут повысить кибербезопасность

Рост удаленной рабочей силы создал множество проблем как для крупных, так и для малых предприятий, поскольку они пытаются реализовать соответствующие уровни кибербезопасности для защиты своих данных и обеспечения соблюдения применимых правил конфиденциальности данных. Чтобы повысить общую безопасность сети, предприятиям и их сотрудникам следует применять основные методы киберпространства, как описано ниже:

Осведомленность о кибербезопасности - всех сотрудников следует регулярно информировать о передовых методах и процедурах обеспечения безопасности, регулирующих обработку данных.

Осведомленность о фишинге. Сотрудники должны быть обучены тому, как выявлять подозрительные электронные письма и работать с ними. Сотрудники могут проявлять бдительность при получении электронных писем, проверяя подлинность электронного адреса отправителя.

Антивирусная защита - сотрудникам должен быть предоставлен доступ к антивирусному и вредоносному программному обеспечению для использования на их домашних рабочих устройствах.

Безопасность домашней сети - удаленные сотрудники могут повысить безопасность своей домашней сети, создав надежный пароль для защиты своего домашнего Wi-Fi.

Используйте VPN - виртуальные частные сети добавляют дополнительный уровень защиты для домашнего использования в Интернете.

Выявление уязвимостей - ни одна ИТ-система не идеальна. Компаниям следует проводить тесты для выявления уязвимостей и исправления наиболее

критических слабых мест системы как можно скорее. Это можно сделать с помощью сканирования уязвимостей или различных упражнений по тестированию на проникновение.

Регулярные проверки системы - компании должны регулярно оценивать подверженность рискам кибербезопасности и определять, достаточны ли существующие меры безопасности. Во время таких проверок следует учитывать все новые формы кибератак.

Подготовка к инцидентам, связанным с безопасностью. В эти периоды повышенного риска компаниям рекомендуется часто проводить упражнения по моделированию инцидентов, связанных с кибербезопасностью, чтобы подготовиться к реагированию на кибератаки. Каждая организация должна также создать команду по кибербезопасности с доверенными консультантами для разработки и внедрения политик и процедур, необходимых для снижения подверженности рискам кибербезопасности...» ***(Jarman J. Smith. CORPORATE TIPS: COVID-19's Impact on Cybersecurity // Brouse McDowell (https://www.brouse.com/corporate-tips-covid19s-impact-on-cybersecurity). 24.11.2021).***

***

Світові тенденції в галузі кібербезпеки

«Примерно 90% лиц, принимающих решения в области ИТ, заявляют, что их бизнесы готовы пойти на компромисс в вопросах кибербезопасности в пользу цифровой трансформации, повышения производительности или других целей. Об этом свидетельствуют данные исследования, проведенного компанией Trend Micro, занимающейся разработкой программного обеспечения для кибербезопасности. Компания также поручила Sapio Research опросить 5 321 ИТ-специалиста и бизнес-специалиста из предприятий с численностью сотрудников более 250 человек в 26 странах.

Исследование показало, что 82% лиц, принимающих решения, вынуждены преуменьшать киберриски для своих советов директоров.

Бхарат Мистри - технический директор Trend Micro в Великобритании.

«ИТ-руководители подвергают самоцензуре перед своими советами директоров, опасаясь повторения или слишком негативной реакции», - сказал Мистри. «Это только увековечит порочный круг, в котором топ-менеджеры не осознают свою истинную подверженность рискам».

По его словам, почти треть лиц, принимающих решения, заявляет, что самоцензура является постоянным давлением.

Организациям необходимо обсуждать риски таким образом, чтобы кибербезопасность рассматривалась как фундаментальный фактор роста бизнеса. Кроме того, им необходимо объединить ИТ-руководителей и руководителей бизнеса, готовых бороться за одно дело.

Переосмысление киберрисков

Фил Гоф - глава отдела информационной безопасности и обеспечения безопасности в Nuffield Health, крупнейшей в Великобритании благотворительной организации в области здравоохранения.

«Лица, принимающие решения в области ИТ, никогда не должны преуменьшать серьезность киберрисков для совета директоров. Но им, возможно, придется изменить свой язык, чтобы обе стороны понимали друг друга», - сказал Гоф. «Это первый шаг к согласованию бизнес-стратегии кибербезопасности, и это очень важный шаг. Формулировка киберрисков с точки зрения бизнеса привлечет к ним внимание, которого они заслуживают».

Он добавил, что это поможет высшему руководству признать безопасность фактором роста, а не препятствием для инноваций.

Исследование показывает, что только половина ИТ-руководителей и чуть более одной трети (38%) лиц, принимающих бизнес-решения, считают, что руководство полностью понимает киберриски. Однако некоторые думают, что это потому, что тема сложная и постоянно меняется. Многие считают, что топ-менеджер либо недостаточно старается (26%), либо не хочет (20%) что-то понимать.

Более того, пандемия усложняет ситуацию, делая компании более уязвимыми для угроз кибербезопасности.

Требование ответственности

Также существуют разногласия между ИТ-лидерами и руководителями бизнеса по поводу того, кто в конечном итоге несет ответственность за управление и снижение рисков. ИТ-руководители почти в два раза чаще, чем бизнес-лидеры, указывают на ИТ-команды и директора по информационным технологиям. Респонденты (49%) утверждают, что киберриски по-прежнему рассматриваются как проблема ИТ, а не как бизнес-риск.

Кроме того, это трение вызывает потенциально серьезные проблемы. Примерно половина (52%) респондентов согласны с тем, что отношение их организации к киберрискам непостоянно и меняется от месяца к месяцу.

Однако около трети (31%) респондентов опроса Trend Micro считают, что кибербезопасность сегодня является самым большим бизнес-риском. Две трети (66%) утверждают, что это имеет наибольшее влияние на затраты из всех бизнес-рисков. Авторы исследования говорят, что это, казалось бы, противоречивое мнение, учитывая общую готовность пойти на компромисс в вопросах безопасности.

Есть три основных способа, которыми, по мнению респондентов, руководитель высшего звена сядет и заметит киберриск.

Шестьдесят два процента считают, что это приведет к нарушению их организации.

Шестьдесят два процента говорят, что было бы полезно, если бы они могли лучше сообщать и легче объяснять бизнес-риски киберугроз.

Шестьдесят один процент говорят, что это повлияет на ситуацию, если клиенты начнут требовать более сложные учетные данные безопасности.

Марк Уолш - архитектор систем безопасности предприятия в Coillte, ирландской коммерческой лесной компании.

«Чтобы сделать кибербезопасность проблемой на уровне совета директоров, начальство должно рассматривать ее как истинный инструмент поддержки бизнеса»,

- сказал Уолш. «Это побудит руководителей ИТ и безопасности сформулировать свои проблемы перед советом директоров на языке бизнес-рисков. И для этого потребуются приоритетные упреждающие инвестиции со стороны совета директоров, а не только временные решения после взлома». ***(Claudia Adrien. Study: 90% of IT Decision Makers Believe Organizations Compromise on Cybersecurity in Lieu of Other Goals // Informa PLC (https://www.channelfutures.com/channel-research/trend-micro-study-organizations-compromise-on-cybersecurity-in-lieu-of-other-goals). 15.11.2021).***

***

«Столкнувшись с обостряющейся нехваткой талантов и все более активными и изощренными злоумышленниками, специалисты по кибербезопасности оказываются истощенными и перегруженными работой.

В 2021 году мы стали свидетелями серьезных инцидентов безопасности, таких как кибератаки на SolarWinds, Microsoft Exchange и Kaseya, которые усугубили стресс, приведший к выгоранию специалистов по безопасности. Приняв следующую стратегию, организации могут дать специалистам по безопасности возможность работать более эффективно, помогая снизить стресс и обеспечивая отказоустойчивость.

Один из наиболее важных уроков кибербезопасности последнего десятилетия заключался в том, что организации должны рассматривать кибербезопасность как издержки ведения бизнеса, а не второстепенную проблему. Ожидается, что руководители будут оценивать риски и принимать соответствующие решения, но слишком часто риск кибербезопасности не учитывается в уравнении. Кибератаки могут стоить организациям миллионы долларов в виде потери производительности, IP или даже выплаты выкупа. Как знает каждый профессионал в области кибербезопасности, вопрос не в том, подвергнется ли компания атаке, а в том, когда.

Для руководителей по информационным технологиям, не имеющих прямой линии связи с генеральным директором, сообщение о серьезности рисков кибербезопасности представляет собой серьезную проблему. Это сообщение сложно передать руководителю, который, возможно, вообще не так податлив для разговора. Если директор по информационной безопасности не может дать правильное представление о потребностях в кибербезопасности, это означает, что он не сможет обеспечить ресурсы, необходимые для запуска эффективной программы безопасности. Когда службы безопасности ограничены в ресурсах, нагрузка на каждого члена команды возрастает. Благодаря тому, что директор по информационной безопасности подчиняется непосредственно генеральному директору, организации могут устранить этот барьер для коммуникации, гарантируя, что генеральные директора будут осведомлены о всей степени киберрисков, с которыми они сталкиваются, и соответствующим образом распределяют ресурсы.

Улучшение взаимоотношений между группами безопасности и разработчиками

Принято считать, что устранение разрозненности между специалистами по безопасности, ИТ-отделом и разработчиками программного обеспечения является

важным ингредиентом успешной программы кибербезопасности. Тем не менее, это то, с чем организации продолжают бороться. Согласно недавнему исследованию Forrester, 52% разработчиков считают, что политика безопасности сдерживает инновации. И только 22% разработчиков «полностью согласны» с тем, что они понимают, какую политику безопасности они должны соблюдать. В целом отношения по-прежнему остаются натянутыми: 37% заявили, что команды их организаций не сотрудничают эффективно или не предпринимают никаких шагов для укрепления отношений между группами безопасности и разработки.

Когда разработчики и группы безопасности не на одной странице, риск безопасности увеличивается. Сети могут страдать от неправильной конфигурации или несовместимых политик приложений, а программное обеспечение может быть выпущено с уязвимостями. Эти недостатки дают хакерам возможность взломать сеть и участвовать в различных дорогостоящих атаках.

Один из способов улучшить отношения между группами безопасности и разработчиками - включить в группы разработчиков защитников безопасности. Эти члены команды должны иметь представление как о безопасности, так и о разработке программного обеспечения, а также должны служить мостом в сообщении разработчикам о потребностях в безопасности. Эти люди также должны помочь командам по безопасности лучше понять проблемы реализации новых политик безопасности или инициатив для своих товарищей по команде разработчиков. Таким образом, безопасность становится совместной, и планы становятся реалистичными, вместо того, чтобы передавать односторонние директивы уже заваленным разработчикам и требовать соблюдения нормативных требований.

Обмен информацией, партнерство и сотрудничество

Администрация Байдена недавно приказала большинству федеральных агентств исправить сотни уязвимостей кибербезопасности, которые, как известно, эксплуатируются, если исправления доступны. Эта директива - один из первых шагов, предпринятых Агентством по кибербезопасности и безопасности инфраструктуры (CISA) и его Объединенным объединением по киберзащите (JCDC), и мы, вероятно, увидим больше такого сотрудничества государственного и частного секторов в 2022 году. В ходе недавних федеральных слушаний, обсуждения и консультации, наиболее последовательно протягивалась нить о том, что организациям необходимо улучшить сотрудничество и обмен информацией не только с федеральным правительством, но и друг с другом.

Разнообразие угроз, жертвами которых может стать организация, слишком велико, чтобы одна команда безопасности могла защититься от них. Вместо этого стратегии должны разрабатываться с прицелом на эффективность, что означает определение приоритетов угроз, которые более распространены, чем другие. Именно здесь аналитика угроз становится жизненно важной, а аналитика угроз наиболее эффективна, когда организации общаются друг с другом о типах атак, которые они наблюдают «в реальных условиях».

Поскольку кибератаки становятся все изощреннее и чаще, усиление защиты систем имеет первостепенное значение для улучшения экосистемы безопасности и защиты киберпространства во всем мире. Очень важно, чтобы у федеральных агентств были инструменты, необходимые для самозащиты, и чтобы они знали об

угрозах, которые ставят под угрозу федеральное правительство. Обладая этой информацией, группы безопасности смогут сосредоточить свою защиту на вероятных точках вторжения, а это означает, что их усилия будут более эффективными и действенными, чем если бы им оставалось только угадывать, какую форму может принять атака.

Важность стратегического видения

Выгорание кибербезопасности - сложная проблема со множеством факторов, и я здесь лишь поверхностно коснулся ее. Существует ряд других стратегий и советов, которые сосредоточены на различных аспектах общей проблемы: приобретение правильных инструментов или создание программ обучения и т.д. Но сила описанных выше шагов заключается в том, что для их достижения требуются небольшие денежные вложения, и вместо этого предложите сдвиг в стратегическом направлении. Кибербезопасность теперь является элементом корпоративной ответственности и должна рассматриваться как функция ведения бизнеса, а не как расходы. От этого зависит ваш бренд. Выгорание из-за кибербезопасности - серьезная проблема, и, как и любая другая серьезная проблема, стратегические организационные директивы будут ключевыми, чтобы помочь отразить ее». ***(Tom Kellermann. How to fend off cybersecurity burnout // VentureBeat (https://venturebeat.com/2021/11/14/how-to-fend-off-cybersecurity-burnout/). 14.11.2021).***

***

«Предприниматели вполне могут стать последними героями кибервойны. Несмотря на возрастающую вероятность злонамеренных атак, владельцы малого и среднего бизнеса продвигаются вперед с новым чувством безопасности.

Четвертый ежегодный отчет Untangle по ИТ-безопасности для малых и средних предприятий, выпущенный 7 октября, показывает, что малые и средние предприятия адаптировались к меняющейся рабочей среде, справились с наплывом кибератак и определили свой подход к ИТ-безопасности.

Исследователи опросили более 740 предприятий малого и среднего бизнеса. На сегодняшний день это самый большой пул респондентов.

Некоторые результаты, кажется, противоречат другим отраслевым отчетам.

Исследование Untangle показало, что даже при ограниченном бюджете и ресурсах малые и средние предприятия внедрили фундаментальные стратегии для решения проблем сетевой безопасности. Малые и средние предприятия также заложили основу для будущих инвестиций в этот процесс.

Восемьдесят процентов респондентов считают, что сейчас они чувствуют себя в большей безопасности по сравнению с прошлым годом. Вероятно, это связано с тенденцией увеличения числа малых предприятий с менее чем 25 сотрудниками, инвестирующих в ИТ.

По словам Скотта Девенса, генерального директора Untangle, подавляющее большинство респондентов, чувствующих себя в большей безопасности в этом году, подтверждается тем фактом, что у предприятий малого и среднего бизнеса годовые бюджеты на ИТ-безопасность выше, чем у опрошенных в предыдущие годы.

«Если посмотреть на даже самые маленькие компании, в которых в 2020 году работало менее 25 человек, только 28 процентов имели годовой бюджет от 1000 до 5000 долларов по сравнению с 35 процентами в 2021 году, а 64 процента тратят более 1000 долларов на ИТ-безопасность, по сравнению с 41 процентом в 2020 году. ; и есть лучшее понимание серьезности атак », - сказал он TechNewsWorld.

Факторы движения

Поскольку кибератаки продолжают расти, заголовки новостей побуждают все больше компаний, включая малый и средний бизнес, обращать внимание на потенциальные угрозы и принимать меры для защиты от них, добавил Девенс. Малые и средние предприятия понимают, что они также являются объектами кибератак, и смотрят на ИТ-безопасность с точки зрения проблемы / решения.

Например, значительно больше половины (64%) опрошенных нарушают правила безопасности, считая их главной проблемой. Согласно отчету, большинство компаний признают брандмауэры (73 процента) и защиту от вирусов и вредоносных программ (62 процента) в качестве своих лучших решений для ИТ-безопасности.

Малые и средние предприятия также начинают полагаться на облачные решения. Признавая необходимость цифровой трансформации, 58 процентов малых и средних предприятий развернули более одной десятой своей ИТ-инфраструктуры в облаке. Это на 32 процента больше, чем в 2020 году.

Ранее Untangle обнаружил, что у SMB есть общие проблемы с безопасностью, и они не имеют четкого представления об облачной безопасности. Это заставило их беспокоиться о потере контроля, когда системы не были локальными, объяснил Девенс.

Несмотря на этот прогресс, препятствия на пути к кибербезопасности по-прежнему привлекают все больше предприятий малого и среднего бизнеса. Сотрудники, не соблюдающие правила, стали главным препятствием на пути к ИТ-безопасности. Несмотря на некоторое увеличение бюджета, многие организации все еще борются с ограничениями по расходам и нехваткой персонала для мониторинга и управления безопасностью.

Основные выводы

Новые бизнес-центры являются движущим фактором необходимости развертывания технологии программно-определяемых глобальных сетей (SD-WAN) для подключения локальных сетей, разделенных значительным расстоянием. Это привело к тому, что более 20 процентов малых и средних предприятий внедрили тот или иной тип инфраструктуры SD-WAN, в то время как еще 19 процентов планируют внедрить или исследовать ее.

Несмотря на то, что компании вкладывают больше средств в ИТ-безопасность, барьеры для малого и среднего бизнеса сохраняются. Сотрудники, не соблюдающие инструкции, стали главным препятствием на пути к ИТ-безопасности (28 процентов).

За последние два года сотрудники стали переключаться между удаленной работой и офисной. Из опрошенных компаний малого и среднего бизнеса в настоящее время большинство сотрудников работают в офисе. Однако в соответствии с текущей тенденцией трансформации рабочих мест 41 процент постоянно перевели четверть или более своих сотрудников на гибридную работу.

Малые и средние предприятия понимают, что они также являются объектами кибератак, а не только крупные предприятия, и смотрят на ИТ-безопасность с точки зрения проблемы / решения, отмечает Девенс. Поскольку 64% случаев нарушения именования являются главной проблемой безопасности, понятно, что большинство компаний признают брандмауэры и защиту от вирусов и вредоносных программ в качестве лучших решений для ИТ-безопасности.

«Делая эти данные доступными, мы даем малым и средним предприятиям возможность учиться друг у друга, узнавать, чем озабочены другие аналогичные предприятия, и видеть, как другие предприятия малого и среднего бизнеса приспосабливаются», - сказал Девенс.

Остерегайтесь программ-вымогателей

Независимо от недавно обретенной для малых и средних предприятий зоны комфорта для кибербезопасности, одной из самых серьезных угроз, которые все еще нередко скрываются, являются атаки программ-вымогателей. Августовский отчет Atlas VPN показал, что количество атак программ-вымогателей увеличилось на 151 процент в первой половине 2021 года по сравнению с тем же периодом 2020 года.

Соединенные Штаты являются страной, наиболее подверженной рискам вымогательства, со значительным отрывом, с 227,3 миллионами попыток атак вымогателей. На втором месте по популярности находятся предприятия из Великобритании, где было совершено 14,6 миллиона попыток атак с использованием программ-вымогателей.

«Атаки программ-вымогателей - серьезная проблема, которая терроризирует многие организации и правительственные учреждения, создавая опасность для всей страны. Поскольку многие люди пренебрегают основными правилами кибербезопасности, они становятся легкой мишенью для киберпреступников. Повышение осведомленности и готовности людей к кибербезопасности является обязательным условием, если компании хотят уменьшить атаки программ-вымогателей», - сказал TechNewsWorld Уильям Меч, исследователь кибербезопасности из Atlas VPN.

Будьте бдительны и готовы

Киберзащита становится более надежной после прошлогоднего отчета. По мере того как поставщики кибербезопасности придумывают инновационные новые решения для защиты от программ-вымогателей, фишинг и утечки данных - это противники кибербезопасности, так же упорно трудятся, чтобы сломать эти решения и найти новые способы опередить этих поставщиков, добавил Девенс из Untangle.

«Держать плохих актеров на расстоянии - это постоянная игра в кошки-мышки. Плохие игроки будут продолжать искать способы обхода даже самых инновационных новых технологий. Чтобы защита оставалась сильной, необходимо идти в ногу с новейшими технологиями», - сказал он.

«Малые и средние предприятия начинают переводить свою ИТ-инфраструктуру в облако. Признавая необходимость цифровой трансформации, учитывая изменения и проблемы последних полутора лет, 58 процентов малых и средних предприятий развернули более 10 процентов своей ИТ-инфраструктуры в облаке. Это на 32 процента больше, чем в 2020 году.

«С изменением рабочего места и продолжающимся ростом кибератак малые и средние предприятия сместили свое мышление с «со мной этого не может» на серьезное отношение к угрозам безопасности», - пояснил Девенс.

«С этой целью они уделяют больше внимания ИТ-безопасности, у них есть более надежные сети, чем год назад, и есть планы по дальнейшему предотвращению атак на будущее. Существует определенная тенденция к размещению большего количества ИТ в облаке и применению многоуровневого подхода к безопасности». ***(Jack M. Germain. SMBs Report Sense of Security Despite Rise in Cyberattacks // ECT News Network, Inc. (https://www.technewsworld.com/story/smbs-report-sense-of-security-despite-rise-in-cyberattacks-87332.html). 10.11.2021).***

***

«Согласно данным ResearchAndMarkets, мировой рынок промышленной кибербезопасности оценивается в 15,2 миллиарда долларов в 2020 году, а к 2026 году он достигнет пересмотренного размера в 22,3 миллиарда долларов, при этом среднегодовой темп роста составит 6,6% за период анализа.

Услуги, один из сегментов, анализируемых в отчете, по прогнозам, будут расти со среднегодовым темпом роста 7,3% и к концу периода анализа достигнут 10 миллиардов долларов.

После тщательного анализа последствий пандемии и вызванного ею экономического кризиса для бизнеса рост сегмента программного обеспечения скорректирован до пересмотренного среднегодового роста в 6,3% на следующий 7-летний период. В настоящее время на этот сегмент приходится 36,1% мирового рынка промышленной кибербезопасности.

Пандемия COVID-19 повысила потребность в удаленном управлении промышленными объектами и производственными цехами по всему миру. Серьезные экономические последствия этой пандемии вынудили предприятия пересмотреть свои бюджеты. Тенденция «Работа из дома» потребовала создания набора процедур и средств безопасности для обеспечения того, чтобы промышленные объекты могли выполнять удаленные операции.

Важность кибербезопасности для производителей

Для производителей важность кибербезопасности значительно возросла, поскольку промышленные компании подключают устройства и программное обеспечение заводского уровня к корпоративным системам, подключенным к Интернету. Промышленный Интернет вещей (IIoT) значительно повысил эффективность производственной деятельности. Однако он также представил много новых векторов возможных кибератак. Увеличивающееся перемещение данных с предприятий может повысить уязвимость локализованных сетей.

Такие новые лазейки используются преступниками для кражи конфиденциальной информации, такой как интеллектуальная собственность, в целях вымогательства. Пандемия COVID-19 усугубила подобные атаки из-за принятия подхода «работа из дома». Домашние офисы не имеют надежных средств защиты кибербезопасности. Удаленный доступ также предоставил хакерам более широкую поверхность для атак.

Кроме того, злоумышленники также использовали чувство неуверенности и страха перед этой пандемией для проведения фишинговых атак, а также других видов социальной инженерии, чтобы обманом заставить пользователей предоставить доступ к различной конфиденциальной информации и системам. Цепочки поставок, сектор здравоохранения и производственные предприятия становятся уязвимыми для кибератак.

В настоящее время наибольший риск, с которым сталкивается сектор здравоохранения, - это фишинговые атаки, при которых злоумышленники используют ряд методов и тактик для получения доступа к частной информации вовлеченных лиц.

В условиях повышенного уровня киберугроз отрасли промышленности все больше инвестируют в развертывание широкого спектра решений безопасности, таких как межсетевые экраны, антивирусы и системы обнаружения вторжений (IDS), для защиты активов и предотвращения любых сбоев в работе из-за кибербезопасности. Растут также расходы на устройства безопасности и программные решения для обеспечения безопасности сетей промышленных систем управления, объектов критической инфраструктуры и центров обработки данных.

Что способствует росту рынка промышленной кибербезопасности?

Увеличение государственного финансирования и увеличение расходов организаций на борьбу с ростом киберугроз по-прежнему будут предоставлять благоприятные возможности для роста рынка промышленной кибербезопасности. Растущее внедрение больших данных, сетевых технологий 5G и искусственного интеллекта в промышленных условиях повлияет на рост рынка в ближайшие годы.

На рынок также повлияет растущий спрос на передовые решения, такие как межсетевые экраны, системы обнаружения вторжений и антивирусы, поскольку промышленные предприятия сосредоточены на повышении кибербезопасности в своих подразделениях. Маршрутизаторы и коммутаторы Ethernet широко используются на рынке промышленной кибербезопасности из-за растущего числа нарушений безопасности, нацеленных на конфиденциальные данные в промышленных процессах и производственных операциях.

Растущее проникновение подключения к Интернету, тенденция к IIoT, постоянное развитие подключенных систем - все это стимулирует использование различных компонентов для кибербезопасности. Поскольку количество кибератак продолжает расти, поставщики сосредотачивают усилия на разработке передового оборудования с улучшенными функциями безопасности. Спрос на различные компоненты также выиграет от увеличения числа подключенных устройств и удаленно управляемых промышленных систем». ***(Industrial cybersecurity market to reach $22.3 billion by 2026 // Help Net Security (https://www.helpnetsecurity.com/2021/11/12/industrial-cybersecurity-market-2026/). 12.11.2021).***

***

«Zscaler объявила о выпуске отчета, в котором отслежено и проанализировано более 20 миллиардов угроз, заблокированных по HTTPS, протоколу, изначально разработанному для безопасной связи по сетям.

Исследование этого года показало рост более чем на 314% по сравнению с прошлым годом в географических регионах, включая Азиатско-Тихоокеанский регион, Европу и Северную Америку, что подчеркивает необходимость модели безопасности с нулевым доверием и более тщательной проверки трафика, чем большинство компаний может достичь с помощью устаревшего межсетевого экрана. модели безопасности.

В семи отраслях, участвовавших в исследовании, уровень атак со стороны угроз в трафике SSL и TLS был выше, в то время как в наиболее целевой отрасли в прошлом году, в здравоохранении, с января 2021 года наблюдалось снижение на 27 процентов. этот показатель намного выше, чем у других видов бизнеса, на него приходится 50 процентов атак.

На современном предприятии более 80 процентов интернет-трафика зашифровано, а это означает, что предприятия сталкиваются с уникальной проблемой обеспечения постоянной безопасности для всех своих удаленных пользователей. Киберпреступники становятся все более изощренными в своей тактике и используют зашифрованные каналы на различных этапах атак вредоносных программ и программ-вымогателей.

«Большинство корпоративных ИТ-отделов и групп безопасности осознают эту реальность, но часто испытывают трудности с внедрением политик проверки SSL / TLS из-за нехватки вычислительных ресурсов и / или проблем с конфиденциальностью», - сказал Дипен Десаи, директор по информационной безопасности и вице-президент по исследованиям и операциям в области безопасности в Zscaler.

«В результате зашифрованные каналы создают значительную слепую зону в их положениях безопасности. Отчет о состоянии зашифрованных атак демонстрирует, что наиболее эффективным способом предотвращения зашифрованных атак является использование масштабируемой облачной прокси-архитектуры для проверки всего зашифрованного трафика, что необходимо для целостной стратегии безопасности с нулевым доверием».

Киберпреступность на рекордно высоком уровне

В период с января 2021 года по сентябрь 2021 года Zscaler заблокировал более 20 миллиардов угроз через HTTPS, что на 314% больше, чем в предыдущем году. Киберпреступники становятся все более сообразительными в своих атаках и извлекают выгоду из аффилированных сетей и инструментов «вредоносное ПО как услуга», доступных в темной сети.

В то время как киберпреступники могут использовать различные типы атак для сокрытия зашифрованного трафика, вредоносный контент составил ошеломляющий 91 процент атак, что на 212 процентов больше, чем в прошлом году. В отличие от этого, количество вредоносных программ для криптодобычи сократилось на 20 процентов, что отражает более широкий сдвиг в тенденциях атак, а программы-вымогатели становятся более прибыльным вариантом.

Технологическая промышленность в осаде

В отчете говорится, что атаки на технологические, розничные и оптовые компании привели к значительному увеличению угроз. Атаки на технологические

компании увеличились на ошеломляющие 2300 процентов, а атаки в розничной и оптовой торговле увеличились более чем на 800 процентов.

Поскольку все больше розничных продавцов предлагают варианты цифровых покупок в период праздничных покупок 2021 года, ожидается, что киберпреступники будут нацеливаться на все больше решений для электронной коммерции и платформ цифровых платежей с помощью вредоносных программ и атак программ-вымогателей. Это усугубляется внезапной необходимостью поддерживать удаленных сотрудников с возможностью удаленного подключения к телеконференцсвязи, приложениям на основе SaaS и рабочим нагрузкам общедоступного облака.

Технологические компании также являются привлекательной целью из-за их роли в цепочке поставок. Успешная атака цепочки поставок, такая как Kaseya и SolarWinds, может дать злоумышленникам доступ к огромному количеству пользовательской информации.

Кроме того, по мере того, как мир начинает возвращаться к нормальной жизни, а по всему миру открываются предприятия и общественные мероприятия, многие сотрудники по-прежнему работают в относительно небезопасных условиях. Получение доступа к критически важным системам продаж чрезвычайно привлекательно для киберпреступников, поскольку открывает дверь к огромным прибылям.

Критические службы видят упадок

Атаки на медицинские организации, которые были главной целью в 2020 году, снизились на 27 процентов в 2021 году. Точно так же количество атак на государственные организации снизилось на 10 процентов. Атаки программ-вымогателей, нацеленные на критически важные службы, в том числе атака Colonial Pipeline и атака программ-вымогателей на Управление служб здравоохранения Ирландии, привлекли внимание правоохранительных органов самого высокого уровня, включая Белый дом, который недавно подписал Указ об улучшении кибербезопасность нации.

«После того, как в 2020 году медицинские и правительственные организации стали двумя секторами, которые наиболее часто подвергаются атакам, они испытывали огромную потребность в срочном обновлении своих позиций безопасности с использованием современных архитектур, которые в значительной степени основаны на нулевом доверии. В ответ на громкие атаки на критически важные службы, такие как Colonial Pipeline, также были усилены меры контроля со стороны правительства и правоохранительные органы предприняли жесткие меры против киберпреступных групп», - сказал Десаи. «В результате действия этих двух факторов в этом году мы стали свидетелями снижения количества атак на медицинские и правительственные организации».

Таргетинг на другие страны

Атаки наблюдались в более чем 200 странах и территориях по всему миру, включая небольшие страны, которые не являются обычными целями, такие как острова в Карибском бассейне. Кроме того, увеличение числа рабочих мест привело к тому, что сотрудники вышли из обычных гигантских технологических центров, таких как район залива Сан-Франциско, Нью-Йорк, Лондон, Париж, Сидней.

В пятерку наиболее целевых стран для зашифрованных атак входят Великобритания (5 446 549 767), США (2 674 879 625), Индия (2 169 135 553), Австралия (1 806 003 182) и Франция (519 251 819).

В целом Европа лидировала с 7 234 747 361 атакой, тройку лидеров замыкают страны Азиатско-Тихоокеанского региона (4 924 732,36) и Северная Америка (2 778 360 051).

Защитите свой бизнес

По мере того, как организации переходят на поддержку новых рабочих моделей с цифровой поддержкой, становится все более важным обеспечивать безопасность своих активов и трафика к этим активам. Чтобы снизить угрозу от зашифрованных атак, рекомендуется стратегия безопасности с нулевым доверием, которая позволяет организациям:

Предотвращение компрометации: Обеспечьте постоянную безопасность для всех пользователей и во всех местах, чтобы гарантировать, что каждый всегда будет иметь одинаковый уровень безопасности, будь то дома, в штаб-квартире или за границей. Используйте облачную архитектуру на основе прокси для проверки всего трафика для каждого пользователя, а также для расшифровки, обнаружения и предотвращения угроз, которые могут скрываться в трафике HTTPS.

Предотвращение бокового движения: используйте архитектуру нулевого доверия с обманом, чтобы уменьшить поверхность атаки и предотвратить боковое движение киберпреступников. Этот тип архитектуры делает приложения невидимыми для злоумышленников, позволяя авторизованным пользователям получать прямой доступ к необходимым ресурсам, а не ко всей сети.

Предотвратите потерю данных: поместите неизвестные атаки или скомпрометированные приложения в изолированную программную среду, управляемую искусственным интеллектом, чтобы остановить вредоносное ПО и программы-вымогатели. В отличие от подходов сквозной передачи на основе брандмауэра, этот дизайн содержит весь подозрительный контент для анализа, гарантируя, что попытки взлома будут остановлены до того, как они смогут получить доступ к конфиденциальным системам и украсть критически важную для бизнеса информацию». ***(Surge in cyber attacks confirms the need for zero trust security // Help Net Security (https://www.helpnetsecurity.com/2021/11/04/need-for-zero-trust/). 04.11.2021).***

***

«Азиатско-Тихоокеанский регион был самым быстрорастущим регионом для приема на работу в сфере кибербезопасности среди компаний фармацевтической отрасли за три месяца, закончившихся в сентябре.

Количество должностей в Азиатско-Тихоокеанском регионе составило 10,7% от общего числа рабочих мест в области кибербезопасности - по сравнению с 10,4% в том же квартале прошлого года.

За ним последовала Европа, где роль кибербезопасности изменилась на -2,3 процентных пункта по сравнению с аналогичным периодом прошлого года.

Цифры составлены GlobalData, которая отслеживает количество новых вакансий от ключевых компаний в различных секторах с течением времени. Затем с

помощью текстового анализа эти объявления о вакансиях классифицируются по тематике.

Тематический подход GlobalData к отраслевой деятельности направлен на то, чтобы сгруппировать ключевую информацию о компаниях по темам, чтобы увидеть, какие компании лучше всего могут пережить потрясения, грядущие в их отрасли.

Эти ключевые темы, в том числе кибербезопасность, выбраны, чтобы охватить «любую проблему, которая мешает генеральному директору спать по ночам».

Отслеживая их по объявлениям о вакансиях, мы можем видеть, какие компании лидируют по конкретным вопросам, а какие медлят - и, что немаловажно, где рынок расширяется и сужается». ***(Michael Goodier. Asia-Pacific is seeing a hiring boom in pharmaceutical industry cybersecurity roles // Verdict Media Limited (https://www.pharmaceutical-technology.com/features/asia-pacific-is-seeing-a-hiring-boom-in-pharmaceutical-industry-cybersecurity-roles/). 16.11.2021).***

***

«Компания Accenture представила отчет «State of Cybersecurity Resilience 2021», в котором исследуется вопрос: насколько эффективные меры предпринимают организации для защиты корпоративных сетей. Команда Accenture Research опросила 4744 руководителя компаний с годовым доходом не менее 1 млрд. долл. в 23 отраслях и 18 странах мира. Далее приведены некоторые выводы исследования.

Более 55% крупных компаний недостаточно эффективно предупреждают кибератаки, а также слишком медленно обнаруживают и устраняют уязвимости;

81% респондентов полагают, что затраты на предупреждение кибератак неоправданно высоки. В исследовании 2020 г. так считали только 69% опрошенных;

82% компаний увеличили расходы на кибербезопасность, но количество взломов, включая несанкционированный доступ к данным, приложениям, сервисам, сетям или устройствам, выросло на 31% по сравнению с прошлым годом. В среднем на одну компанию пришлось 270 таких инцидентов.

В отчете подчеркивается необходимость использовать меры по защите информации не только внутри компании, но и в рамках партнерской сети – во всей экосистеме. Взломы корпоративных сетей происходят зачастую через «звенья» в цепочке связанных электронными документооборотом организаций. 67% компаний считают, что их экосистема безопасна, однако непрямые (через партнера) атаки составили в этом году 61% от общего числа (44% – годом ранее).

Аналитики Accenture выявили среди респондентов небольшую группу компаний – 5%, которые оказались не только киберустойчивы, но и окупили инвестиции в безопасность. Их назвали «киберчемпионами».

Стратегия «киберчемпионов» состоит из нескольких пунктов:

существует баланс между возможностями технологий обеспечить кибербезопасность и желаниями и бизнес-целями компании развиваться и расширяться;

ИБ-департаменты подчиняются непосредственно генеральному директору и совету директоров, демонстрируя большее понимание стратегии развития и рисков в тесной работе с бизнес-подразделениями и финансовым директором;

предприняты дополнительные меры и внедрены технологии для обеспечения безопасности данных, в том числе для приложений и данных в облаках;

зрелость и работоспособность программы кибербезопасности оценивается регулярно, не реже раза в год.

Для достижения устойчивой и измеримой киберустойчивости директорам по ИБ необходимо выйти за рамки своей функции, ориентированной только на безопасность, и начать сотрудничать с другими подразделениями в организации, чтобы получить полное представление о бизнес-рисках и приоритетах». ***(Доля непрямых кибератак на компании через партнерскую сеть возросла до 61% // Компьютерное Обозрение (https://ko.com.ua/dolya_nepryamyh_kiberatak_na_kompanii_cherez_partnerskuyu_set_vozrosla_do_61_139316). 09.11.2021).***

***

«Компанії адаптувалися до обмежень пандемії і віддаленої роботи. Водночас загрози інформаційної безпеки стали більш витонченими, а їх кількість збільшилася. Закономірно, що служби безпеки в умовах переходу на віддалену роботу зосередилися на підготовці захищених каналів зв'язку та іншої інфраструктури.

Варто зазначити, що понад три чверті оприлюднених у засобах масової інформації випадків, які пов'язані з компрометацією, стосувалися безфайлових методів. Опублікована інформація про успішно проведені атаки на різні державні та комерційні організації — це всього лише маленька частина від їх реальної кількості. Із впевненістю можна стверджувати, що кількість кіберінцидентів і рівень їх наслідків набагато вищий, ніж зазначається.

Так, згідно дослідження незважаючи на зростання ризиків безпеки, пов'язаних із віддаленою роботою, лише 47% організацій цілодобово стежать за своїми мережами, і лише 50% шифрують конфіденційні дані, що зберігаються на пристроях.

Наприклад, глобальний лідер у галузі кібербезпеки, Bitdefender дотримується політики безперервного технологічного розвитку, регулярно оновлює систему та впроваджує вдосконалені засоби захисту. Все це дозволяє антивірусу виявити і заблокувати навіть найновітніші інтернет-загрози. З цим програмним забезпеченням віруси, програми-шифрувальники і здирники просто не досягнуть своєї мети.

Потенційні загрози і рекомендації щодо їх усунення

Сучасний захист потребує адаптації до складних загроз і має включати функціональність із виявлення комплексних атак, спрямованих на кінцеві точки і, разом із тим, оперативно реагувати на нові знайдені інциденти.

Водночас, компанії, які планують використовувати функціональність із виявлення складних загроз на кінцевих точках, стикаються з тим, що співробітники департаменту безпеки не володіють необхідними знаннями.

«Завдяки встановленню централізованого антивірусного програмного забезпечення нам вдалося мінімізувати витрати часу на обслуговування інфраструктури, виокремити додатковий периметр безпеки із зручним центром моніторингу, управління та оперативного реагування на інциденти, при цьому зменшивши вплив на продуктивність робочих станцій», — ділиться досвідом

керівник відділу інформаційних технологій енергетичної компанії зі штатом понад 500 співробітників.

Спостерігаючи за еволюцією загроз від масових до спрямованих, виникає необхідність у додаванні до автоматичного блокування простіших загроз ще й ефективного виявлення спрямованих складних загроз. Крім того, необхідна зміна фокусу від захисту окремих робочих місць до безпеки цілого підприємства із залученням не тільки фахівців IT-департаменту, а й фахівців з інформаційної безпеки й аналітиків.

«Після впровадження продукту співробітники перестали відволікатися на роботу антивірусного захисту, а весь контроль за безпекою та адміністрування перейшов до спеціалістів відділу інформаційних технологій», — розповідає керівник відділу інформаційних технологій енергетичної компанії зі штатом понад 500 співробітників.

Централізований захист

Організація антивірусного захисту корпоративної інформації не тільки не втрачає своєї актуальності, а, навпаки, все більше компаній останніми роками потребують цього Проте основний фокус своєї діяльності розробники рішень у сфері інформаційної безпеки зараз перевели на комплексні продукти.

Антивірусний захист бізнесу значною мірою відрізняється від антивірусного захисту комп'ютерних систем невеликого офісу. Для маленьких компаній обирають рішення, що дозволяє охопити групу завдань, що має централізоване управління через єдину консоль. На великих підприємствах для захисту використовуються кілька рішень, кожне з яких відповідає за виконання свого завдання, наприклад, захист сервера або захист від витоку інформації.

Але незалежно від того, який бізнес веде компанія, вона завжди знаходиться в групі ризику, бо завжди є що вкрасти. Надійний антивірусний захист даних дозволяє мінімізувати ці ризики та убезпечитися від великих фінансових втрат. Одним із провідних постачальників, який задіяний в більш ніж 38% світових рішень з безпеки, є компанія Bitdefender. «Це технологічна компанія в області розвитку світового ринку інформаційної безпеки, яка є лідером серед виробників області інформаційних технологій та інформаційної безпеки. Антивірусні рішення Bitdefender захищають більш ніж 500 мільйонів систем у понад 150 країнах. Це гарантія кібербезпеки і захисту від загроз фізичних і приватних осіб, підприємств, локальних мереж і хмарних сервісів», — зауважує Олександр Бутусов, Head of Information Security Solutions компанії SOFTICO.

Ще одна причина використання Bitdefender — це зручний і зрозумілий інтерфейс, простота використання. Продумане інтуїтивно зрозуміле меню дозволить швидко виявити та усунути порушення безпеки комп'ютера. Крім того, антивірус допомагає значно підвищити продуктивність ПК шляхом виправлення системних помилок.

«Стрімке зростання кількості користувачів вимагало застосування антивірусного захисту з централізованою системою керування а також розширення функціоналу комплексного захисту кінцевих точок», — розповідає керівник відділу інформаційних технологій енергетичної компанії зі штатом понад 500 співробітників.

Попередити атаки та діяти на випередження

Спроби хакерів отримати доступ до IT-інфраструктури компанії та заволодіти конфіденційними даними реальні. Більшість кібератак здійснюється зловмисниками продумано та їх дії плануються заздалегідь. Вони готуються і використовують спеціальне програмне забезпечення. Хоча і неможливо гарантувати повноцінний захист від усіх типів нападів, проте можна діяти на випередження.

«Ми перейшли від режиму моніторингу та захисту до роботи на випередження. Завдяки впровадженню централізованого антивірусного програмного забезпечення, ми отримали розуміння поточного стану безпеки, отримали додаткову інформацію про потенційні загрози і рекомендації щодо їх усунення», — зазначає керівник відділу інформаційних технологій енергетичної компанії зі штатом понад 500 співробітників.

Завдяки контролю за пристроями співробітників, які зловмисники часто обирають, як вихідну точку для проникнення в мережу компанії, атаки можна виявити швидше та локалізувати ще до того, як зараження набуде серйозних масштабів. Щоб попередити та знизити можливі ризики, краще довірити кібербезпеку компанії фахівцям, які краще знаються на цій справі.

Матеріал підготувала компанія SOFTICO — рішення з інформаційної безпеки, постачання та ліцензування програмного забезпечення від світових лідерів, CAD-рішення, IT-сервіси з інтеграції та обслуговування». ***(Захист від кібератак у новому віртуальному світі // Компьютерное Обозрение (https://ko.com.ua/zahist_vid_kiberatak_u_novomu_virtualnomu_sviti_139421). 18.11.2021).***

***

«Электронная почта является одним из основных векторов угроз для кибератак в сфере здравоохранения, поэтому безопасность должна быть в центре внимания. Утечки данных не только создают проблемы для медицинских организаций в случае взлома сети, но также могут привести к проблемам с федеральным правительством.

Вот несколько основных советов по кибербезопасности электронной почты для медицинских работников. Но сначала давайте посмотрим, как играет HIPAA.

Понимание HIPAA и его отношение к кибербезопасности

Закон 1996 года о переносимости и подотчетности медицинского страхования (HIPAA) - это закон, который защищает права и конфиденциальность пациентов. Правило HIPAA конфиденциальности устанавливает требования защищенной медицинской информации (PHI) безопасности и соответствия требованиям, а также HIPAA правила безопасности определяет стандарты для защиты PHI в электронном виде (ePHI).

Нарушение HIPAA может привести к значительным штрафам и другим расходам. Некоторые из наиболее распространенных нарушений HIPAA включают несанкционированный доступ или раскрытие PHI с помощью успешных фишинговых атак по электронной почте.

Шифрование электронной почты

Даже если вас не нарушат, отсутствие соответствующих мер безопасности также может нарушить HIPAA, если вы отправите электронное письмо в виде простого текста. Шифрование электронной почты предотвращает перехват сообщений хакерами. Это гарантирует, что единственные глаза, читающие вашу переписку, принадлежат предполагаемому получателю.

Министерство здравоохранения и социальных служб (HHS) оставило некоторые требования безопасности HIPAA расплывчатыми, чтобы позволить организациям выбирать меры защиты, которые лучше всего соответствуют их потребностям.

Согласно HIPAA, требование шифрования электронной почты является «адресуемым», что означает, что оно должно быть реализовано только в том случае, если оценка риска определяет, что это необходимо для управления риском PHI. Если PHI передается в электронном виде (например, по электронной почте), она должна быть зашифрована «всякий раз, когда это будет сочтено целесообразным».

Если защищенные организации определяют, что шифрование - не лучший способ действий, им необходимо задокументировать свои аргументы и реализовать эквивалентные меры безопасности для защиты PHI. Однако нет альтернативы, которая была бы столь же эффективной, как шифрование, что означает, что шифрование электронной почты фактически требуется.

Многие поставщики услуг электронной почты автоматически шифруют свои сообщения с помощью протокола TLS. Но не все почтовые службы поддерживают шифрование. Около 10% электронной почты передается в виде обычного текста, то есть его может прочитать любой.

Следовательно, для отправки электронной почты, соответствующей требованиям HIPAA, вы должны изучить комплексное решение для шифрования электронной почты, которое защищает все исходящие сообщения как в состоянии покоя, так и в пути.

Постоянное обучение сотрудников

Чем проще использовать вашу систему защиты электронной почты, тем лучше - люди склонны делать ошибки. Фактически, человеческая ошибка является причиной 95% утечек данных, поэтому важно непрерывное обучение сотрудников по вопросам кибербезопасности.

Киберпреступники атакуют поставщиков медицинских услуг с помощью вредоносных электронных писем, содержащих вредоносное ПО. Все, что требуется, - это один сотрудник, щелкнувший ссылку или открыв вложение, чтобы программа-вымогатель заразила вашу систему.

Обучение должно охватывать такие темы, как:

Политики и процедуры кибербезопасности

Как безопасно пользоваться электронными устройствами

Как распознать и заблокировать вредоносные электронные письма

Хакеры часто меняют свои методы, поэтому сотрудники должны постоянно получать информацию о последних проблемах безопасности и способах их предотвращения. Вы также можете проверить готовность своей команды, отправив поддельное фишинговое письмо и узнав, кто нажимает на него, чтобы убедиться, что все сохраняют бдительность.

Однако независимо от того, насколько хорошо обучены ваши сотрудники, вы не можете гарантировать, что кто-то не совершит ошибку, поэтому вам необходимо использовать надежные меры безопасности входящей электронной почты.

Безопасность входящей электронной почты

Хотя вам не нужна защита входящей электронной почты, чтобы соответствовать требованиям HIPAA, это, безусловно, помогает предотвратить утечки данных. В конце концов, поставщики медицинских услуг являются большой мишенью для киберпреступлений из-за большого количества ценных данных, которые они хранят, уязвимых поверхностей для атак и слабой кибербезопасности, которая широко распространена в этой области.

Киберпреступники полагаются на слабую безопасность входящей электронной почты и человеческую ошибку, чтобы проникнуть в вашу систему. Они могут заблокировать вас из вашей сети и повлиять на вашу способность лечить пациентов или потребовать выкуп за безопасное возвращение украденных данных.

Управление по гражданским правам (OCR) HHS может провести расследование после нарушения, которое может привести к большим штрафам и составлению плана корректирующих действий, если обнаружит вашу вину.

В конечном счете, реализовать защиту входящей электронной почты дешевле, чем стать жертвой киберпреступности.

Заключение

Самый значительный риск безопасности не связан с вашей ИТ-системой; именно ваши сотрудники склонны к человеческой ошибке и становятся жертвами мошенничества по электронной почте. Вот почему обучение персонала так важно для предотвращения кибератак.

Но независимо от того, сколько обучения вы проводите, человеческая ошибка неизбежна, поэтому наличие надежной защиты входящей электронной почты также необходимо для здравоохранения.

Даже если ваша электронная почта поддерживает шифрование, ваша электронная почта будет доставлена в виде обычного текста, если ваш получатель этого не сделает, что само по себе является нарушением HIPAA. Не забудьте добавить дополнительный уровень безопасности, прежде чем делиться ePHI по электронной почте с пациентами». ***(Hoala Greevy. Cybersecurity best practices for email communications // Contemporary OB/GYN® (https://www.contemporaryobgyn.net/view/cybersecurity-best-practices-for-email-communications). 23.11.2021).***

***

«В то время как кибербезопасность неизменно рассматривается как главная проблема государственных и местных органов власти, согласно недавнему опросу, почти четверти чиновников местных органов власти и их сотрудников разрешено отказаться от обучения по вопросам кибербезопасности.

Национальный обзор инициатив по кибербезопасности и облачным технологиям местных органов власти от CompTIA Public Technology Institute в 2021 году показал, что 92 процента респондентов заявили, что их юрисдикция предлагает

обучение сотрудников по вопросам кибербезопасности, при этом 59 процентов заявили, что обучение проводится на постоянной основе в течение года, а 34 процента заявили, что обучение предоставляется 1 раз в год.

Однако на вопрос, освобождены ли избранные должностные лица, их сотрудники и высшее руководство от обучения киберпространству, 24 процента ответили утвердительно, что, как указывается в отчете, проблематично по нескольким причинам.

«Важно помнить, что адреса электронной почты и контактная информация избранных лидеров и руководства легко доступны, а это означает, что эти должностные лица являются основными целями для попыток фишинга и зондирования государственных ИТ-систем», - отмечается в отчете. «Разрешение на исключения также может стать плохим и деморализующим примером для других в организации, которые обязаны следовать строгим протоколам».

Алан Шарк, генеральный директор и исполнительный директор Института общественных технологий CompTIA, сказал Route Fifty, что для высших должностных лиц нет оправдания освобождению от кибер-обучения. «Эти сокращения вызваны тем, что они не хотят быть частью этого», - говорит он, отмечая один пример, когда ИТ-директор округа был наказан за рассылку фишингового теста избранным должностным лицам. «Когда у вас есть эти исключения, слухи становятся известными, и это плохо для морального духа».

Что такое кибербезопасность местного самоуправления?

Опрос проводился в августе и сентябре 2021 года, в нем приняли участие более 75 ИТ-руководителей местных органов власти.

Согласно отчету, 81 процент ИТ-руководителей заявили, что в их местных органах власти действует государственная политика кибербезопасности, которая устанавливает правила поведения сотрудников, а также меры безопасности и процедуры, а 73 процента респондентов заявили, что их политика была пересмотрена за последние 12 месяцев. «PTI напоминает руководителям, что эффективность политик и процедур зависит от их анализа и, при необходимости, тестирования», - отмечается в отчете.

Что касается сетевой безопасности и аудита, 33 процента респондентов заявили, что их муниципалитет «провел аудит сети или безопасности всех ИТ-систем и политик» в течение последних 12 месяцев, согласно отчету.

В то время как 54 процента сообщили, что они тестировали или проверяли некоторые системы и политики, «тревожные» 13 процентов не проводили никаких системных тестов или проверок в прошлом году, согласно отчету.

Все больше местных правительственных агентств используют политики управления мобильными устройствами, при этом 65 процентов респондентов заявили, что у них есть политика для доступа сотрудников или подрядчиков к правительственным информационным системам. Этот показатель вырос на 10% по сравнению с опросом PTI 2020 года.

Полностью 90 процентов респондентов заявили, что их организация имеет страхование кибер-ответственности, по сравнению с 78 процентами в 2020 году. Однако, согласно отчету, полисы киберстрахования становятся все более сложными.

«Возможно, именно поэтому только 23% ИТ-руководителей заявили, что полностью знакомы с требованиями и процедурами страховых полисов, которым необходимо незамедлительно следовать в случае нарушения или инцидента; 65% считают, что они в некоторой степени знакомы со своими политическими требованиями, а 12% считают, что они совсем не знакомы со своими политическими требованиями», - говорится в отчете.

Как населенные пункты работают с государствами по вопросам кибербезопасности?

Эксперты давно указали на необходимость более тесного сотрудничества между правительствами штата и местными властями в области кибербезопасности.

Когда его попросили оценить отношения между местными органами власти и правительствами штата в области кибербезопасности, в частности, в отношении обмена информацией, ресурсов, образования и обучения, предоставляемых государством местным органам власти, 31% оценили отношения как отличные.

Еще 44 процента респондентов оценили отношения как справедливые, а 25 процентов - как плохие.

«Очевидно, что необходимо проделать большую работу для развития сотрудничества», - отмечается в отчете. «Такие организации, как CompTIA-PTI и Национальная ассоциация государственных директоров по информационным технологиям (NASCIO), продолжают настаивать на информировании государственных и местных властей о необходимости построения эффективных и надежных партнерских отношений. Несмотря на эти стоящие цели и инициативы, многие технические лидеры часто сетуют на то, что у них почти нет отношений с государственными ИТ-агентствами, не говоря уже о государственном ИТ-директоре»…». ***(Phil Goldstein. Local Officials Are Sometimes Exempted from Cybersecurity Awareness Training // CDW LLC (https://statetechmagazine.com/article/2021/11/local-officials-are-sometimes-exempted-cybersecurity-awareness-training). 24.11.2021).***

***

«…основные проблемы кибербезопасности сегодня в каждом уголке земного шара.

Африка

В нескольких африканских странах есть очень хорошо развитые системы мобильных цифровых валют с миллионами пользователей, такие как M-Pesa и MFS Africa. Люди используют их для заработной платы, продуктов и транспорта в некоторых странах, особенно в Кении. Банды атакуют эти системы в надежде украсть деньги у клиентов. В то время как большинство глобальных оценок уязвимости больше всего беспокоит защиту данных, эти мобильные системы цифровой валюты заботятся о защите денег.

Прибрежные городские районы Африки также подвергаются риску атак программ-вымогателей в портах. Например, порты в Южной Африке были отключены после крупной кибератаки на один из портов.

Региональная и международная напряженность в Восточной Африке и других регионах порождает угрозы кибербезопасности со стороны кибершпионажа, в

последнее время с использованием шпионского ПО Pegasus. По состоянию на конец 2020 года около 11 африканских национальных правительств обнаружили шпионское ПО Pegasus. Они предположили, что это часть шпионской работы как внутри региона, так и из-за границы.

Угрозы кибербезопасности в Северной и Южной Америке

Латинская Америка сталкивается с двойным ударом: широкое использование Интернета и высокий уровень атак по всем направлениям, но низкая координация между правительствами и промышленностью. Также существует низкая осведомленность общественности о киберпреступности из-за отсутствия государственных программ по просвещению населения.

В основе новостей лежат темы кибербезопасности, связанные с пандемией, которая вызывала волну за волной мошенничества, атак программ-вымогателей и фишинговых атак, связанных с утечкой данных. Многие из них используют материалы социальной инженерии, связанные с COVID. Одна из основных причин - это разжигающие страх фишинговые атаки, связанные с COVID. Они нацелены на сбор информации, необходимой преступникам для совершения страховых случаев и мошенничества с личными данными. Электронная почта предлагает стимулирующие деньги, доступ к вакцинам и другие преимущества в обмен на личную информацию или загрузку вредоносного ПО.

Самыми целевыми странами Латинской Америки являются страны с крупнейшей экономикой: Бразилия, Мексика, Колумбия и Аргентина.

Мексика недавно подверглась очень крупномасштабным атакам вредоносного ПО на нефтяного гиганта Pemex, а также на Министерство экономики.

В Латинской Америке и Карибском бассейне количество атак, спонсируемых государством, как правило, увеличивается до заключения международных договоров, экономических саммитов и других подобных мероприятий. Вредоносное ПО EVILNUGGET было развернуто для этой цели, в основном, против транспортных компаний и объектов, затронутых китайской инициативой «Один пояс, один путь».

Соединенные Штаты являются мишенью для всех видов угроз кибербезопасности, особенно для очень крупномасштабных атак, спонсируемых государством, таких как атака Solar Winds. Это долгосрочные и очень сложные. Злоумышленники могут преследовать самые разные цели - от политического и промышленного шпионажа до оказания влияния на операции.

Азия

Геополитическая напряженность в регионе является движущей силой спонсируемых государством операций по оказанию влияния, кибершпионажа и целенаправленных финансовых преступлений. Фишинговые атаки остаются распространенной отправной точкой для многих кибератак в Азии.

Напряженность между странами порождает большое количество киберугроз как со стороны национальных государств, так и со стороны неправительственных субъектов во всех вовлеченных странах. Посмотрите на Китай и Индию, Китай и Тайвань, Индию и Пакистан, Северную Корею и Южную Корею и, конечно, напряженность между США и Китаем, Северной Кореей и Россией.

Кроме того, большая часть мировой инфраструктуры цепочки поставок электроники находится в Азии. Таким образом, глобальная тенденция к атакам и сбоям в цепочке поставок остро ощущается в регионе. Экспортеры электроники, такие как Вьетнам и Малайзия, зависят от покупателей и производителей в Китае, и наоборот. Кроме того, мир зависит от товаров, произведенных в Китае. Нарушение любой части этой цепочки поставок замедляет поставки, поднимает цены и оказывает давление на всех, кого это касается.

Многие из этих связей предполагают сотрудничество и партнерство на публике и соперничество в частной жизни. Соперничество разыгрывается через нападения и шпионаж.

Особого упоминания заслуживает Северная Корея, поскольку у этой страны есть надежный государственный аппарат для кибератак. С другой стороны, у страны почти нет целей для иностранных противников из-за отсутствия там развития и подключения к Интернету.

Россия и Турция

Турция и Россия находятся как в Европе, так и в Азии. Многие глобальные угрозы кибербезопасности, как спонсируемые государством, так и преступные, исходят, в частности, из России. В прошлом году, согласно отчету Microsoft, почти 60% наблюдаемых в мире атак, спонсируемых государством, начинались с правительства России, и одна треть успешных кибератак в мире со стороны негосударственных субъектов также началась с него. Новая волна атак типа «программа-вымогатель как услуга» - это в основном российский тренд. Непропорционально большая доля информационных операций и кампаний по дезинформации, связанных с выборами, также начинается в России.

Угрозы кибербезопасности в Европе

Европейские больницы серьезно пострадали от опасных атак с использованием программ-вымогателей в Ирландии, Франции и других странах. Две французские больницы атакованы в течение недели после того, как в 2020 году пострадали больницы в семи французских городах, злоумышленники, использующие криптовирус, Рюк усилили стрессовый фактор. В конце концов, оба боролись с COVID-19 и были на пределе возможностей. Нападение на Ирландию в начале этого года нанесло удар по Управлению здравоохранения, которое нарушило работу системы здравоохранения по всей стране и вынудило медицинских работников прибегать к использованию бумажных документов.

В целом, по данным Агентства по кибербезопасности Европейского союза, количество серьезных кибератак с 2020 по 2021 год примерно удвоилось. Количество атак троекратного вымогательства растет. Цена взлома данных в этом регионе стремительно растет.

Ближний Восток

Ближневосточный регион имеет более чем справедливую долю угроз кибербезопасности, спонсируемых государством. Они направлены на то, чтобы сбить с толку соперников, вызвать экономические трудности, а иногда даже вызвать внутренние политические трения. Например, недавняя атака в Иране привела к серьезным сбоям в продажах бензина потребителям. В очевидной реакции люди взломали таблички с бензином, критикуя правительство за бензиновые линии.

Любой анализ уязвимости на Ближнем Востоке должен учитывать региональный конфликт.

Многие типы и методы кибератак во всем мире схожи, и их возглавляют вредоносные программы и программы-вымогатели. При этом цели атакующих сильно разнятся. Все эти атаки объединяет одно: они происходят по всему миру. ***(Mike Elgan. Top Cybersecurity Threats Around the Globe // IBM (https://securityintelligence.com/articles/top-cybersecurity-threats-global/). 17.11.2021).***

***

«Ряд явных атак с использованием программ-вымогателей проливает свет на меры, доступные федеральному правительству для помощи целевым компаниям. Ключевое слово там - «помощь», - сказал на прошлой неделе в CyberNext DC представитель Джим Ланжевен, доктор медицинских наук. Правительство не защитит их полностью. Наиболее значимые компании в секторах, определяемых как критическая инфраструктура, должны сначала иметь достаточный уровень зрелости кибербезопасности, чтобы они могли участвовать в собственной защите.

Индустрии финансовых услуг является одним из таких отраслей. Учитывая, что это глобально критически важно, и поэтому большая часть его деятельности сегодня на 100% зависит от ИТ-систем и Интернета, финансовые фирмы, такие как банки и кредитные союзы, должны быть одними из самых бдительных.

Новый отчет Constella Intelligence поднимает вопросы о том, достаточно ли делает сектор для защиты себя, особенно среди крупнейших - а значит, наиболее важных - фирм. Компания «провела анализ показателей, относящихся к цифровым уязвимостям крупных организаций Finserv… путем агрегирования и анализа уязвимостей двадцати крупнейших финансовых компаний из списка Fortune Global 500, включая выборку руководителей этих компаний». Анализ охватывал период 2018-2021 гг.

Он выявил 6 472 утечки и утечки, а также более 3,3 миллиона незащищенных записей от 20 компаний, при этом количество раскрытых записей выросло «в шесть раз» всего за два года. Около двух третей нарушений и утечек включали информацию, позволяющую установить личность (PII), в том числе топ-менеджеров взломанных компаний в 71% зарегистрированных случаев.

В отчете признается, что всемирная пандемия сыграла свою роль. Многие финансовые учреждения были вынуждены перейти на гибридные модели и модели удаленной работы, что резко увеличило количество конечных точек, подверженных риску, и лишило компании ресурсов кибербезопасности.

Но «без контроля эти открытые данные представляют собой серьезный цифровой риск для финансовых компаний с обширными поверхностями атак, конфиденциальными данными и критически важными операциями», - написал Шон Тирни, вице-президент Constella по анализу угроз.

Сотрудники сектора Finserv увеличивают этот риск из-за своего собственного поведения, говорится в отчете, используя учетные записи электронной почты своей компании, например, для посещения второстепенных сайтов - развлечений, новостей, розничной торговли и игр. И раскрытие PII руководителей высшего звена

является еще одним фактором, ускоряющим риск, потому что они, как правило, имеют привилегированный доступ к сетям, данным и критически важной инфраструктуре своих компаний.

«Хотя кибератаки могут показаться исключительно технологическими или корпоративными угрозами, человеческий и социальный компоненты имеют центральное значение», - сказал Тирни Nextgov. «Все более распределенные сети означают, что злоумышленники могут нарушить работу критически важных систем из-за широкого спектра векторов атак, часто используя сотрудников и их открытую личную информацию и корпоративные учетные данные для проникновения в сети и причинения значительных сбоев и беспорядков. Финансовые учреждения должны учитывать эти факторы, чтобы снизить свой кибер-риск».

Constella предлагает четыре рекомендации по снижению профиля риска финансовых организаций:

Избегайте использования корпоративной электронной почты и связанных корпоративных учетных данных за пределами рабочей среды.

Ограничьте использование личных данных как в корпоративной среде, так и в социальных сетях.

Используйте надежный пароль, соответствующий установленным в компании политикам безопасности, и не используйте этот пароль для личных учетных записей.

Постоянно отслеживайте внешний вид угроз на предмет любых признаков раскрытых учетных данных». ***(Patience Wait. A new report by Constella Intelligence raises questions as to whether the sector is doing enough to protect itself // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/report-shows-global-financial-giants-are-risk-cyberattacks/187087/). 24.11.2021).***

***

«Исторически сложилось так, что между ИТ-командами и командами по кибербезопасности было много негатива и разногласий. Команды безопасности можно рассматривать как «блокираторов», которые не позволяют ИТ-специалистам вносить позитивные изменения в организацию. Между тем, группы безопасности часто чувствуют, что их коллеги по ИТ-операциям просто не заинтересованы в защите организации от внешних угроз.

Хотя есть аргументы с обеих сторон, мы в индустрии безопасности должны принять простой факт: ИТ-отделы существуют намного дольше, чем мы, и их процессы более зрелые.

40 ЛЕТ УЛУЧШЕНИЯ ПРОЦЕССА

Рассмотрим одну из самых известных структур для управления ИТ-услугами (ITSM): библиотеку ИТ-инфраструктуры (ITIL). Разработанная в 1980-х годах правительством Великобритании, ITIL превратилась в наиболее полный набор ИТ-практик из когда-либо созданных. Он используется более широко, чем любой другой фреймворк, и даже Microsoft использовала его в качестве основы для своей Microsoft Operations Framework (MOF).

Чтобы увидеть, чему команды по кибербезопасности могут извлечь из этого урок, рассмотрим пять принципов жизненного цикла ITIL:

Стратегия обслуживания определяет перспективу, позицию, планы и шаблоны, которые поставщик услуг должен выполнять для достижения бизнес-результатов.

Дизайн услуг включает в себя дизайн услуг, управленческих практик, процессов и политик, необходимых для реализации стратегии.

Переход службы гарантирует, что новые, измененные или выведенные из эксплуатации службы соответствуют ожиданиям бизнеса.

Работа службы координирует действия и процессы по предоставлению и управлению услугами на согласованных уровнях. Он также управляет технологиями, используемыми для предоставления и поддержки услуг.

Непрерывное совершенствование услуг обеспечивает соответствие услуг изменяющимся потребностям бизнеса путем выявления и внедрения улучшений ИТ-услуг.

ЗАЩИТА ОПЕРАЦИЙ, НЕ БЛОКИРОВКА УГРОЗ

Обратите внимание на то, что ITIL фокусируется не на отдельных системах или процессах, а на удовлетворении бизнес-ожиданий на заранее согласованном уровне. ITIL делает упор на правильное освоение основ и наличие систем и процессов для достижения самой важной цели: минимизации времени простоя.

Группы ИТ-операций уже много лет знают, что простои неизбежны, и все, что они могут сделать, - это ограничить их продолжительность и частоту. Это цель соглашений об уровне обслуживания - сводить время простоя к приемлемому минимуму. Это жизненно важно, и это резко контрастирует с тем, как индустрия кибербезопасности изображает свою функцию.

В кибербезопасности мы часто думаем о блокировании угроз, устранении уязвимостей и поиске индикаторов компрометации. Но это просто действия, они не являются целью кибербезопасности. Наша истинная цель - поддерживать доступность, целостность и конфиденциальность систем, активов и данных наших организаций.

Подобно ИТ-отделам, мы можем предположить, что некоторый уровень «неудач» неизбежен, поскольку мы стремимся к этой цели. Почти все организации в какой-то момент будут взломаны, поэтому важно рассмотреть вопрос о том, как минимизировать частоту, влияние и продолжительность взломов. Скотт Аллдридж, президент Института ИТ-процессов (ITPI) и MSSP IP Services, объясняет:

«Используйте подход выжженной земли. Предположим, что вы уже были взломаны и вам нужно восстановить. Какая точка восстановления вам удобна и сколько времени это может занять? Как только вы получите ответы, перепроектируйте элементы управления безопасностью оттуда, как ИТ отдел бы».

ВАЖНОСТЬ УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ

Чтобы гарантировать соответствие бизнес-ожиданиям, одним из наиболее важных компонентов ITIL является управление изменениями, которое является основной функцией передачи услуг. На протяжении многих лет ИТ-отделы осознавали важность управления изменениями для поддержания SLA на приемлемом уровне.

В The Visible Ops Handbook авторы объясняют (выделено нами):

«Высокопроизводительные ИТ-организации исключают изменения как причинный фактор для простоя как можно раньше в цикле ремонта. Они идентифицируют активы, непосредственно связанные с перебоями в обслуживании, и проверяют все изменения, внесенные в эти активы за предыдущие 72 часа. Эта информация [сравнивается] со всеми санкционированными и запланированными изменениями. [...] Когда проблемы передаются менеджерам по проблемам, они имеют под рукой все соответствующие и причинно-следственные доказательства и [...] могут успешно диагностировать проблемы без входа в какую-либо инфраструктуру более 50% времени!»

Этот подход напрямую применим к кибербезопасности. Устанавливая цели (стратегия обслуживания), базовый план для приемлемых уровней обслуживания и действий (дизайн сервиса) и управляя изменениями по сравнению с этим базовым уровнем (переход сервиса), группы кибербезопасности могут достичь того же уровня операционного успеха (работа сервиса), что и ИТ-отделы.

Подумайте об этом. Когда в последний раз ИТ-системы вашей организации отключались по причинам, не связанным с безопасностью, и как долго это длилось?

Обеспечение целостности системы: огромный шаг за пределы FIM

Традиционные концепции ИТ-операций, такие как управление изменениями, имеют решающее значение для достижения истинной цели кибербезопасности - не блокирование конкретной угрозы, а поддержание доступности, целостности и конфиденциальности системы.

Однако для того, чтобы управление изменениями работало, вам необходимо точно знать, как должна выглядеть ваша среда, чтобы вы могли отслеживать изменения, исходя из этого базового уровня.

Обеспечение целостности системы (SIA) — это совершенно другой подход к кибербезопасности, в котором основное внимание уделяется основам. Вместо того, чтобы пытаться определить и классифицировать все плохие вещи, вместо этого он определяет все, что это разрешено в экологически и блокирует все остальное.

Конечно, необходим некоторый уровень управления в порядке исключения. Но по сути, SIA и проверка целостности дает организациям полный контроль над тем, что происходит в их среде.

Что произойдет, если вы будете знать каждый раз, когда что-то добавляется, удаляется или изменяется в вашей среде, и вы останавливаете все, что не санкционировано… и расширяете эту возможность для всех классов активов?

Программы-вымогатели и другие вредоносные программы не могут работать в этой среде.

Злоумышленники не могут проникать в сеть или извлекать данные.

Никто не может изменять файлы или конфигурации, чтобы сделать их опасными или несовместимыми.

Пользователи не могут случайно запустить вредоносные вложения.

Никто (даже привилегированные администраторы) не может изменять важные системные файлы.

Такой подход устраняет значительную часть угроз, которые могут возникнуть в ИТ-среде, с минимальным участием человека...» ***(Jacqueline von Ogden. What***

Cybersecurity Can Learn from IT // Cimcor, Inc (https://www.cimcor.com/blog/what-cybersecurity-can-learn-from-it). 04.11.2021).

***

«…Кибербезопасность — это профессия, в которой важны навыки. Независимо от вашей сертификации или образования, вы должны быть опытным и талантливым профессионалом. И именно здесь не срабатывают самые традиционные стратегии найма. Исторически сложилось так, что рекрутеры сосредотачивались на требовании формальной квалификации в области кибербезопасности. Проблема с использованием только этих показателей заключается в том, что на сертификационных экзаменах часто используются вопросы с несколькими вариантами ответов, и они сосредоточены на формировании традиционных теоретических знаний. Отрасли необходимо сместить акцент на распознавание навыков в интерактивных сценариях, поскольку современный профессионал в области кибербезопасности требует хакерского мышления, сформированного с помощью практических упражнений и реальных лабораторий по тестированию на проникновение.

Сертификаты могут быть способом определить теоретические знания кандидата на работу, если они хорошо разработаны. Но лучший подход - дополнить сертификационные экзамены с несколькими вариантами ответов данными из программ практического обучения. Такие организации, как (ISC) I и SANS, безусловно, играют важную роль в проверке знаний. Но участие кандидата в сообществе кибербезопасности может лучше отражать возможности кандидата. Это показывает понимание как теории, так и практики.

Оценка практических навыков показывает, что соискатели не только понимают теорию, но также могут применять ее в реальных жизненных ситуациях как в защитных, так и в наступательных ролях. Образование должно быть совместным делом, в котором предприятия извлекают выгоду из личного опыта экспертов. Можно доверить экзаменам с несколькими вариантами ответов для проверки теоретических знаний, но оценка практических навыков лучше отражает практические способности кандидата. Ландшафт угроз кибербезопасности постоянно развивается, и заявители должны иметь возможность воспроизводить те же эксплойты, которые используют злоумышленники. Многие компании на собственном горьком опыте убедились, что сертификаты не всегда являются лучшим доказательством опыта и способностей.

Умерьте свои ожидания

Еще одна проблема для отрасли — это нереалистичные требования к определенным должностям, которые часто запрашиваются рекрутерами, практически не имеющими опыта в области кибербезопасности. Это приводит к тому, что огромное количество вакантных должностей остаются незаполненными. Например, распространенной проблемой является настойчивое требование кандидата, имеющего сертификат CISSP, во всех объявлениях о вакансиях в сфере кибербезопасности. Людям необходимо несколько лет опыта работы в отрасли, чтобы получить квалификацию CISSP, и эта сертификация в основном подходит для ролей в исполнительном менеджменте. CISSP отлично подходит для этих ролей в

области кибербезопасности, но нереально ожидать его для должностей начального уровня.

Медицинская промышленность решила эту проблему. Медсестры нанимают с квалификацией медсестры. Хирурги имеют медицинские степени, применимые к хирургии. Есть специализации доктора медицины для всех медицинских работников, будь то хирург, дерматолог или терапевт. Никто не ожидает, что медсестра будет иметь степень доктора медицины, и никто не ожидает, что у хирурга будет степень медсестры. Так, например, тестировщикам нужны учетные данные для тестирования проникновения, а не исполнительные полномочия, такие как CISSP.

Сертификаты отлично подходят для измерения роста сотрудника. Рекрутеры начали использовать сертификаты, чтобы отфильтровать неквалифицированных кандидатов, чтобы помочь им решить проблему отсутствия знаний, необходимых для отбора кандидатов. Эта система работала какое-то время, но со временем соискатели обнаружили, что они могут сдать экзамены и получить сертификат, не имея опыта. В настоящее время трудно идентифицировать кандидатов, получивших сертификацию, потому что они были квалифицированными и увлеченными, и кандидата, получившего сертификацию, потому что она была обязательной.

Сообщества по кибербезопасности

Именно здесь приходят на помощь преданные, целенаправленные сообщества кибербезопасности. Здесь люди могут играть, тренировать и развивать свои навыки на основе современных практик кибербезопасности. Команды по найму должны использовать эти платформы в своих интересах; наблюдение за последними инструкциями по обучению и навыкам, чтобы увидеть, какие проблемы распространены в отрасли. Он не только может предоставить доказательства недавнего обучения кандидата, но и команды по найму также должны использовать форумы сообщества для поиска лучших талантов.

Рекрутеры должны использовать практические методы при поиске новых талантов. Зоны обучения также могут использоваться компаниями для создания внутреннего процесса оценки, или они могут работать с компаниями, которые обучают этих профессионалов, и доверять им.

Поскольку менеджеры по найму часто не имеют опыта работы в сфере кибербезопасности, компаниям следует искать и работать рука об руку с платформами обучения, центрами оценки и органами сертификации, чтобы убедиться, что они оценивают необходимые навыки. С помощью этих инструментов они могут совместно создавать оценочные лаборатории и приглашать кандидатов для демонстрации в них своих знаний. Последний момент, к которому нужно обратиться, - это время. Проще говоря: если бизнес ждет атаки, прежде чем создавать команду кибербезопасности, очевидно, что это слишком мало, слишком поздно.

Компании должны работать над усилением безопасности, разрабатывать строгие политики безопасности и создавать сильную культуру безопасности. Это требует найма правильных людей. Все могут быть обучены, и компании должны инвестировать в свою базу талантов в области кибербезопасности, проводя для них обучение. Тренировки также должны проводиться периодически и непрерывно, а не один раз. Технологии и ландшафт угроз кибербезопасности постоянно развивается. Эффективная защита требует, чтобы ваша команда по кибербезопасности всегда

была в курсе своих навыков и знаний». ***(Nikos Fountas. How to Fix Cybersecurity Recruiting // Techstrong Group Inc. (https://securityboulevard.com/2021/11/how-to-fix-cybersecurity-recruiting/). 23.11.2021).***

***

«В недавнем отчете Unisys утверждается, что 61 процент удаленных сотрудников считают себя ответственными за поддержание цифровой безопасности, однако лишь 21 процент помнит о сложных кибератаках и проблемах безопасности (таких как взлом SIM-карты).

Во время пандемии Covid-19 людям приходилось работать в домашнем режиме, а не в офисе. И теперь это стало образцом новой нормальной жизни.

В отчете Unisys утверждается, что нет уверенности в том, что офисный режим работы вернется. 83% рекрутеров указывают, что переход с офиса на удаленную работу стал эффективным и выгодным для их компаний. Он также утверждает, что более пятидесяти пяти процентов их сотрудников стремятся работать удаленно, по крайней мере, трижды в неделю, несмотря на уменьшение пандемических условий. Подозрения в отношении кибербезопасности в Интернете резко возросли, и, несмотря на все опасения, в отчете отмечается, что отсутствие знаний об основных опасностях и рисках кибербезопасности приводит к тому, что удаленные работники невежественно ведут себя неуверенно, заставляя рекрутеров рисковать.

В ходе анализа было обнаружено полное отсутствие у работников понимания того, как предотвращать кибератаки и как справляться с ними. Около 39 процентов респондентов заявили, что они не проявляют осторожности при переходе по сомнительным ссылкам, несмотря на более 80 процентов зарегистрированных фишинговых атак. Только 21 процент опасаются и осведомлены о дальнейших замысловатых уловках мошенничества, таких как взлом SIM-карты, при котором мошенник получает доступ к управлению сим-картой пользователя.

В отчетах также говорится, что около сорока пяти процентов пользователей в США, Австралии и Новой Зеландии устанавливают программное обеспечение, не санкционированное их подразделениями информационных технологий, поскольку для такого рода приложений обычно используются те, которые они используют лично или, возможно,, ожидается, будут более достойными, чем предлагаемые их фирмами.

Около 40% сотрудников очень довольны тем, что делятся своими данными лично и в офисе. Для них тщательный контроль за их работой и деятельностью кажется им заглядыванием через их плечи, чем они не удовлетворены, однако только 18% говорят, что не будут возражать против наблюдения и контроля, но только 12% заявили, что они будут довольны мониторингом микрофона». ***(Arooj Ahmed. Around 8 in 10 of remote workers are not familiar with the sophisticated cybersecurity threats including SIM jacking, reveals a new report // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/around-8-in-10-of-remote-workers-are.html). 24.11.2021).***

***

«В условиях экспоненциального роста объема и разнообразия данных, появления строгих законов о конфиденциальности и постоянно меняющегося ландшафта цифровых угроз кибербезопасность выдвинулась на первый план при принятии важнейших бизнес-решений, включая стратегии слияний и поглощений и оценки. Сегодня на этапе комплексной проверки сделок M&A (слияний и поглощений) необходимо тщательно изучить состояние кибербезопасности цели, чтобы избежать унаследования нежелательных уязвимостей. Однако вместо того, чтобы создавать дополнительную нагрузку на соответствие нормативным требованиям, включение в этот процесс динамично развивающихся методов автоматизации кибербезопасности может дать явное преимущество - получение информации для снижения риска и обогащения процесса принятия решений.

Основные вопросы кибербезопасности при слияниях и поглощениях: регуляторный риск, затраты и общественное доверие

Ставки высоки на пересечении кибербезопасности и слияний и поглощений. Необходимо учитывать вопросы соблюдения нормативных требований и соблюдения конфиденциальности данных, юридические обязательства, стоимость сделки, способность компании поддерживать доверие среди партнеров и потребителей, а также угрозу кибератак.

Консультационный барометр устойчивости 2021 FTI® обнаружил, что почти треть компаний в G20 столкнулись с кибератаками за последние 12 месяцев. Закупки на ранней стадии и до закрытия также оказались привлекательными целями для киберпреступников. В последние годы кибератаки привели к утечке необъявленных деталей транзакций и использовали преимущества расширенных поверхностей атаки для использования после слияния организаций. Злонамеренное вмешательство в процесс слияний и поглощений на любом из этих этапов наносит ущерб финансовым рынкам, влияет на стоимость акций, повышает юридический риск и риск соблюдения нормативных требований и угрожает подорвать как репутацию компании, так и сами сделки. В связи с бурным ростом активности в сфере слияний и поглощений,

Как автоматизация кибербезопасности поддерживает комплексную проверку

Технологии автоматизации, призванные управлять угрозами кибербезопасности, также могут использоваться для повышения скорости, эффективности и стандартизации процесса комплексной проверки данных, что значительно улучшает управление рисками на протяжении всего жизненного цикла слияний и поглощений.

Аналитические данные, основанные на данных, являются ключом к принятию решений, связанных с осмотрительностью, обеспечивая беспрецедентную возможность анализировать комбинацию данных компании, информации из открытых источников и внешней аналитики. Например, понимание существующих и потенциальных уязвимостей имеет решающее значение для определения того, может ли сделка открыть дверь для утечки данных и кибератак. Автоматизация также может ускорить сопоставление данных отчетов о кибербезопасности с фреймворками, чтобы представить общую позицию организации в отношении

конфиденциальности и кибербезопасности таким образом, чтобы способствовать принятию решений на основе рисков.

Дополнительные способы использования автоматизации для поддержки оценок кибербезопасности для комплексной проверки и снижения рисков включают:

Автоматическая пометка рисков до заключения сделки: механизмы оптического распознавания символов и взвешивания позволяют быстро и автоматически идентифицировать конфиденциальную информацию в PDF-файлах, изображениях и других визуальных файлах во всей совокупности данных целевой компании. Эти сведения можно использовать для обозначения областей риска перед заключением сделки, а также для поддержки мер по предотвращению потери данных.

Обнаружение скрытых уязвимостей: цифровой след может выявить области риска, которые ранее не были известны ни цели, ни покупающей стороне, например, случаи подделки домена и взлома бренда.

Понимание масштабов и силы существующих мер защиты данных: визуальная аналитика, измеряющая существующие меры безопасности организации в отношении ее контрактов, список внешних партнеров, хранилища конфиденциальных данных и процессы уведомления о нарушениях, могут помочь покупателям понять, в какой степени целевая компания защита своих конфиденциальных данных. Возможно, потребуется внести корректировки в оценку с учетом пробелов в существующей практике.

Быстрый анализ ключевых документов: расширенные возможности поиска, такие как те, которые используются для сложных электронных обнаружений и расследований, могут быть применены для просмотра существующих контрактов и других документов, чтобы выявить потенциальные риски безопасности. Аналитика также может использоваться для управления и оценки рисков третьих сторон у огромного числа поставщиков, и, поскольку организация устойчива настолько, насколько устойчива ее самая слабая третья сторона, эта аналитика обеспечивает критически важную информацию. Функции автоматического интеллектуального поиска также могут помочь командам понять, что на самом деле существует в наборах данных, которые в конечном итоге будут интегрированы в бизнес, когда сделка будет закрыта.

Помимо комплексной проверки кибербезопасности и конфиденциальности, эти стратегии также помогают проводить оценку зрелости и внутренние расследования. Например, данные, полученные в результате оценки зрелости кибербезопасности, основанной на технологиях, могут превратиться в живую адаптивную информационную панель, которая обеспечивает сравнительный анализ как для портфеля, так и для отрасли.

Риск лежит в основе слияний и поглощений. Именно уверенность и устойчивость, основанные на этих рисках и в ответ на них, определяют лидеров отрасли. То же верно и в отношении кибербезопасности. Таким образом, объединение этих пространств с помощью технологий автоматизации, управляющих процессом должной осмотрительности, представляет собой прекрасную возможность. Поскольку позиция целевой компании в области кибербезопасности быстро становится решающим элементом рисков и выгод, связанных с

потенциальными инвестициями, тщательное изучение гигиены безопасности должно стать приоритетом. Однако именно за счет автоматизации организации, участвующие в слияниях и поглощениях, могут обрести душевное спокойствие, используя возможности технологий, данных и аналитики для управления рисками сделки и создания оптимальных условий для успеха». ***(Dave Harvey, Laura Kippin. How Cybersecurity Automation Can Boost Deal Value and Insights in M&A Due Diligence // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/opinions/cybersecurity-automation-ma-due/). 23.11.2021).***

***

«Новые данные CyberSeek показывают, что за 12 месяцев с октября 2020 года по сентябрь 2021 года в Интернете было 597767 вакансий на должности, связанные с кибербезопасностью.

Работодатели ищут профессионалов в области кибербезопасности на всех этапах карьерного роста; от специалистов по кибербезопасности начального уровня (8 889 вакансий) до аналитиков по кибербезопасности среднего уровня (27 919) и до инженеров по кибербезопасности продвинутого уровня (61 579).

«Заполнение вакансий, связанных с кибербезопасностью, является критической проблемой для работодателей», - сказал Уилл Маркоу, вице-президент по прикладным исследованиям в Emsi Burning Glass. «Устранение этой нехватки талантов жизненно важно для нашей экономической и национальной безопасности, но вы не можете ликвидировать разрыв в талантах, которого не понимаете. Вот почему так важно, чтобы работодатели, преподаватели, политики и частные лица имели действенные данные об их местном персонале в области кибербезопасности».

Новые данные показывают, что предложения специалистов по кибербезопасности хватит только на 68% требуемых рабочих мест в сфере кибербезопасности. В среднем для заполнения должностей в сфере кибербезопасности требуется на 21% больше времени, чем для других должностей в сфере ИТ…» ***(Nearly 600,000 open cybersecurity-related jobs were listed over 12 months // Help Net Security (https://www.helpnetsecurity.com/2021/11/25/open-cybersecurity-related-jobs/). 25.11.2021).***

***

«Несмотря на рост числа кибератак, таких как программы-вымогатели, в последние годы, во многих организациях до сих пор нет директора по информационной безопасности (CISO). Более того, некоторые из них считают, что они им даже не нужны, а другие говорят, что им трудно найти подходящего кандидата из-за растущего дефицита навыков и так называемой «большой отставки».

Новый отчет, опубликованный Navisite, в котором приняли участие 130 специалистов по безопасности, ИТ и комплаенсу, показал, что почти половина (45%) не нанимают CISO. Из этой группы лишь незначительное большинство (58%) считает, что у них должен быть один в команде.

У большинства организаций есть стратегия кибербезопасности, но для большинства (60%) она была разработана другими командами и людьми, кроме

директора по информационной безопасности, - либо ИТ-отделом, либо отделом комплаенс, либо исполнительным руководством.

Фактически, в некоторых компаниях (21%) вообще нет человека, занимающегося исключительно кибербезопасностью, в то время как большинство из них (75%) испытали увеличение общего объема угроз кибербезопасности за последние 12 месяцев.

Вселить уверенность

В отчете также говорится, что отсутствие руководителя, отвечающего за кибербезопасность, подрывает доверие к этим компаниям. Среди фирм, у которых есть директор по безопасности, 70% были уверены в эффективности своих стратегий, а среди фирм без него - 58%.

Наконец, многие респонденты хотели бы, чтобы их организация тратила немного больше денег на решения по кибербезопасности, персонал и обучение.

«Результаты опроса подтверждают то, что мы наблюдаем повсеместно: организации уделяли приоритетное внимание своим усилиям по обеспечению безопасности во время Covid, но в то же время они четко осознают, сколько еще им нужно сделать для эффективной защиты от киберугроз», - сказал он. Аарон Буассонно, директор по информационной безопасности Navisite.

«Данные также указывают на сохраняющуюся проблему в отрасли: нехватку навыков кибербезопасности, которая распространяется на самые высокие уровни. Компании ценят и хотят лидера в области кибербезопасности, но найти и удержать этих людей становится все труднее». ***(Sead Fadilpašić. Nearly half of firms still don't have a CISO // Future US, Inc. (https://www.techradar.com/news/nearly-half-of-firms-still-dont-have-a-ciso). 22.11.2021).***

***

«71% вице-президентов и ИТ-директоров считают, что большое количество инструментов кибербезопасности, которые они используют, негативно влияет на способность их организации обнаруживать и предотвращать угрозы, говорится в отчете Perimeter 81.

В исследовании оценивались ответы 500 ИТ-специалистов из компаний с 50 и более сотрудниками в США. В нем рассматриваются новые тенденции в рабочей силе из-за COVID-19, то, как эти изменения повлияли на кибербезопасность, и их влияние на ИТ-специалистов.

«Гибридная и удаленная работа определенно никуда не денется, - говорит Амит Барекет, генеральный директор Perimeter 81. «Замечательные 87% ответивших компаний будут иметь гибридных работников даже после COVID, и более половины из них будут работать удаленно три-четыре дня в неделю. Это радикальное развитие событий, которое постоянно увеличивает размер поверхности атаки сети и требует от ИТ-специалистов быстрого поиска долгосрочных решений».

«По мере развития кибератак многие поставщики пытаются решить эту постоянно меняющуюся проблему с помощью большего количества решений и дополнительных ограждений», - говорит Саги Гидали, технический директор Perimeter 81.

«Это привело к болезненной и сложной реальности, в которой средний директор по информационной безопасности вынужден управлять десятками решений по кибербезопасности, что ограничивает их способность обеспечивать безопасность и защиту своих сетей. Мы называем эту проблему «ловушкой киберсложности».

Дополнительные выводы

50% компаний с более чем 1000 сотрудников используют 20 или более инструментов и решений для кибербезопасности.

64% сообщают, что в 2020-2021 годах они столкнулись с серьезным инцидентом в области кибербезопасности, в том числе с программами-вымогателями или фишингом.

34% компаний сделали кибербезопасность своим приоритетом из-за освещения киберинцидентов в новостях

59% признали, что платили выкуп кибер-ворам.

Затраты на восстановление 47% жертв кибератак составили от 100 000 до 1 миллиона долларов.

«Одна из сложностей, связанных с быстрым внедрением гибридной работы, связана с растущим стеком приложений SaaS в организации - средами, которые являются динамическими, непрерывно обновляющимися, с ошеломляющим количеством конфигураций, которые должны контролировать и контролировать CISO и группа безопасности. Более того, зачастую команда безопасности не имеет никакого представления о том, что происходит в приложениях SaaS, поскольку администраторы SaaS находятся вне группы безопасности, в отделе, который преимущественно использует этот SaaS», - сказал Маор Бин, генеральный директор Adaptive Shield. Справка Net Security». ***(Cyber complexity negatively impacts a company's ability to respond to threats // Help Net Security (https://www.helpnetsecurity.com/2021/11/18/number-cybersecurity-tools/). 18.11.2021).***

***

Сполучені Штати Америки та Канада

«Конгресс США в пятницу принял Закон об инвестициях в инфраструктуру и рабочие места на 1,2 триллиона долларов, знаменательный законопроект администрации Байдена, который выделит 1,9 миллиарда долларов в виде нового финансирования кибербезопасности для федерального правительства. Законопроект, долгое время находившийся на рассмотрении в Конгрессе на фоне борьбы демократов, был принят Палатой 228-206 голосов и теперь перемещен на стол Джо Байдена, который планирует провести церемонию подписания после перерыва в работе Конгресса.

Среди его компонентов кибербезопасности законопроект включает программу грантов в размере 1 миллиарда долларов для оказания помощи правительствам штатов, местных, племенных и территориальных органов власти в защите от киберугроз и модернизации систем, особенно вокруг критически важной

инфраструктуры. Согласно законопроекту, средства будут распределяться Федеральным агентством по чрезвычайным ситуациям (FEMA) в течение четырех лет, начиная с 2022 года, под руководством Агентства по кибербезопасности и безопасности инфраструктуры США (CISA).

Также в законопроект включены: Закон о киберответе и восстановлении от 2021 года, предусматривающий 100 миллионов долларов в Фонд киберответа и восстановления для поддержки жертв киберпреступлений. Автономная мера была первоначально введена в апреле сенатором Гэри Петерсом из штата Мичиган, председателем сенатского комитета по внутренней безопасности и делам правительства, и Робом Портманом из штата Огайо, высокопоставленным членом комитета.

Законопроект об инфраструктуре также предусматривает выделение 21 миллиона долларов на привлечение средств для офиса Национального кибердиректора Криса Инглиса, который планирует нанять до 25 специалистов к концу 2021 года, а в конечном итоге от 75 до 80 в целом.

Закон также обязывает Агентство по охране окружающей среды (EPA) работать с CISA над выявлением общественных систем водоснабжения, которые в случае кибератаки могут поставить под угрозу общественное здоровье и безопасность. Эта мера последовала за новыми усилиями CISA по выявлению «основных системно важных объектов» для защиты систем от глобальных киберугроз.

Законопроект также направлен на модернизацию стареющей инфраструктуры страны, включая средства на строительство дорог и мостов, общественного транспорта, пассажирских и грузовых железнодорожных перевозок, электромобилей, электросетей, аэропортов, а также систем водоснабжения и канализации. Он включает 65 миллиардов долларов на широкополосный доступ, в частности на улучшение интернет-услуг в сельской местности за счет государственных грантов.

Важное законодательство

Президент Байден назвал законопроект об инфраструктуре самым значительным достижением с момента создания системы межгосударственных автомагистралей в 1950-х годах; Белый дом также заявляет, что эти фонды будут создавать около 2 миллионов рабочих мест в год в течение следующих 10 лет, сообщает Associated Press.

«Двухпартийная сделка по инфраструктуре - это крупнейшая инвестиция в устойчивость физических и природных систем в американской истории», - говорится в информационном бюллетене по законопроекту, опубликованному в понедельник в Белом доме. «Сделка делает наши сообщества более безопасными, а нашу инфраструктуру - более устойчивой к воздействию изменения климата и кибератак».

«Инвестиции почти в 2 миллиарда долларов в защиту инфраструктуры от кибератак… являются хорошим шагом в правильном направлении, особенно в отношении государственных и местных органов власти, но в лучшем случае их следует рассматривать как первоначальный взнос», - говорит Скотт Шакелфорд, директор по кибербезопасности. и программа управления Интернетом в Университете Индианы.

Другие киберэксперты говорят, что подобное законодательство имеет решающее значение, поскольку США остаются уязвимыми для атак со стороны национальных государств. По словам Грегга Смита, председателя Ассоциации кибербезопасности Мэриленда, а также соучредителя и генерального директора фирмы Attila Security, наличие значительного притока федеральных долларов - «отличное начало» для «помощи правительственным областям» в их кибер-позиции.

«Остается целый ряд проблем, которые остаются без внимания: от защиты от программ-вымогателей и обновления планов реагирования на инциденты и политик конфиденциальности до местных тренингов по кибергигиене», - говорит Шакелфорд из IU. «Надеюсь, что по мере развертывания этих грантовых программ появятся возможности для использования надежных сетей и организаций… для расширения пула и обеспечения максимальной эффективности этих средств».

Об эффективном использовании выделенных средств Лиза Плаггемьер, временный исполнительный директор Национального альянса по кибербезопасности, говорит: «Мы должны убедиться, что деньги направляются на ориентированные на людей стратегии кибербезопасности, такие как обучение и повышение осведомленности, - а не только на технологическую сторону уравнение. В конце концов, большинство кибератак по-прежнему связано со значительными человеческими ошибками ".

Предоставление криптовалюты

Одним из спорных положений законопроекта является требование о налоговой отчетности за криптовалюту, которое расширяет определение тех, кто считается «брокером», включая такие стороны, как крипто-майнеры. Эта мера была добавлена к законопроекту в июле после того, как было подсчитано, что она может принести около 28 миллиардов долларов новых налоговых поступлений.

Положения о криптовалюте требуют, чтобы обо всех криптовалютных транзакциях на сумму свыше 10 000 долларов США сообщалось в IRS, и, несмотря на усилия группы сенаторов на одиннадцатом часу сузить определение термина «брокер», эта мера не изменилась.

Законопроект об инфраструктуре задерживался в Конгрессе в течение нескольких месяцев, поскольку демократы пытались связать законопроект об инфраструктуре с отдельным планом расходов на 1,75 триллиона долларов - законопроектом Build Back Better, который увеличит социальные расходы.

Этот законопроект обеспечит еще 500 миллионов долларов на финансирование кибербезопасности для CISA, в том числе 100 миллионов долларов на безопасность федеральных гражданских систем, 50 миллионов долларов на облачную безопасность, 50 миллионов долларов на системы управления производством и 20 миллионов долларов для правительств штатов, местных властей и племен.

Законопроект «Build Back Better» может подвергнуться тщательному рассмотрению в Сенате, где эксперты ожидают, что общая сумма законопроекта будет снижена после сопротивления умеренного сенатора-демократа Джо Манчина из Западной Вирджинии.

Консенсус по отчетности об инцидентах

В четверг несколько сенаторов объявили, что после согласования двух законопроектов об инцидентах, они намерены добавить 72-часовой механизм отчетности - и 24-часовое требование для жертв программ-вымогателей - в законопроект о расходах на оборону 2022 года, который необходимо принять.

Сенатор Петерс внес поправку в Закон о государственной обороне на 2022 год, согласно которой владельцы и операторы критически важной инфраструктуры, а также гражданские федеральные агентства должны сообщать в CISA, если они испытают кибератаку, и требуют от большинства организаций, включая предприятия, некоммерческие организации, а также правительства штатов и местных органов власти. - сообщить, если они совершили платеж с помощью программы-вымогателя.

Поправка получила поддержку сенаторов Роб Портмана, штат Огайо, и Сьюзан Коллинз, штат Вашингтон, а также Марка Уорнера, штат Вирджиния, председателя сенатского комитета по разведке, который в июле выступил соавтором аналогичного законопроекта, сужающего окно отчетности до 24 часов. Позже Уорнер сказал, что он стремился провести переговоры со своими коллегами из Сената и использовать NDAA в качестве потенциального средства для прохождения (см.: Сенаторы вносят федеральный закон об уведомлении о нарушениях).

«Эта двухпартийная поправка предпримет важные шаги для усиления защиты кибербезопасности», - говорится в заявлении Петерса. «И самое главное, (это) требует своевременного сообщения об этих атаках федеральному правительству, чтобы мы могли лучше предотвращать инциденты в будущем и привлекать злоумышленников к ответственности за их преступления». ***(Dan Gunderman. Infrastructure Bill Features $1.9 Billion in Cyber Funding // Information Security Media Group, Corp. (https://www.govinfosecurity.com/infrastructure-bill-features-19-billion-in-cyber-funding-a-17867). 08.11.2021).***

***

«Пентагон изложил предстоящие изменения в своей программе сертификации модели зрелости кибербезопасности с двумя новыми процессами нормотворчества.

Министерство обороны значительно сокращает программу, которую развернуло в прошлом году для проверки кибербезопасности своих поставщиков с помощью сторонних аудитов, и приостанавливает ее реализацию до тех пор, пока изменения не станут официальными.

Предполагалось, что программа будет реализована в течение пяти лет с конечной целью - потребовать от каждого оборонного подрядчика, располагающего определенной контролируемой, но несекретной информацией, получить сертификат от стороннего оценщика, подтверждающий их приверженность стандарту сертификации модели зрелости кибербезопасности.. Ряд программ Министерства обороны США были отобраны для пилотной программы в этом году. Теперь Пентагон заявляет, что стремится упростить программу - в CMMC 2.0 - и сделать ее более тесной для сотрудничества с промышленностью в двух новых нормах посредством Кодекса федеральных правил.

«До тех пор, пока изменения CMMC 2.0 не вступят в силу посредством процессов нормотворчества как в разделе 32 CFR, так и в разделе 48 CFR, департамент приостановит пилотные усилия CMMC и не утвердит включение требования CMMC в запросы Министерства обороны», - говорится в уведомлении, опубликованном Пятница в Федеральном реестре. «Требования программы CMMC 2.0 не будут обязательными до тех пор, пока нормотворчество в соответствии с разделом 32 CFR не будет завершено, а требования программы CMMC не будут включены по мере необходимости в правила приобретения через нормотворчество в соответствии с разделом 48».

В основе CMMC лежало утверждение должностных лиц Пентагона о том, что нынешняя система, позволяющая подрядчикам оборонной промышленности проводить самопроверку или просто заявлять о том, что они соблюдают стандарты кибербезопасности, установленные Национальным институтом стандартов и технологий, не работает. Официальные лица указали на продолжающееся воровство интеллектуальной собственности китайскими национальными государственными структурами в качестве главного индикатора. CMMC установила для подрядчиков пять уровней кибербезопасности в зависимости от важности данных, с которыми они будут работать.

Согласно уведомлению, CMMC 2.0 удалит второй и четвертый уровни, уменьшив модель до трех уровней. Всем подрядчикам первого уровня будет разрешено самостоятельно подтверждать свою кибербезопасность. В уведомлении говорилось, что подрядчики второго уровня - ранее третий уровень - будут «раздвоены» на приоритетные и неприоритетные приобретения, причем первый также сможет избежать независимой оценки третьей стороной. Правила для третьего и самого высокого уровня - ранее пятого - еще предстоит определить.

Новая модель также удалит дополнительные элементы управления, добавленные в рамках первоначальной программы, и будет полагаться только на элементы из специальной публикации NIST 800-171, давней основы для оценок кибербезопасности департамента. Изменения будут включать «удаление уникальных практик CMMC и всех процессов зрелости из модели CMMC», - говорится в уведомлении.

Еще одно важное изменение в CMMC 2.0 будет заключаться в принятии отделом плана действий и этапов - или PoAM, своего рода списка дел с указанием сроков - от подрядчиков. Бывший руководитель CMMC Кэти Аррингтон, в настоящее время находящаяся в отпуске, подавая иск на департамент по поводу предполагаемого неправильного обращения с секретной информацией, заявила, что PoAM не будут рассматриваться и что компании должны будут пройти сертификацию на требуемый уровень стандарта во время присуждения контракта.

Согласно уведомлению, в случае утверждения будет также действовать общий процесс отказа.

«CMMC 2.0 значительно укрепит кибербезопасность оборонно-промышленной базы», - заявил в четверг в пресс-релизе Джесси Салазар, заместитель помощника министра обороны по промышленной политике. «Устанавливая более тесные отношения сотрудничества с промышленностью, эти обновления будут поддерживать предприятия в принятии необходимых им практик

для предотвращения киберугроз, сводя к минимуму препятствия на пути соблюдения требований Министерства обороны».

Министерство обороны заявило, что изменения связаны с внутренним обзором программы, который начался в марте. Согласно сообщению, обзор был проведен Салазаром, заместителем помощника министра обороны по киберполитике Мике Эоян, исполнительным директором киберкомандования США Дэвидом Фредериком и заместителем главного информационного директора по кибербезопасности Дэвидом Маккеуном». ***(Mariam Baksh. DOD Suspends Cybersecurity Certification Program Pending Major Changes // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/dod-suspends-cybersecurity-certification-program-pending-major-changes/186639/). 04.11.2021).***

***

«Две трети респондентов сочли рекомендации Национального института стандартов и технологий «чрезвычайно» или «очень» ценными.

Поскольку администрация Байдена работает над укреплением партнерства государственного и частного секторов в области защиты данных, опрос показал, что большинство сотрудников, работающих в инфраструктуре кибербезопасности, хотят более активных действий на федеральном уровне для защиты данных и систем США.

В опросе, проведенном разработчиками программного обеспечения Tripwire и Dimensional Research, приняли участие 306 сотрудников, занимающихся информационными технологиями, как в частных компаниях, так и в государственных учреждениях. Около трети респондентов работают непосредственно в федеральном правительстве, в то время как другие сообщили, что работают в производственных секторах, а также в энергетической и технологической отраслях.

Большинство задаваемых вопросов касалось стандартов, рекомендованных Национальным институтом стандартов и технологий, а также того, внедряются ли они на бесчисленном количестве рабочих мест и отраслей.

В общей сложности 66% всех респондентов сочли рекомендации NIST, касающиеся онлайн-безопасности, «чрезвычайно» или «очень» ценными, независимо от того, как компания или организация их внедряют.

Несмотря на широкое позитивное восприятие стандартов NIST, только половина частных и неправительственных организаций сообщили о принятии руководящих принципов агентства по кибербезопасности в полном объеме. Между тем 82% респондентов заявили, что федеральному правительству следует принять более решительные меры для обеспечения того, чтобы частные компании выполняли эти руководящие принципы, либо путем усиления рекомендаций, либо путем обеспечения соблюдения стандартов за пределами федеральных агентств.

«Ясно, что организации - как государственный, так и частный - ищут дальнейших указаний со стороны федерального правительства», - заявил Тим Эрлин, вице-президент по стратегии Tripwire. «Как правило, долгосрочное обеспечение соблюдения и реализация политики кибербезопасности требует времени, но важно, чтобы агентства разработали план и оценили выполнение этого плана для защиты нашей критически важной инфраструктуры и не только».

Профедеральная философия правоприменения разделилась на работников государственного и частного секторов. Отвечая на вопрос о применении стандартов NIST федеральным правительством, 43% сотрудников федеральной службы безопасности ответили, что государственные системы лучше справляются с проблемами безопасности, в то время как 46% нефедеральных организаций ответили, что государственные органы обычно хуже справляются с управлением данными и данными. сетевая безопасность.

Для сотрудников государственных и негосударственных структур ключевой компонент поддержания строгих практик и протоколов кибербезопасности был разным. Как федеральные, так и нефедеральные служащие чувствовали, что их организация отстает в принятии рекомендаций NIST из-за нехватки внутренних ресурсов и опыта. Другие нефедеральные служащие также добавили, что низкий уровень внедрения кибербезопасности объясняется отсутствием риска в их отрасли.

Для обоих секторов программы-вымогатели были самой большой проблемой с точки зрения киберугроз и взломов: 53% всех респондентов указали это в качестве своей основной проблемы. На втором месте по значимости стояли другие уязвимости». ***(Alexandra Kelley. Most Employees Want Stronger Enforcement of Cybersecurity Protocols in the Workplace, Survey Finds // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/most-employees-want-stronger-enforcement-cybersecurity-protocols-workplace-survey-finds/186839/). 15.11.2021).***

***

«В недавнем отчете MITER излагаются восемь способов, которыми федеральное правительство может улучшить привычки кибербезопасности во всех агентствах, опираясь на усиление финансирования и надзора со стороны Конгресса.

Согласно недавнему исследованию, Конгрессу следует принять оценочную карту для измерения прогресса агентств по внедрению передовых практик кибербезопасности в качестве одного из способов улучшения общей позиции правительства.

Предоставленные исследователями в MITER, белая бумага, раскладывает восемь рекомендаций для федерального правительства, чтобы улучшить гигиену кибербезопасности и инфраструктуры безопасности для предотвращения вредоносных программ и атак вымогателей. Они также отмечают, что последнее крупное законодательное обновление практики кибербезопасности в рамках федерального правительства произошло с принятием Федерального закона о модернизации информационной безопасности 2014 года.

«Необходимы обновления законов, регулирующих федеральную кибербезопасность, чтобы привести их в соответствие с текущими передовыми практиками кибербезопасности, сократить расходы на аудиты и отчеты, а также прояснить роли и обязанности многих вовлеченных федеральных игроков», - говорится в документе.

Одна из восьми рекомендаций советует использовать Федеральный закон о реформе закупок информационных технологий в качестве руководства для надзора Конгресса за кибербезопасностью и отчетности. FITARA, принятая в 2014 году,

обеспечивает основу для закупки компьютерных технологий государственными учреждениями.

Исследователи говорят, что показатели оценки FITARA обеспечивают прозрачность усилий федеральных агентств по модернизации ИТ, которые должны быть воспроизведены на надзорных слушаниях Конгресса, направленных на оценку практики кибербезопасности.

«Система показателей кибербезопасности в стиле FITARA может быть предметом надзорных слушаний Конгресса, на которых руководители исполнительной власти и агентств могут свидетельствовать о своем прогрессе и о тех областях, где необходимы улучшения и дополнительная поддержка Конгресса», - говорится в документе. «Эту модель отчетности также можно использовать для оптимизации обширных агентств по отчетности, которые в настоящее время готовят для Конгресса, GAO и сообщества IG».

В документе также содержится призыв к конкретной модернизации системы защиты Агентства по кибербезопасности и безопасности инфраструктуры. Исследователи пишут, что нынешние системы киберзащиты CISA были разработаны для того времени, когда большинство агентских систем эксплуатировались внутри компании с ограниченным незашифрованным внешним трафиком.

С появлением и внедрением большего количества облачных вычислений требуется больше программного обеспечения с нулевым доверием для защиты конфиденциальных данных. Один из способов, которым авторы рекомендуют поддержать эту инициативу, - это увеличение финансирования Конгрессом США оборонных сетей CISA.

«Действия Конгресса могут помочь гарантировать, что федеральное правительство будет способно противостоять текущим и возникающим угрозам и будет управляться в соответствии с передовой современной практикой», - заключает документ. «Восемь рекомендаций в этом документе предоставляют Конгрессу варианты, которые будут поддерживать усилия по повышению кибербезопасности федеральных агентств, делая процесс надзора более эффективным и действенным».

Остальные рекомендации включают наделение федерального руководства кибербезопасностью более широкими полномочиями по надзору, модернизацию устаревших ИТ-систем, создание новых рамок киберрисков, поддержку инфраструктуры нулевого доверия в федеральных агентствах, обновление и управление рисками цепочки поставок, а также требование о том, чтобы методы кибербезопасности были межведомственными. приоритет в администрации Байдена.

На прошлой неделе документ был отправлен в несколько комитетов Конгресса вместе с федеральным директором по информационной безопасности Крисом ДеРуша». ***(Alexandra Kelley. Researchers Push FITARA-Like Scorecard for Cybersecurity // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/researchers-push-fitara-scorecard-cybersecurity/186532/). 01.11.2021).***

***

«Министерство внутренней безопасности США, ключевое агентство по кибербезопасности, только что объявило о новой системе, которая поможет ему

нанимать, развивать и переобучать профессионалов в области кибербезопасности в федеральном правительстве.

Новая система найма DHS, получившая название Система управления талантами в кибербезопасности (CTMS), запускается в условиях ограниченного рынка труда для профессионалов в области кибербезопасности, которые пользуются чрезвычайно высоким спросом и поэтому могут получать большие зарплаты.

DHS - это всего лишь одно федеральное ведомство, но оно играет особую роль в реагировании на крупные кибератаки на критически важную инфраструктуру США. Он надеется, что новая система поможет ему в поиске и сохранении талантов для выполнения критически важных ролей с целью найма 150 приоритетных ролей в течение 2022 года.

«CTMS позволит DHS заполнить критически важные позиции в области кибербезопасности путем отбора кандидатов на основе продемонстрированных компетенций, конкурентной компенсации сотрудников и сокращения времени, необходимого для приема на работу в отдел», - говорится в сообщении.

Первыми ролями, которые будут заполнены с помощью CTMS, будут «высокоприоритетные» должности в CISA и офисе главного информационного директора DHS. Затем в 2022 году вакансии в Службе кибербезопасности DHS будут доступны в нескольких агентствах DHS с миссией кибербезопасности, сообщает DHS.

Диапазон заработной платы CTMS имеет верхний предел зарплаты вице-президента (255 800 долларов в 2021 году), а также расширенный диапазон для использования в ограниченных обстоятельствах, который имеет верхний предел в 332 100 долларов в 2021 году.

В настоящее время DHS набирает сотрудников для выполнения различных ролей в сфере кибербезопасности, включая реагирование на инциденты, анализ рисков, обнаружение и оценку уязвимостей, разведку и расследование, сетевых и системных инженеров, криминалистику и обеспечение безопасности программного обеспечения.

CTMS «в корне меняет представление о том, как Департамент нанимает, развивает и удерживает высокопоставленных и разнообразных специалистов в области кибербезопасности», - говорит министр внутренней безопасности Алехандро Н. Майоркас.

«Поскольку наша страна продолжает сталкиваться с растущим ландшафтом угроз, мы не можем полагаться только на традиционные инструменты найма для заполнения критически важных вакансий. Эта новая система позволит нашему отделу лучше конкурировать за специалистов по кибербезопасности и оставаться достаточно гибкими, чтобы соответствовать требованиям наших критическая миссия кибербезопасности ".

Администрация Байдена-Харриса сделала кибербезопасность приоритетом на раннем этапе, например, назначив первого заместителя советника США по национальной безопасности по кибербезопасности Анну Нойбергер, которая вела федеральное расследование атак SolarWinds и Exchange.

DHS, в частности его Агентство по кибербезопасности и безопасности инфраструктуры (CISA), также получила повышенную роль в области

кибербезопасности в соответствии с указом Байдена о кибербезопасности». ***(Liam Tung. The US government just launched a big push to fill cybersecurity jobs, with salaries to match // ZDNet (https://www.zdnet.com/article/the-us-government-just-launched-a-big-push-to-fill-cybersecurity-jobs-with-salaries-to-match/). 16.11.2021).***

***

«Нет никаких сомнений в том, что в настоящее время области космоса и киберпространства оспариваются антагонистическим поведением по всему миру.

Соседние противники уже стратегически определили их как предпочтительные области действий как в соревновании, так и в конфликте. Кибернетические атаки на цепочки поставок все чаще и чаще используются во всем мире в качестве тактики гибридной войны для получения преимуществ. Как и следовало ожидать, они предоставляют противникам относительно рентабельные средства взаимодействия, правдоподобного отрицания и избегают политической реакции, которая неизбежно возникает в результате смертельных действий и физического вторжения. Принимая во внимание то внимание, которое уделяется этим областям, американские космические, оборонные и разведывательные сообщества должны сосредоточить усилия на защите космических ресурсов, сохранении стратегических и военных преимуществ и укреплении национальной безопасности и глобальной стабильности. Кибербезопасность и целостность цепочки поставок должны стать неотъемлемой и серьезной проблемой для космического сообщества.

В 2007 году Китай потряс мир, когда он сбил один из своих стареющих метеорологических спутников в ходе испытания противоспутниковой ракеты, что привело космическое сообщество планеты к окончательному осознанию этого. С того момента космическая область уже не могла считаться благоприятной, а скорее спорной ареной. С тех пор космическое сообщество стало свидетелем других агрессивных действий, таких как российские спутники-«инспекторы», совершающие маневры вокруг секретных объектов, принадлежащих США, в 2020 году. Публично признав это плохое поведение, генерал космических сил США Джон Реймонд, начальник космической службы операции, нарушившие традиционную практику космического сообщества, чтобы хранить молчание в интересах защиты возможностей США. Эта прозрачность ценна для широкой общественности,

Китай делает серьезный стратегический упор на наступательное пространство и продвижение в контркосмическом пространстве. В 2015 году Китай создал новую силу в составе Народно-освободительной армии (НОАК), известную как Силы стратегической поддержки, объединив информационные операции НОАК в космосе и контркосмосе, кибернетической войне, электромагнитной войне и психологических операциях, чтобы обеспечить военное преимущество в информационных конфликтах. Точно так же информационная конфронтация вызывается во множестве российских стратегических документов, включая Политику национальной безопасности 2015 года и Концептуальные взгляды 2016 года на деятельность вооруженных сил в информационном пространстве. Стратегия России включает не только кибератиность, но также радиоэлектронную борьбу и

психологические операции. В то время как космос играет менее явную роль в российской стратегии информационного противостояния, снижение точности, возможности навигации и синхронизации рассматриваются как важнейшее информационное оружие. Это отражает мнение российского руководства о том, что космос - это во многом сфера боевых действий. В отличие от Китая, России не хватает ресурсов для освоения космоса, что требует сосредоточенного внимания на наступательных возможностях против космических средств и наземной космической инфраструктуры. Именно здесь возникают кибер-атаки на цепочки поставок.

Космическая область очень восприимчива к атакам с использованием кибер-цепочек поставок из-за уникальности, долговечности и коммерциализации космической цепочки поставок. США полагаются как на союзников, так и на конкурирующие страны в отношении критически важных редкоземельных материалов, что представляет собой уязвимость в отслеживании и непрерывности цепочки поставок. Точно так же многие космические объекты, находящиеся сегодня на орбите, были спроектированы и построены годы, если не десятилетия назад; не все унаследованные компоненты были разработаны с учетом современных технологий и угроз. Наконец, быстрая коммерциализация космоса расширила поверхность атаки угроз. Частные промышленные предприятия и готовые коммерческие продукты все чаще используются для удовлетворения требований, поскольку они имеют финансовую и стратегическую ценность. Промышленность вводит новшества и производит более быстро и с меньшими затратами, чем правительство. Учитывая текущие ограничения ресурсов, из-за компактности новых космических сил США и стремления к гибкости и быстрому приобретению коммерческая зависимость, вероятно, возрастет. Увеличение числа поставщиков, предоставляющих данные, программное обеспечение, оборудование и услуги в этой среде, предоставляет противникам множество возможностей с каскадными эффектами, что подчеркивает важность немедленного повышения кибергигиены и управления рисками цепочки поставок (SCRM).

Чтобы защитить интересы США в космосе, должна произойти смена парадигмы, которая не только охватит кибербезопасность и управление рисками цепочки поставок, но и подчеркнет их важность для миссии.

Во-первых, управление рисками кибербезопасности и цепочки поставок должно быть полностью интегрировано - не только при проектировании, строительстве и эксплуатации космических объектов и программ, но и друг с другом. Этого можно добиться с помощью комбинации средств:

Преднамеренный учет угроз кибербезопасности и цепочки поставок при разработке и реализации стратегии;

Оценка и пересмотр организационных структур;

Включение приоритетов кибербезопасности и целостности цепочки поставок в показатели эффективности и результативности; созревание функций и процессов управления рисками предприятия;

Ускоренное развитие механизмов обмена информацией.

Выполнение некоторой комбинации этих действий изменит роль кибербезопасности и управления рисками цепочки поставок как неотъемлемых частей миссии.

Во-вторых, США должны стремиться к устойчивости, как будто от этого зависит будущее. Устойчивость может иметь несколько форм: техническую, миссионерскую или организационную. Диверсификация сырья и поставщиков, избыточность космических компонентов и активов (например, микроспутников), а также быстрое приобретение и продвижение спутников классов B, C и D с более коротким сроком службы - все это поддерживает более устойчивую позицию. Но это также касается организационной культуры. Космическое сообщество должно избегать избегающей риска и защитной изоляции прошлого в пользу подхода, который учитывает ценность неудач, конструктивно привлекает партнеров и критически склоняется к риску. В этой связи тот факт, что космическое сообщество в настоящее время переживает значительный переходный период, открывает новые возможности. Как новые организации, бизнес-процессы, и установлены международные нормы, это идеальное время для значимого управления изменениями, побуждающего сообщество принять как устойчивость, так и риски. Более того, это дает возможность попробовать что-то новое, например, определить сотрудника по устойчивости для крупных программ или даже, возможно, создать должность для главного сотрудника по устойчивости в высшем эшелоне организации.

В-третьих, космическое сообщество должно создавать и расширять общеорганизационные программы управления рисками цепочки поставок. Традиционный акцент на крупных приобретениях должен быть перенесен на все критически важные приобретения, включая программное обеспечение и данные. Проверка продавцов первого уровня больше не достаточна; освещение всей цепочки поставок должно требоваться и проверяться по контракту. Точно так же целостность цепочки поставок должна быть приоритетом на протяжении всего жизненного цикла любого критически важного приобретения, а не только до заключения контракта. (Следует отметить, что искусственный интеллект и машинное обучение могут многое предложить в плане непрерывного мониторинга). Несмотря на то, что за последние несколько лет были достигнуты значительные успехи в обеспечении поддержки нескольких общеорганизационных программ, существует внешнее давление со стороны Руководящих принципов консолидированной разведки и Федерального закона о модернизации информационной безопасности для быстрого созревания. Более того, по мере того, как рабочая сила знакомится с этими программами, операционный спрос будет расти. Соответственно, приоритетные бюджетные программы и программы выбора правильного размера на будущее должны стать ключевыми целями для высшего руководства.

Наконец, сотрудничество имеет первостепенное значение. Организационные границы и узкие программные каналы вызывают фрагментацию космического сообщества. Хотя эти организационные границы, вероятно, возникли из желания защитить конфиденциальную правительственную информацию, эти организационные границы пагубно кальцинировались, предоставляя современным противникам уязвимые места. Чтобы освободиться от этого шаблона и своевременно

обмениваться разведданными об угрозах и передовым опытом для продвижения нашей коллективной защиты, космическое сообщество должно делать упор на целенаправленное сотрудничество. Инвестирование во внутриправительственные и государственно-частные технологии, предоставление совместных межведомственных обязанностей, посвященных кибербезопасности и целостности цепочки поставок, стандартизация таксономии и уточнение ролей и обязанностей, значительно улучшили бы прозрачность и понимание уязвимостей и угроз, снизить затраты на национальную безопасность из-за беспорядочной передачи информации и наладить значимое взаимодействие с заинтересованными сторонами. Одним из примеров этого может быть Национальный центр разведки цепочки поставок, к которому призывает Консультативный совет национальной безопасности, Комиссия по киберпространству солярия и корпорация MITER. Независимо от механизма, срочно требуется конструктивное и организованное сотрудничество, чтобы закрыть уязвимые швы и стимулировать столь необходимый обмен информацией.

Интегрированная кибербезопасность и целостность цепочки поставок необходимы для сохранения господства США в космосе. Наши противники хорошо осведомлены о существующих слабостях и будут продолжать их использовать. Атаки на космические объекты с помощью кибернетических цепочек поставок являются частью их стратегии, направленной на получение экономического, военного и стратегического преимущества в будущем. Чтобы противостоять размаху и скорости этой угрозы, правительственные и коммерческие космические организации должны действовать быстро, чтобы интегрировать и повысить уровень кибербезопасности и управления рисками цепочки поставок в космическую стратегию, проектирование, строительство и эксплуатацию; сделать упор на отказоустойчивость; зрелые программы управления рисками цепочки поставок; и сотрудничать с намерением». ***(Dan Lewis, Megan Moloney and Nicole Ussery. Op-ed | SOS Space: Why cybersecurity and supply chain risk management must go hand in hand // SpaceNews (https://spacenews.com/op-ed-sos-space-why-cybersecurity-and-supply-chain-risk-management-must-go-hand-in-hand/). 16.11.2021).***

***

«Поскольку 2021 год, как ожидается, станет худшим годом в истории для кибератак, Совет по стратегии CIO опубликовал новый стандарт, который поможет малым предприятиям защитить свои системы от злоумышленников.

Новый стандарт, поддерживаемый Советом по стандартам Канады (SCC), станет частью требований CyberSecure Canada, программы добровольной сертификации, учрежденной Инновациями, наукой и экономическим развитием (ISED) и Службой безопасности связи (CSE), чтобы помочь МСП достигают разумного уровня кибербезопасности.

Написанный для неопытных пользователей, стандарт включает инструкции и готовые шаблоны, которые помогут малым и средним предприятиям (МСП) улучшить свои средства контроля кибербезопасности. Стандарт основан на опыте CSE (Базовые меры кибербезопасности для малых и средних организаций), а также на международных стандартах, таких как Управление информационной безопасностью ISO (ISO / IEC 27001)…» ***(New standard brings clarity on cybersecurity***

to SMEs // GlobeNewswire, Inc. (https://www.globenewswire.com/news-release/2021/11/24/2340693/0/en/New-standard-brings-clarity-on-cybersecurity-to-SMEs.html). 24.11.2021).

***

«Отчет, в котором представлены некоторые из ведущих оборонных подрядчиков США, показывает, что около 20% из них «очень восприимчивы» к атакам программ-вымогателей, при этом 42% испытали утечку данных только в 2020 году.

Эти данные получены от компании Black Kite, занимающейся исследованиями в области кибербезопасности. Авторы отчета изучили подрядчиков оборонного сектора, работающих в сфере финансовых услуг, здравоохранения, производства, критически важной инфраструктуры и бизнес-услуг, и оценили каждую компанию на предмет их протоколов и процедур кибербезопасности, чтобы определить отраслевой индекс среди подрядчиков оборонной промышленности.

Средний балл подразумевает безопасный уровень управления рисками - и 54% подрядчиков защиты считаются относительно безопасными от атак программ-вымогателей. Однако было обнаружено, что 43% подрядчиков имеют старые или устаревшие системы кибербезопасности, что повышает риск кибератак.

«Киберпреступники чаще, чем когда-либо, атакуют критически важную инфраструктуру, и каждая атака оказывает более сильное воздействие на нашу национальную безопасность. Тенденции, которые мы наблюдаем в наших результатах RSI, вызывают тревогу», - сказал в пресс-релизе директор Black Kite Боб Мейли. «Когда организации постоянно отслеживают состояние своих киберрисков, они получают подробную информацию для защиты своих наиболее важных активов и средств контроля».

В отчете также подчеркивается, что некоторые отрасли, а именно производственный сектор, особенно часто становятся объектами атак хакеров.

Авторы также добавили, что низкий индекс риска, который означает, что компания защищена от хакеров, не гарантирует иммунитета к программам-вымогателям.

В отчете рекомендуется, чтобы понимание рисков цепочки поставок и постоянная бдительность в отношении состояния кибербезопасности компании имели решающее значение для предотвращения взломов. Он также выступает за обмен информацией между компаниями государственного и частного секторов, которые подвергаются кибератакам, что является опорой в борьбе администрации Байдена за предотвращение крупномасштабных атак с использованием программ-вымогателей.

«Правительство будет нести ответственность за установление приоритета сотрудничества при поддержке кибер-ориентированных организаций, которые понимают точки концентрированного риска в сегодняшних цифровых цепочках поставок», - говорится в отчете». ***(Alexandra Kelley. Report: 20% of Defense Contractors at Risk for Ransomware Attack // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/survey-20-defense-contractors-risk-ransomware-attack/186887/). 17.11.2021).***

***

«Организации из разных секторов должны начать подготовку к изменениям в правилах кибербезопасности, содержащихся в Законе о безопасности критической инфраструктуры 2018 (Cth). Недавние инциденты, такие как закрытие колониального трубопровода США, указывают на то, что критически важные объекты инфраструктуры являются уязвимой и привлекательной целью для кибератак, особенно с учетом того, что угрозы для таких активов развиваются в мире после COVID. Чтобы устранить эту потенциальную уязвимость, 22 ноября 2021 года правительство приняло Закон о поправках к законодательству о безопасности (критическая инфраструктура) 2021 года (законопроект), который вносит поправки в Закон о безопасности критически важной инфраструктуры 2018 (Cth) (Закон о SOCI).), чтобы наложить различные обязательства по кибербезопасности на организации, ответственные за активы критически важной инфраструктуры. Поправки применяются в различных организациях, которые принадлежат к разным секторам, включая секторы связи и хранения или обработки данных.

Поправки к Закону о SOCI в этом транше (с учетом того, что следующий транш, обсуждаемый ниже, как ожидается, будет введен позже) вводят следующее:

обязательная отчетность о киберинцидентах; а также

расширенные правительственные полномочия в отношении организаций, ответственных за активы критически важного сектора инфраструктуры, в ответ на серьезные кибератаки, затрагивающие такие активы.

Важно отметить, что правила, которые еще не опубликованы, будут действовать как переключатели `` включено " / `` выключено " для различных обязательств, изложенных в Законе о SOCI, например, при условии, что определенные активы не являются критически важными активами инфраструктуры или что определенные обязательства не применяются к определенным секторам / активам.

На кого распространяются обязательства?

Эти обязательства будут применяться к организациям, ответственным за критически важные объекты инфраструктуры в следующих:

хранение или обработка данных;

коммуникации;

защита;

энергия;

финансовые услуги и рынки;

еда и бакалея;

здравоохранение и медицина;

высшее образование и исследования;

космическая техника;

транспорт; а также

вода и канализация.

Расширенные правительственные полномочия также будут применяться к организациям, которые являются прямыми держателями акций, операторами или поставщиками управляемых услуг в отношении таких активов.

Что включают в себя обязательства?

Обязательное сообщение о киберинцидентах

В соответствии с реформированным режимом, если Ответственное лицо узнает, что происходит или произошел инцидент кибербезопасности, который повлияет на доступность соответствующего актива, ответственное лицо должно уведомить соответствующий регулирующий орган (это должно быть указано в правилах или в противном случае - Австралийское управление связи). Информация, которая будет включена в такой отчет, также будет детализирована в следующих правилах. Отсутствие уведомления приведет к наложению штрафа в размере 50 штрафных единиц, который на дату этой статьи составляет 11 100 долларов США.

Уведомление должно происходить в течение:

12 часов (при значительном влиянии на актив); или

72 часа (когда есть влияние на актив, но оно не является «значительным»).

В этом контексте «значительный» относится к ситуации, когда актив используется в связи с предоставлением основных товаров или услуг, и доступность таких товаров или услуг была существенно нарушена, или такие другие обстоятельства, которые должны определяться правилами.

Расширенные государственные полномочия

В соответствии с Законом SOCI с внесенными в него поправками регулирующие органы также будут иметь расширенные полномочия в случае возникновения или возникновения инцидента кибербезопасности, который может повлиять на критически важный объект инфраструктуры.

В таких обстоятельствах и где:

существует существенный риск того, что инцидент нанесет серьезный ущерб социальной или экономической стабильности, обороне или национальной безопасности Австралии; а также

никакая другая существующая австралийская регулирующая система не может быть использована для обеспечения эффективного реагирования на инцидент, соответствующий министр может (при определенных обстоятельствах) санкционировать выдачу юридическому лицу следующих документов:

инструкции по сбору информации, которые требуют от организации предоставлять информацию секретарю;

указания к действию, которые требуют от организации выполнить или воздержаться от выполнения определенного действия или вещи; а также

Запросы на вмешательство: которые требуют от Австралийского управления сигналов выполнения одного или нескольких указанных действий или действий (таких как доступ или изменение компьютера, анализ компьютера, его программ или данных, доступ, восстановление, копирование, изменение или удаление данных, изменение компьютера функционирование, или удалить, отключить или подключить компьютер) по отношению к активу.

Мы отмечаем, что указания о действиях и запросы на вмешательство должны быть соразмерными, разумно необходимыми и технически выполнимыми, а также

подлежать другим ограничениям, например, они должны выдаваться только в том случае, если организация не желает или не может предпринять все разумные шаги для реагирования на инцидент.

Когда возникнут обязательства?

Оба обязательства возникают, когда Билл получает королевское одобрение. Нет установленного периода времени, в течение которого будет получено такое согласие.

Что дальше?

Позднее правительство планирует также ввести следующее (которые были исключены из принятой версии законопроекта):

обязательные программы управления рисками критической инфраструктуры;

повышенные обязательства по кибербезопасности для определенных организаций; а также

обозначения систем государственного значения, к которым будут применяться более строгие обязательства». ***(Sophie Dawson, Julie Cheeseman, Joel Parsons, James Hoy, Jessica Laverty, Emma Croft. Reforms to the Security of Critical Infrastructure Act 2018 (Cth) passed // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/australia/reforms-to-the-security-of-critical-infrastructure-act-2018-cth-passed). 24.11.2021).***

***

«Министерство внутренней безопасности США, ключевое агентство по кибербезопасности, только что объявило о новой системе, которая поможет ему нанимать, развивать и переобучать профессионалов в области кибербезопасности в федеральном правительстве.

Новая система найма DHS, получившая название Система управления талантами в кибербезопасности (CTMS), запускается в условиях ограниченного рынка труда для профессионалов в области кибербезопасности, которые пользуются чрезвычайно высоким спросом и поэтому могут получать большие зарплаты.

DHS — это всего лишь одно федеральное ведомство, но оно играет особую роль в реагировании на крупные кибератаки на критически важную инфраструктуру США. Он надеется, что новая система поможет ему в поиске и сохранении талантов для выполнения критически важных ролей с целью найма 150 приоритетных ролей в течение 2022 года.

«CTMS позволит DHS заполнить критически важные позиции в области кибербезопасности путем отбора кандидатов на основе продемонстрированных компетенций, конкурентной компенсации сотрудников и сокращения времени, необходимого для приема на работу в отдел», - говорится в сообщении.

Первыми ролями, которые будут заполнены с помощью CTMS, будут «высокоприоритетные» должности в CISA и офисе главного информационного директора DHS. Затем в 2022 году вакансии в Службе кибербезопасности DHS будут доступны в нескольких агентствах DHS с миссией кибербезопасности, сообщает DHS.

Диапазон заработной платы CTMS имеет верхний предел зарплаты вице-президента (255 800 долларов в 2021 году), а также расширенный диапазон для

использования в ограниченных обстоятельствах, который имеет верхний предел в 332 100 долларов в 2021 году.

В настоящее время DHS набирает сотрудников для выполнения различных ролей в сфере кибербезопасности, включая реагирование на инциденты, анализ рисков, обнаружение и оценку уязвимостей, разведку и расследование, сетевых и системных инженеров, криминалистику и обеспечение безопасности программного обеспечения.

CTMS «в корне меняет представление о том, как Департамент нанимает, развивает и удерживает высокопоставленных и разнообразных специалистов в области кибербезопасности», - говорит министр внутренней безопасности Алехандро Н. Майоркас.

«Поскольку наша страна продолжает сталкиваться с растущим ландшафтом угроз, мы не можем полагаться только на традиционные инструменты найма для заполнения критически важных вакансий. Эта новая система позволит нашему отделу лучше конкурировать за специалистов по кибербезопасности и оставаться достаточно гибкими, чтобы отвечать требованиям наших критическая миссия кибербезопасности ".

Администрация Байдена-Харриса на раннем этапе сделала кибербезопасность приоритетом, например, назначив первого заместителя советника США по национальной безопасности по кибербезопасности Анну Нойбергер, которая вела федеральное расследование атак SolarWinds и Exchange.

DHS, в частности его Агентство по кибербезопасности и безопасности инфраструктуры (CISA), также получила повышенную роль в области кибербезопасности в соответствии с указом Байдена о кибербезопасности». ***(Liam Tung. The US government just launched a big push to fill cybersecurity jobs, with salaries to match // ZDNet (https://www.zdnet.com/article/the-us-government-just-launched-a-big-push-to-fill-cybersecurity-jobs-with-salaries-to-match/). 16.11.2021).***

***

«Прошлая неделя была напряженной для кибернетической среды. Правительство опубликовало свой ответ как на его призыв высказать мнение о безопасности цифровых цепочек поставок, так и на предлагаемые изменения в правилах NIS. На той же неделе NCSC опубликовал свой годовой отчет. Риск цепочки поставок является ключевой проблемой для многих организаций и присутствует во всех трех из них.

Новые правила для цифровых цепочек поставок?

15 ноября правительство ответило на его призыв высказать мнение о рисках кибербезопасности цепочки поставок. Призыв к мнениям направлен на получение обратной связи по следующим вопросам:

как организации в настоящее время управляют рисками цепочки поставок и какая дополнительная государственная поддержка позволит им делать это более эффективно: отзывы подтвердили, что ключевые препятствия на пути эффективного управления рисками кибербезопасности цепочки поставок варьируются от низкого уровня признания риска и ограниченной видимости в цепочках поставок до недостаточного инструменты для оценки риска и ограничений на действия из-за

структурного дисбаланса. Многие респонденты также упомянули, что в настоящее время они используют Руководство NCSC по безопасности цепочки поставок и Вопросы по обеспечению поставщиков; а также предложенная структура для обеспечения безопасности поставщика управляемых услуг (MSP): респонденты на запрос мнений подчеркнули важность MSP и зависимость от группы наиболее важных MSP, которые несут уровень риска, которым необходимо управлять проактивно. Они также отметили сложность доступа к информации о кибербезопасности MSP. Большинство считает, что принципы системы оценки кибер-оценки NCSC применимы к киберустойчивости поставщиков услуг мобильной связи, предполагая, что эти принципы следует учитывать при установлении базовых показателей безопасности или структуры гарантий в будущем.

Респонденты также положительно отзывались о других предложениях, например, об образовании, сертификационных и контрольных знаках, международном сотрудничестве и минимальных требованиях в сфере государственных закупок. Правительство подтвердило, что в рамках предстоящей Национальной киберстратегии (ожидается в конце этого года) оно продолжит работу с промышленностью по разработке набора политических решений для повышения киберустойчивости цифровых решений, и его работа будет включать «законодательную работу для обеспечения что [MSP] принимают разумные и соразмерные меры кибербезопасности».

Обновление NIS

17 ноября правительство ответило на его призыв высказывать мнения о внесении поправок в Правила безопасности сетей и информационных систем. Правила NIS налагают обязательства по безопасности и уведомлению об инцидентах на операторов основных услуг или OES (в таких секторах, как здравоохранение и энергетика) и соответствующих поставщиков цифровых услуг или DSP (онлайн-поисковые системы, онлайн-рынки и услуги облачных вычислений). В настоящее время пороги уведомления об инцидентах для OES устанавливаются соответствующими отраслевыми регулирующими органами, тогда как пороговые значения для DSP устанавливаются законодательством. Эти пороги DSP больше не подходят по назначению. Они были установлены на уровне, который считается подходящим для рынка ЕС и не подходит после Брексита, учитывая меньший рынок Великобритании. В июле, Правительство опубликовало призыв высказаться по поводу своего предложения о переносе пороговых значений отчетности для DSP из законодательства в руководство ICO (ICO является соответствующим регулятором в этой сфере). Ответы на предложение были в целом положительными или нейтральными, и правительство подтвердило, что «твердо верит, что предлагаемые изменения… сохранят и повысят эффективность законодательства NIS в защите безопасности сети и информационных систем для поставщиков цифровых услуг». Следующие шаги будут опубликованы «в должное время». Хотя эта разработка явно ориентирована на DSP, она представляет интерес для всех организаций, пользующихся их услугами. и Правительство подтвердило, что оно «твердо верит, что предлагаемые изменения… сохранят и повысят эффективность законодательства NIS в защите безопасности сети и информационных систем для поставщиков

цифровых услуг». Следующие шаги будут опубликованы «в должное время». Хотя эта разработка явно ориентирована на DSP, она представляет интерес для всех организаций, пользующихся их услугами. и Правительство подтвердило, что оно «твердо верит, что предлагаемые изменения… сохранят и повысят эффективность законодательства NIS в защите безопасности сети и информационных систем для поставщиков цифровых услуг». Следующие шаги будут опубликованы «в должное время». Хотя эта разработка явно ориентирована на DSP, она представляет интерес для всех организаций, пользующихся их услугами.

Годовой обзор NCSC

Наконец, 17 ноября NCSC начал свой пятый ежегодный обзор. В нем подчеркивается работа, проделанная NCSC в связи с пандемией, с учетом того, что сектор здравоохранения сфокусирован на многих атаках, и выделены программы-вымогатели и цепочка поставок как два основных киберриска, с которыми в настоящее время сталкиваются организации. Генеральный директор NCSC Линди Кэмерон охарактеризовала программы-вымогатели как «самую непосредственную угрозу кибербезопасности для британских предприятий, которая… должно быть выше в повестке дня совета директоров». В обзоре также обсуждались ресурсы, предлагаемые NCSC, и поддержка, которую он оказал 777 значительным инцидентам (по сравнению с 723 в предыдущем году)». ***(Natalie Donovan. A busy week for cyber: new rules for digital service providers and supply chains? // Slaughter and May (https://thelens.slaughterandmay.com/post/102hc03/a-busy-week-for-cyber-new-rules-for-digital-service-providers-and-supply-chains). 22.11.2021).***

***

Країни ЄС та Великобританія

«28 октября 2021 года Комитет Европейского парламента по промышленности, исследованиям и энергетике принял проект директивы о кибербезопасности («Директива NIS2»). Директива NIS2 расширит сферу действия существующей Директивы NIS и будет применяться к «важным секторам», таким как управление отходами, почтовые услуги, химикаты, продукты питания, производители медицинских устройств, поставщиков цифровых услуг и производителей электроники, в дополнение к «основным секторам». Директива NIS2 устанавливает особые требования к кибербезопасности, связанные с реагированием на инциденты, безопасностью цепочки поставок, шифрованием и обязательствами по раскрытию уязвимостей. Директива NIS2 также направлена на улучшение сотрудничества и обмена информацией между государствами-членами ЕС, а также на создание общей европейской базы данных уязвимости.

Комитет объявит свой отчет по законопроекту на пленарном заседании 10 ноября, после чего начнутся переговоры с Европейским советом». ***(European Parliament Adopts Draft Cybersecurity Directive // Hunton Andrews Kurth LLP (https://www.huntonprivacyblog.com/2021/11/03/european-parliament-adopts-draft-cybersecurity-directive/). 03.11.2021).***

***

«Согласно последнему аналитизу GlobalData, Европа расширила свое доминирование в сфере найма сотрудников в сфере кибербезопасности среди компаний пищевой промышленности.

За три месяца, закончившихся в сентябре, количество должностей в Европе составило 23,8% от общего числа рабочих мест в сфере кибербезопасности - по сравнению с 12,5% в том же квартале прошлого года.

За ним последовал Азиатско-Тихоокеанский регион, где роль кибербезопасности изменилась на 0,5 процентного пункта в годовом исчислении.

Цифры составлены GlobalData, которая отслеживает количество новых вакансий от ключевых компаний в различных секторах с течением времени. Затем с помощью текстового анализа эти объявления о вакансиях классифицируются по тематике.

Тематический подход GlobalData к отраслевой деятельности направлен на то, чтобы сгруппировать ключевую информацию о компаниях по темам, чтобы увидеть, какие компании лучше всего могут пережить потрясения, грядущие в их отрасли.

Эти ключевые темы, в том числе кибербезопасность, выбраны, чтобы охватить «любую проблему, которая мешает генеральному директору спать по ночам».

Отслеживание их в объявлениях о вакансиях позволяет отрасли видеть, какие компании лидируют по конкретным вопросам, а какие медлят - и, что немаловажно, где рынок расширяется и сужается.

В каких странах наблюдается наибольший рост роли кибербезопасности в пищевой промышленности?

Самой быстрорастущей страной стала Франция, где за три месяца, закончившихся июнь прошлого года, было размещено 0,6% всех объявлений о работе в сфере кибербезопасности, а за три месяца, закончившихся в сентябре этого года, этот показатель вырос до 6%.

Далее следуют Великобритания (рост на 2,6 процентных пункта), Испания (рост на 2,6 процентных пункта) и Польша (рост на 0,7 процентных пункта)…» ***(Michael Goodier. Europe is seeing hiring boom in food industry cybersecurity roles // Verdict Media Limited (https://www.just-food.com/features/europe-is-seeing-hiring-boom-in-food-industry-cybersecurity-roles/). 15.11.2021).***

***

«Reportlinker.com объявляет о выпуске отчета «Рынок кибербезопасности в Центральной и Восточной Европе, по типу решений, по типу развертывания, по типу безопасности, по отрасли конечного использования, по странам, прогноз конкуренции и возможности, 2026»...

Рынок кибербезопасности Центральной и Восточной Европы был оценен в 4,95 млрд долларов США в 2020 году и, по прогнозам, достигнет 11,02 млрд долларов США к 2026 году, при этом в течение прогнозируемого периода CAGR составит 14,35%. Увеличение случаев утечки данных, рост государственных инициатив, расширение базы пользователей Интернета, рост кибератак в здравоохранении, BFSI, розничной торговле и государственном секторе с целью кражи личных данных, финансовой выгоды, доступа к счетам и т.д., Что

положительно повлияет на рынок кибербезопасности Центральной и Восточной Европы в будущем. годы.

Рынок кибербезопасности Центральной и Восточной Европы можно сегментировать по типу решений, типу развертывания, типу безопасности, отрасли конечного использования и стране. В зависимости от типа решений рынок можно разделить на брандмауэр, антивирус и защиту от вредоносных программ, управление рисками и соблюдением требований, идентификацию и управление доступом, предотвращение потери данных, система обнаружения / предотвращения вторжений, шифрование и дешифрование, безопасные веб-шлюзы, фильтрация электронной почты и другие, включая унифицированное управление угрозами, безопасность инфраструктуры, обнаружение конечных точек и реагирование на них и т. д.

Межсетевой экран занял 15,78% доли рынка кибербезопасности Центральной и Восточной Европы в 2020 году; однако ожидается, что сегмент безопасных веб-шлюзов будет расти более быстрыми темпами благодаря их способности выявлять и защищать от передовых интернет-атак с помощью проверки веб-трафика на уровне приложений.

В зависимости от типа развертывания рынок подразделяется на локальные и облачные. Доля рынка локального сегмента в 2020 году составила 56,20%. Тем не менее, ожидается, что облачный сегмент будет расти значительными темпами в течение прогнозируемого периода благодаря широкому распространению облачных платформ хранения данных во всех отраслях.

В зависимости от типа безопасности рынок подразделяется на сетевую безопасность, безопасность конечных точек, облачную безопасность, безопасность приложений, безопасность контента и другие, включая веб-безопасность, критическую инфраструктуру и т.д. Сегмент сетевой безопасности занял 26,91% доли рынка в 2020 году. Ожидается, что сегмент облачной безопасности будет расти более высокими темпами в течение прогнозируемого периода из-за непрерывного роста инвестиций в облачную инфраструктуру.

В зависимости от отрасли конечного использования рынок подразделяется на BFSI, оборону, ИТ и телекоммуникации, здравоохранение, розничную торговлю, энергетику и другие отрасли, включая производство, автомобилестроение и т.д. Доля оборонного сегмента в 2020 г. составила 20,80%, однако сегмент здравоохранения остается ожидается, что он будет расти более высокими темпами.

По странам Центральная и Восточная Европа делится на Чехию, Эстонию, Литву, Польшу, Хорватию, Румынию, Латвию, Венгрию, Словению, Болгарию, Албанию и Черногорию. Ожидается, что среди этих стран Чешская Республика будет доминировать на рынке из-за повсеместного принятия стратегий кибербезопасности, однако ожидается, что Румыния будет расти более высокими темпами.

Основными игроками на рынке кибербезопасности Центральной и Восточной Европы являются Cisco Systems Inc., IBM Corporation, Fortinet Inc., Palo Alto Networks Inc., McAfee Corp, Sophos Group Plc, CrowdStrike Holdings Inc., FireEye Inc., Juniper Networks Inc.., Check Point Software Technologies Inc, CyberArk Software Ltd., Trend Micro Inc., Zscaler Inc., Sonicwall Inc., Barracuda Networks Inc. Эти компании

разрабатывают передовые технологии и запускают новые услуги, чтобы оставаться конкурентоспособными на рынке. Другие конкурентные стратегии включают слияния и поглощения и разработку новых услуг…» ***(Central & Eastern Europe Cybersecurity Market, By Solutions Type, By Deployment Type, By Security Type, By End Use Industry, By Country, Competition Forecast & Opportunities, 2026 // yahoo! finance (https://finance.yahoo.com/news/central-eastern-europe-cybersecurity-market-121400443.html). 22.11.2021).***

***

Китай

«Регулятор киберпространства Китая в воскресенье предложил потребовать от компаний, проводящих листинг акций в Гонконге, подавать заявки на проверки кибербезопасности, если они обрабатывают данные, касающиеся национальной безопасности.

Администрация киберпространства Китая сообщила в проекте правил, что крупные интернет-платформы, планирующие создать штаб-квартиру, операционные или исследовательские центры за рубежом, также должны представить отчет регулирующим органам.

Документ, опубликованный на веб-сайте регулирующего органа в WeChat, призывает требовать общественного обсуждения интернет-платформ, формулирующих политику конфиденциальности или вносящих поправки в правила, которые могут существенно повлиять на права и интересы пользователей.

Фирмы с более чем 100 миллионами активных пользователей в день должны будут проверять изменения сторонними агентствами и получать одобрение правительства.

По словам регулирующего органа, компании, предоставляющие услуги обмена мгновенными сообщениями, должны, если у них нет уважительных причин, прекратить ограничивать доступ пользователей к другим интернет-платформам или передачу файлов на другие интернет-платформы.

Предложения, открытые для публичного рассмотрения до 13 декабря, поступили в связи с усилением надзора Пекина над своим технологическим сектором правилами о том, как они должны обрабатывать огромные массивы данных, которые они контролируют, обращаться с пользователями и взаимодействовать с конкурентами.

Китай, в котором недавно были приняты законы о безопасности данных и защите личной информации, стремится установить правила корпоративного управления для использования фирмами алгоритмов. Он также призвал компании прекратить давно используемую практику «огороженных стенами садов», которая не позволяет делиться ссылками и услугами конкурентов на их платформах.

В июле агентство предложило компаниям с данными для более чем 1 миллиона пользователей пройти проверку безопасности https://www.reuters.com/world/china/china-widens-clampdown-overseas-listings-with-pre-ipo- review-firm-with-large-2021-07-10 перед листингом акций за рубежом, всего

через несколько дней после приостановки первичного публичного размещения акций гиганта Didi Chuxing в связи с предполагаемыми нарушениями данных». ***(China regulator proposes cybersecurity review for some Hong Kong IPOs // Fusion Media Limited (https://uk.investing.com/news/economy/china-regulator-proposes-cyber-security-review-for-some-firms-planning-hong-kong-ipos-2511324). 14.11.2021).***

***

«14 ноября 2021 года Администрация киберпространства Китая (CAC) опубликовала проект Правил управления безопасностью сетевых данных (проект Правил) и принимает общественные комментарии до 13 декабря 2021 года.

Проект Положения состоит из 9 глав и 75 статей с широким охватом всех видов электронных данных. После доработки и принятия CAC проект правил будет содержать более подробные практические рекомендации о том, как выполнять общие юридические требования в соответствии с национальными законами с более высокими юридическими полномочиями, которые были приняты Всекитайским собранием народных представителей и его Постоянным комитетом, такими как Закон о кибербезопасности (CSL), Закон о безопасности данных (DSL) и Закон о защите личной информации (PIPL).

В этом предупреждении мы сосредотачиваемся и резюмируем дополнительные правила, введенные проектом Регламента, включая: (i) классификацию данных и схему многоуровневой защиты (MLPS); (ii) особые обязательства для обработчиков важных данных; (iii) особые обязательства операторов онлайн-платформ; (iv) запрещенная деятельность; (v) отчеты об инцидентах с данными; и (vi) оценки сетевой безопасности». ***(Amy Yin Charmian Aw. China releases draft Network Data Security Management Regulations for comment // Reed Smith LLP (https://www.reedsmith.com/en/perspectives/2021/11/china-releases-draft-network-data-security-management). 23.11.2021).***

***

Російська Федерація та країни ЄАЕС

«В Москве на крупнейших открытых киберучениях завершился конкурс The Standoff Digital Art, в ходе которого «белые» хакеры взламывали картины современных представителей отечественного цифрового искусства. Спойлер: у них получилось.

The Standoff Digital Art — это виртуальная галерея, каждая картина в которой представлена в виде уникального NFT-токена. Именно его и пытались взломать специалисты по кибербезопасности. Свои работы предоставили российские диджитал-художники Desinfo, Meta Rite, Артем Ткач, volv_victory, Anomalit Kate и Loit.

NFT — невзаимозаменяемый токен. Его нельзя разделить на части или заменить на аналогичный. NFT обладает всеми свойствами уникального предмета в физическом мире, поэтому ценится не меньше, а в некоторых случаях даже больше

своей аналоговой версии. Но спрос рождает не только предложение. Произведения искусства всегда кто-то хочет присвоить. Из галереи картину можно украсть, проникнув на выставку. Диджитал-картину можно украсть не вставая с дивана.

При этом технического способа вернуть украденный NFT прежнему владельцу не существует. Вся технология блокчейна, смарт-контрактов подразумевает, что выполненные действия нельзя отменить. Если в самом смарт-контракте не прописан вариант возвращения NFT, то нет и возможности это сделать. С другой стороны, вывести деньги за украденный NFT-объект очень сложно. И замести следы сложнее, чем в случае кражи реальной картины. Все транзакции видны в эксплорере, отследить, кто, что и когда сделал, довольно просто. При этом из блокчейна невозможно что-либо вывести в реальный мир, не используя криптобиржу, а все криптобиржи сейчас запрашивают подробные персональные данные о каждом из своих пользователей. И тем не менее, кражи совершаются. Одним из громких «дел» стала кража двух криптопанков с платформы NFTX в июне 2021 года. Взломщику удалось выручить лишь 6 ETH, в итоге платформа выкупила их обратно. Другой инцидент случился с коллекцией авторов криптопанков (Larva Labs) под названием Meebits. В коде смарт-контракта была обнаружена уязвимость, которая позволяла предугадать редкость нового meebit при его минтинге. Хакеру удалось получить сверхредкий NFT и продать его за 200 ETH.

«NFT — это токен, который реализуется по определенным стандартам, — говорит руководитель отдела исследований по защите приложений Positive Technologies Арсений Реутов. — Но они являются лишь предписанием о том, что должно быть в смарт-контракте. При этом стандарт не регламентирует сам код — отсюда и возникают проблемы. Конечно, есть библиотеки, в которых уже все реализовано и протестировано, но ничто не мешает изменять этот код или добавлять свой. Как правило, именно в этом причина всех уязвимостей».

Подобные слабые места и искали участники The Standoff Digital Art, проверяя на прочность смарт-контракты настоящих российских NFT-объектов. Чтобы завладеть картиной, нападающие находили уязвимости в смарт-контрактах путем анализа исходного кода. Они были опубликованы в тестовой сети блокчейна Ethereum. Каждую из уязвимостей проэксплуатировали только один раз.

Состоялась также дискуссия, участие в которой приняли ведущие эксперты в области кибербезопасности и диджитал-арта. Свое мнение о том, сложно ли украсть NFT-токен, высказали организатор конкурса Арсений Реутов, а также художник, креатор, артист Александр Тито, цифровой художник Артем Ткач, один из драйверов российского NFT-сообщества и другие представители кибер-арта.

Спикеры сошлись во мнении, что NFT — это безусловный тренд нашего времени, а NFT-картины могут не уступать по стоимости аналоговым. Это связано с механизмом ценообразования: «NFT обеспечил CG-художникам возможность выхода на арт-рынок. Появилась возможность продавать — появился и рынок, — заметил Артем Ткач. — Именно рынок формирует стоимость диджитал-арта: самые дорогие работы — это либо самые известные изображения, либо то, что создано медийным автором. Ценность определяется вовлеченной аудиторией».

Спикеры отметили также, что наметилась определенная тенденция на взаимопроникновение аналогового и цифрового искусства:

«Диджитал-направление принесло офлайновым художникам инструмент, чтоб создавать свои произведения и делиться ими. Например, когда был карантин, многие традиционные художники занялись созданием цифрового арта, которым было удобно делиться со всем миром, — отметил Александр Тито. — Так что, с моей точки зрения, это направление — дополнительный инструментарий для художников, чтобы показать миру, чту ты умеешь. Также это удобно. Технологии должны работать на человека».

Однако очевидно, что об обеспечении безопасности NFT-арта известно недостаточно. Итоги конкурса доказывают актуальность этого направления для ИБ-компаний. Ведь хакеры внимательно следят за трендами, и все новейшие технологии мгновенно попадают в их поле зрения.

«Становится ли больше попыток взлома? Ответ будет «да», — отметил Арсений Реутов. — Все больше людей погружаются в тему, изучают язык Solidity и блокчейн-платформы. Но порог вхождения остается довольно высоким, особенно в сфере децентрализованных финансов. Чтобы разобраться в смарт-контрактах, нужно не только знать Solidity, но и сам протокол и всю связанную с ним математику и финансовую сторону, а также то, как другие протоколы могут взаимодействовать с тем, который ты изучаешь. В NFT все попроще, но и там есть очень сложная логика, с которой необходимо разобраться». ***(Кибер-арт проверили на прочность — он не устоял // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5862780-Kiberart-proverili-na-prochnost.html). 18.11.2021).***

***

«Компания «Ростелеком-солар» открыла в Ростове-на-Дону филиал коммерческого центра противодействия кибератакам Solar JSOC. Региональное подразделение обеспечит киберзащиту организаций Южного и Северо-Кавказского федерального округов (ЮФО и СКФО), а также ряда крупных федеральных заказчиков. Сегодня работу филиала обеспечивают свыше 40 аналитиков и инженеров, отвечающих за мониторинг киберинцидентов и эксплуатацию средств защиты информации.

«Solar JSOC в Ростове-на-Дону будет отвечать за безопасность всех региональных клиентов “Ростелекома” в круглосуточном режиме и оказывать полный комплекс услуг: от контроля и управления системами защиты до отражения и расследования кибератак. Новый филиал станет важнейшим технологическим центром по обеспечению кибербезопасности России на Юге», — сказал вице-президент — директор «Ростелекома» на Юге Сергей Мордасов.

Открытие филиала Solar JSOC в Ростове-на-Дону обусловлено высоким уровнем киберугроз в ЮФО. Так, за неполный 2021 г/ эксперты Solar JSOC зафиксировали здесь 58 тыс. атак, из которых более 40% было реализовано с помощью вредоносного ПО (вирусов-шифровальщиков, троянов, шпионского ПО и т.п.), что является крайне высоким показателем на фоне остальных регионов. Вторым и третьим по популярности методами взлома корпоративных инфраструктур стали атаки на веб-приложения (29%) и DDoS (6%). При этом достаточно часто инструментарий злоумышленников в ЮФО базируется на коммерческом фреймворке Cobalt Strike, предназначенном для эксплуатации

уязвимостей. Это косвенно говорит о высокой активности в регионе именно киберкриминальных группировок, нацеленных на прямую монетизацию атак.

«Мы видим запрос на экспертизу информационной безопасности со стороны организаций Южного федерального округа. При этом в регионе наблюдается кадровый дефицит в сфере информационной безопасности. Открытие локального центра Solar JSOC в Ростове-на-Дону позволит сделать технологии кибербезащиты для компаний Юга более доступными, а также увеличит кадровый потенциал и привлечет в отрасль молодых талантливых специалистов», — отметил вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов.

«Ростелеком-Солар» активно сотрудничает с ведущими вузами Ростовской области (Донской государственный технический университет, Южный федеральный университет, Южно-Российский государственный политехнический университет имени М. И. Платова) в практической подготовке студентов к работе в сфере информационной безопасности. Уже сегодня более 70 ростовских студентов прошли специализированные стажировки. Лучшим из них будет предложена работа в центре противодействия кибератакам». ***(«Ростелеком» открыл в Ростове-на-Дону центр противодействия кибератакам // CNews (https://www.cnews.ru/news/line/2021-11-18_rostelekom_otkryl_v_rostove-na-donu). 18.11.2021).***

***

«Около 68% опрошенных сервисом SuperJob россиян сообщили, что не получили от работодателей инструкцию по кибербезопасности в условиях удаленной работы.

Лишь 16% респондентов получили при переходе на новый режим ценные указания и стали соблюдать новые требования. Кого-то обязали подписать дополнительное соглашение в сфере защиты данных (о таком нововведении сообщили 4% участников опроса), других призвали использовать выделенные VPN-каналы (2%) и программы-антивирусы, а также защищенное соединение и двухфакторную аутентификацию — по 1% опрошенных по всем пунктам. Еще 1% россиян получил указание работать с документами только в одиночестве, передают «Известия».

Только 16% респондентов получили дополнительные инструкции и обязанности в период пандемии коронавируса. Некоторых россиян (4%) обязали подписать соглашение в сфере защиты данных, а кто-то был вынужден использовать при работе VPN-каналы и антивирусные программы (2%). Помимо этого, 1% опрошенных сообщили, что получили от работодателя требование находиться одному в комнате при работе с документами.

Удаленный формат работы, предполагают эксперты, останется в жизни россиян надолго. Поэтому риски информационной безопасности будут только расти. Примеров, когда один сотрудник по невнимательности или из-за отсутствия средств защиты информации ставил под угрозу функционирование все организации, предостаточно». ***(68% россиян, работающих на удаленке, не получили инструкции по кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/526727.php). 20.11.2021).***

***

«По словам генерал-лейтенанта Раджеша Панта, национального координатора по кибербезопасности в канцелярии премьер-министра в правительстве Индии, который сделал объявление на выступлении экспертов Microsoft в прошлую пятницу, новая стратегия кибербезопасности Индии скоро будет развернута.

«Мы работали над формированием новой стратегии в течение последних двух лет. Стратегия сейчас находится в кабинете министров для окончательной печати», - сказал Пант.

Во время саммита по борьбе с мошенничеством и нарушениями в 2019 году компании Information Security Media Group Пант заявил, что структура безопасности, необходимая для стратегии кибербезопасности Индии, была создана, и все, что осталось, - это развертывание и внедрение.

В ходе беседы на тему «Expert Speak» с Кешавом Дакадом, генеральным советником Microsoft в Индии, отставной генерал-лейтенант индийской армии сказал, что стране в первую очередь нужна структура управления. «В целом структура существует, но нет никакой организации, которая бы контролировала распределение ролей и ответственности», - сказал он.

По словам Панта, одним из основных результатов новой стратегии кибербезопасности является определение и назначение регулирующих органов для различных организаций, таких как Группа реагирования на компьютерные чрезвычайные ситуации или CERT-In, Координационный центр киберпреступлений, Агентство защиты киберпреступлений и Национальный центр защиты критической информационной инфраструктуры или NCIIPC.

Пант сказал, что, хотя в Индии действует национальная политика кибербезопасности, стране нужна киберстратегия. «Разница между стратегией и политикой заключается в том, что первая представляет собой план, ориентированный на действия. Он определяет цель. Он сообщает нам, кто будет выполнять эту задачу, а также указать финансирование и сроки для достижения цели», - сказал он.

Более того, растущее проникновение Интернета в сельских районах Индии делает граждан, менее осведомленных о киберугрозах, уязвимыми для новых форм кибератак и кибермошенничества. «Большое количество частных предприятий, которые являются частью критически важной инфраструктуры Индии - например, электроэнергетический и телекоммуникационный секторы - также подвергаются кибератакам со стороны национальных государств», - отметил Пант. По его словам, это еще одна причина, по которой правительству необходимо вмешаться, чтобы защитить отрасль.

Подчеркивая текущую картину угроз в Индии, Пант сказал, что государственные учреждения подвергаются почти 20% всех кибератак в Индии. Банковское дело и финансы занимают второе место, за ним следует ИТ-сектор.

Дорожная карта кибербезопасности Индии

По словам Панта, помимо создания высшего регулирующего органа, новая стратегия также учитывает различные архитектурные требования, необходимые для достижения целей, определенных в стратегии.

Пант сказал, что, например, если бы кто-то сегодня сообщил о вредоносном ПО, люди перешли бы на частный веб-сайт VirusTotal. По его словам, проблема в том, что теперь у VirusTotal есть все данные о вредоносных программах в Индии и целевых организациях. По его мнению, это плохо для национальной безопасности.

«Итак, мы создали наш собственный национальный отчет о вредоносных программах. Он находится на заключительной стадии бета-тестирования, и у нас уже есть 75 миллионов образцов в репозитории, так что он будет не хуже VirusTotal», - сказал он.

Пант заявил, что правительство работает над созданием национальной системы обмена разведданными об угрозах с целью сбора всей информации об угрозах в одном месте и распространения ее среди различных организаций и государственных органов.

Кроме того, Пант объяснил, как проект Национального киберкоординационного центра сможет обеспечить безопасность на шлюзах: «Если есть 200 интернет-шлюзов от всех поставщиков услуг, на каждом из этих шлюзов будут зонды, которые будут читать только метаданные. Метаданные покажут IP-адреса и пакеты данных, а также их источник и место назначения. С помощью этой информации можно прогнозировать угрозы ».

Поэтому он предположил, что если на один конкретный IP-адрес отправляется много пакетов, можно предположить, что это, скорее всего, распределенная атака типа отказ в обслуживании или DDoS-атака.

Последние достижения в кибернетической сфере

Пант сказал, что индийские кибер-агентства добились значительных успехов в недавнем прошлом.

Он сказал, что CERT-In отлично справляется с реагированием на инциденты. «Индийский координационный центр киберпреступности в прошлом году также проделал фантастическую работу по борьбе с киберпреступностью с помощью анализа угроз и цифровой криминалистики», - добавил он.

Пант рассказал о том, как Министерство электроники и информационных технологий обеспечивает просветительскую работу. Он сказал, что Министерство иностранных дел создало отдел по кибердипломатии, кибер-агентство по защите было создано для защиты оборонных учреждений Индии, а NCIIPC был создан для защиты критически важных активов страны.

Пант сообщил, что CERT-In недавно стал центром нумерации CVE после аккредитации MITER ATT & CK Framework.

Он также сказал, что в дополнение к телекоммуникационному сектору Министерство энергетики заслуживает похвалы за создание Операционного центра безопасности в каждом из своих секторов, от производства электроэнергии до распределения.

«Два сверхкритических сектора смогли отразить и смягчить множество целевых атак в недавнем прошлом», - сказал он.

Кроме того, Центральное управление электроэнергетики Индии недавно выпустило Руководство по кибербезопасности в электроэнергетическом секторе до 2021 года для организаций в энергетическом секторе, чтобы защитить системы OT, создать структуру кибербезопасности, усилить оценку киберрисков и улучшить реагирование на инциденты и отчетность». ***(Soumik Ghosh. India's National Cybersecurity Strategy Awaiting Approval // Information Security Media Group, Corp. (https://www.govinfosecurity.com/indias-national-cybersecurity-strategy-awaiting-approval-a-17829). 01.11.2021).***

***

«Национальное управление кибербезопасности Израиля (INCD) объявило в понедельник, что страна собирается создать лабораторию для исследований, а также получения дополнительной информации об искусственном интеллекте (AI) в секторе кибербезопасности. По сообщению INCD, лаборатория будет создана в районе Беэр-Шева южного города в сотрудничестве с городским университетом Бен-Гуриона, сообщает агентство Синьхуа.

INCD также отметил, что это учреждение является частью правительственной инициативы по благоустройству городов в пустыне Негев. Также выяснилось, что исследование, которое будет проводиться в лаборатории, будет сосредоточено исключительно на партнерстве между учеными, правительством и бизнесом. Лаборатория даже будет распознавать и бороться с киберугрозами ИИ и будет создавать инновационные методы защиты и навыки на основе ИИ для повышения кибербезопасности интеллектуальных систем.

«Израиль стал наиболее уязвимым объектом атак программ-вымогателей с 2020 года»

Стоит отметить, что Израиль подвергся нескольким кибератакам. Согласно недавнему анализу, проведенному испанской фирмой по кибербезопасности Virus Total, в октябре Израиль стал наиболее пострадавшим от атак программ-вымогателей с 2020 года. Проведенное по заказу Google расследование кибербезопасности показало, что сионистское государство представило наибольшее количество образцов. который был обнародован 14 октября. Результат исследования, получивший название «Отчет об активности программ-вымогателей», был основан на более чем 80 миллионах образцов, взятых из 140 стран.

Более того, программы-вымогатели превратились в одну из самых серьезных и растущих киберугроз в мире. В июле в результате удара программы-вымогателя Kaseya, американского поставщика услуг, были временно закрыты сотни организаций в 17 странах. После этого ФБР начало полное расследование ситуации, сотрудничая с Агентством кибербезопасности и безопасности инфраструктуры и другими правительственными учреждениями США, чтобы понять всю широту опасности.

Совместная рабочая группа США и Израиля по борьбе с кибератаками

В дополнение к этому, 14 ноября, в воскресенье, министерство финансов США заявило, что будет сотрудничать с министерством финансов Израиля в борьбе с программами-вымогателями и угрозами кибербезопасности, сообщает The Hill. Согласно сообщению министерства финансов, целевая группа будет стремиться

защищать важные финансовые системы и разрабатывать технологии, способствуя дальнейшему развитию международного сотрудничества для борьбы с опасностью программ-вымогателей на международном уровне.

Министерство финансов также сообщило, что страны составят меморандум о взаимопонимании (MOU), чтобы помочь обмену информационными инициативами в финансовой отрасли, включая рекомендации по кибербезопасности, происшествия и информацию об угрозах, а также обучение сотрудников и другие операции». ***(Anwesha Majumdar. Israel To Build Artificial Intelligence Research Laboratory For Dealing With Cybersecurity // REPUBLICWORLD (https://www.republicworld.com/world-news/middle-east/israel-to-build-artificial-intelligence-research-laboratory-for-dealing-with-cybersecurity.html). 16.11.2021).***

***

«В сегодняшнюю цифровую эпоху есть только два типа компаний. Те, которые были взломаны, и те, которые будут взломаны. В-третьих, если мы добавим тех, кто был взломан, но просто не знает об этом.

Развивающиеся рынки в Латинской Америке и за ее пределами наиболее уязвимы для взломов и взломов, потому что на общем уровне кибербезопасности они пытаются наверстать упущенное. В настоящее время Латинская Америка еще не имеет прочной основы кибербезопасности, необходимой для защиты будущего своего бизнеса.

В то же время Латинская Америка становится еще более привлекательным местом для киберпреступников, поскольку в ее компании закачиваются беспрецедентные суммы денег. Согласно данным Crunchbase, местные стартапы собрали рекордные 9,6 млрд долларов в первой половине 2021 года, а SoftBank только что объявил о создании нового многомиллиардного фонда для региона.

Латинской Америке срочно необходимо разработать более совершенные решения в области кибербезопасности, чтобы обеспечить долговечность бизнеса следующего поколения. Но более того, мы смотрим на огромные возможности в процессе становления.

Тот факт, что Латинская Америка находится на заднем плане, на самом деле означает, что у нее есть уникальный шанс построить более прочную инфраструктуру кибербезопасности с нуля, максимально используя потенциал современных передовых технологий, чего не могут сделать более развитые рынки. И он может экспортировать эти решения по всему миру.

Вот как я вижу развитие многообещающего сценария кибербезопасности Латинской Америки, если все игроки приложат все усилия.

Передовые технологии должны стать отправной точкой

Ранее в этом году агентство по кибербезопасности ЕС предупредило, что традиционные механизмы кибербезопасности больше не эффективны против современных быстро развивающихся атак.

Развивающиеся рынки уже находятся на переднем крае новых технологий, от нео-банков, которые предоставляют гражданам больше возможностей для входа в финансовую систему, до стартапов B2B, сглаживающих путь для предприятий в разных отраслях. Закладывая фундамент в этих новых нишах, они также должны

внедрять технологии, которые развиваются такими же темпами, как и киберпреступность.

Одно из самых важных нововведений - это уникальные «онлайн-персонажи». Когда каждый из ваших банков, платежных платформ и сайтов электронной коммерции имеет полностью отдельную личность пользователя для одного и того же человека, каждая из этих платформ является точкой входа для хакера, который может украсть вашу личность или совершить мошенничество. Но когда ваша личность является единичной децентрализованной «личностью», вы один являетесь точкой входа в этот сетевой идентификатор.

Такие технологии, как блокчейн, позволяют вашей личности быть по-настоящему суверенной - уникальной и контролируемой вами - потому что хакерам, использующим блокчейн, практически невозможно клонировать или взломать эту информацию. А другие новейшие технологии, такие как передовое антифишинговое программное обеспечение, такое как Pixm, устраняют риск человеческой ошибки при потере этой информации в Интернете.

Развивающиеся рынки могут возглавить прогресс

Когда компании на развитых рынках укрепляют свою цифровую защиту, они опираются на существующие структуры кибербезопасности, с которыми киберпреступники тоже хорошо разбираются. Или им нужно создать новую структуру кибербезопасности вокруг существующих продуктов, сохраняя при этом эти продукты в рабочем состоянии. Это похоже на старый дом, когда вы понимаете, что фундамент разваливается, и пытаетесь восстановить фундамент, сохранив при этом остальную часть дома нетронутой.

Ретроактивное применение средств защиты кибербезопасности имеет огромные ставки. Для малого и среднего бизнеса это означает, что нужно время, чтобы интегрировать лучшие решения в свои сайты электронной коммерции; для банков речь идет о переосмыслении своей защиты, но при этом никогда не ставят под угрозу средства, которые доверили им миллионы людей.

Но у развивающихся рынков есть то преимущество, что они обходят устаревшие кибертехнологии и сразу переходят к самым непреодолимым - и масштабируемым против будущих итераций киберпреступлений - технологиям, и это не следует недооценивать.

Латинская Америка готова к процветанию в космосе

Большая часть роста Латинской Америки - это устойчивость. Стартапам на развивающихся рынках приходится сталкиваться с гораздо большим давлением - деньгами, управлением, социально-экономическими проблемами, - а это означает, что они должны вводить новшества, одновременно обеспечивая устойчивое строительство с первого дня.

Что это означает для кибербезопасности в регионе? Эта устойчивость в сочетании с безотлагательностью киберпреступности подтолкнет феноменальные технические таланты Латинской Америки на передний план волны новых технологий. Индустрия кибербезопасности растет на развивающихся рынках до такой степени, что привлекает инвестиции из Кремниевой долины. И горшок становится все больше: венчурное финансирование в области кибербезопасности

достигло ошеломляющих 9 миллиардов долларов в первой половине 2021 года - больше, чем за весь 2020 год.

Бизнес в Латинской Америке уже открывает новые возможности. LACChain альянс фокусировкой на Латинской Америки и Карибского бассейна экосистемами стремится к более эффективной интеграции blockchain технологии в организации и страны, а также работает в направлении суверенного ID полностью основанной на blockchain. Аргентина движется к концепции суверенного идентификатора с помощью потребительского приложения MODO, которое объединяет транзакции крупных банков страны на единой платформе.

Правительству и частному бизнесу необходимо сотрудничать

По мере того как предприниматели ищут решения, правительства должны способствовать созданию открытой экосистемы, в которой молодые компании побуждаются преодолевать существующие ограничения инфраструктуры и выходить на малоизученные территории.

Государственные органы могут предлагать стратегии финансирования, от поддержки местных инвестиционных фондов до привлечения иностранных венчурных капиталистов с помощью конференций, поощрений и информационных кампаний, а также привлечения внимания к наиболее выдающимся цифровым стартапам сегодняшнего дня для развития стартапов будущего.

Также крайне важно, чтобы правительства способствовали лучшему образованию молодежи в области ИТ-безопасности. Страны также не могут отказаться от обновления своих законов в отношении конфиденциальности, согласия пользователей или права на забвение. Речь идет не только о том, чтобы их ускорить - закону Аргентины о защите данных уже 20 лет, - речь идет об унификации нормативных требований в разных странах, чтобы технологии завтрашнего дня, изменяющие жизнь, могли быть поистине безграничными.

Наконец, частный бизнес должен поддерживать постоянный диалог с правительствами по вопросам кибербезопасности и технологического прогресса, обеспечивая постоянную обратную связь и выступая в качестве источника текущей информации о тенденциях, которая поможет правительству регулировать и расширять технологическое пространство…». ***(Sebastian Stranieri. Why Latin America Needs To Build A Cybersecurity Fortress ASAP // Crunchbase, Inc. (https://news.crunchbase.com/news/latin-america-emerging-markets-cybersecurity/). 15.11.2021).***

***

«20 сентября 2021 года Министерство общественной безопасности (МОБ) Вьетнама опубликовало проект указа об административных санкциях в области кибербезопасности («Проект указа»). MPS собирает общественные мнения по данному проекту Указа до 18 ноября 2021 года.

Проект Указа состоит из четырех глав и 51 статьи, основное содержание которых касается административных правонарушений, штрафов и корректирующих мер, охватываемых главой II.

Ключевые выводы

Внесудебные рамки регулирования проекта указа повлияют как на национальные, так и на офшорные организации и частных лиц.

Штраф, применяемый к организации-нарушителю, может составлять до 5% от ее дохода, полученного на рынке Вьетнама.

Некоторые положения Проекта Указа дают некоторое представление о том, как МОБ обновило проект Указа о защите персональных данных (« Проект НДПИ »), который был выпущен в феврале 2021 года, излагая конкретные санкции в отношении режима защиты персональных данных, применимого к « Контроллер персональных данных», «Организация, контролирующая и обрабатывающая персональные данные»и «Третья сторона». Эти условия не упоминаются в версии проекта PDPD, выпущенной в феврале 2021 года…» ***(YEE CHUNG SECK AND MANH HUNG TRAN. Vietnam: Draft decree on cybersecurity administrative sanctions released // Global Compliance News (https://www.globalcompliancenews.com/2021/11/11/vietnam-draft-decree-on-cybersecurity-administrative-sanctions-released031121/). 11.11.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Белорусское правительство обвиняют как минимум в «частичной ответственности» за атаки Ghostwriter в Европе.

В то время как компании, занимающиеся кибербезопасностью, часто проявляют осторожность, когда дело доходит до атрибуции групп угроз, в Mandiant заявляют, что «глубоко уверены» в том, что Ghostwriter, также связанный с деятельностью UNC115, является киберпреступной организацией, потенциально работающей от имени правительства страны.

Санкции были введены в отношении Беларуси в начале этого года после принудительного перенаправления коммерческого самолета в воздушное пространство Беларуси для ареста пассажира, журналиста-диссидента по имени Роман Протасевич. Теперь в отместку президента страны Александра Лукашенко обвинили в создании миграционного кризиса с целью дестабилизации ЕС.

Тем не менее, похоже, что возмездие может пойти и дальше, с приписыванием Ghostwriter правящему правительству.

Европейский совет ранее обвинял Россию в причастности к Ghostwriter.

По мнению исследователей кибербезопасности, вмешательство России нельзя «исключать», но другие индикаторы указывают на то, что интересы Беларуси лежат в основе операции, в которой обычно участвуют государственные и частные организации в Украине, Литве, Латвии, Польше и Германии. целевой.

Кроме того, Ghostwriter также участвовал в нападениях на белорусских диссидентов, СМИ и отдельных журналистов.

UNC1151 - активен с 2016 года - и Ghostwriter когда-то сосредоточились на продвижении антинатовских материалов с помощью фишинга, спуфинга и взлома уязвимых веб-сайтов. Однако с 2020 года группы расширили свою деятельность в

попытках повлиять на политику Польши и украсть конфиденциальную информацию с помощью кражи учетных данных.

UNC1151 также был нацелен на белорусские СМИ и представителей оппозиции в преддверии выборов 2020 года, что является убедительной победой. Нападений на госструктуры России и Беларуси не зафиксировано.

«Кроме того, в нескольких случаях лица, ставшие мишенью UNC1151 перед выборами в Беларуси 2020 года, позже были арестованы белорусским правительством», - сообщает Мандиант.

Многие кампании Ghostwriter сосредоточены на антинатовских нарративах. С середины 2020 года группа распространяет материалы, в которых обвиняются НАТО в коррупции, вооруженные силы - в распространении COVID-19, а также в коррупции в политике Литвы и Польши. ЕС также подвергался критике в ходе недавних кампаний.

«Рассказы авторов-призраков, особенно критики соседних правительств, были показаны на белорусском государственном телевидении как факт», - добавили исследователи. «Мы не можем установить, является ли это частью скоординированной стратегии или это просто белорусское государственное телевидение, продвигающее нарративы, которые соответствуют интересам режима и не интересуются точностью». ***(Charlie Osborne. Belarus government accused of 'partial responsibility' for Ghostwriter campaigns // ZDNet (https://www.zdnet.com/article/belarus-government-accused-of-partial-responsibility-for-ghostwriter-hacking/). 16.11.2021).***

***

«По данным британского агентства по киберзащите, западные страны как никогда прежде подвергаются атакам со стороны киберпреступников и стран-изгоев.

По данным Национального центра кибербезопасности (NCSC), количество атак увеличилось почти на 7% с начала года по 31 августа по сравнению с предыдущим годом: количество попыток взлома достигло рекордно высокого уровня, а многочисленные угрозы были связаны с «враждебными» государствами, такими как Китай и Россия.

NCSC заявляет, что за последний год ему пришлось иметь дело с 777 киберинцидентами по сравнению с 723 за предыдущие 12 месяцев.

В эту статистику была включена глобальная хакерская кампания, организованная американской технологической фирмой SolarWinds, которая сильно повлияла на правительство США.

При поддержке китайского государства взлом серверов Microsoft Exchange в марте стал еще одной крупномасштабной кибербезопасностью с целью кражи информации, такой как интеллектуальная собственность.

Возросшая киберугроза приводит к тому, что компании усиливают свою безопасность, чтобы защитить себя от любых будущих атак, и увеличивают доходы компаний в этом секторе.

Corero Network Security PLC (AIM: CNS), провайдер высокопроизводительных распределительных атак типа «отказ в обслуживании», объявил ранее сегодня, что

он обеспечил выполнение нескольких значительных заказов клиентов на общую сумму более 4 миллионов долларов США.

Представитель Corero подтвердил, что он заметил, что «уровень атак значительно растет из года в год».

Киберзащита теперь является необходимостью, и Оксфордский университет стал последним, кто предотвратил попытку атаки благодаря внедрению услуг NCSC.

Атаки программ-вымогателей, при которых хакеры блокируют пользователей своих систем данных и требуют выкуп перед тем, как вернуть хост обратно, были названы в отчете агентства одной из самых быстрорастущих опасностей.

Линди Кэмерон (NYSE: CAM), исполнительный директор NSCS, заявила, что программы-вымогатели «сейчас представляют собой самую непосредственную угрозу кибербезопасности британского бизнеса».

Sophos, глобальная компания, занимающаяся кибербезопасностью, заявила, что ожидает, что кибератаки станут более распространенными в течение следующих 12 месяцев, при этом хакеры-специалисты предоставят разным группам злоумышленников набор методов, позволяющих им запускать собственные атаки». ***(Jai Singh. Hacking attacks at record high sparks boom for cybersecurity firms // Proactive (https://www.proactiveinvestors.co.uk/companies/news/966555/hacking-attacks-at-record-high-sparks-boom-for-cybersecurity-firms-966555.html). 17.11.2021).***

***

«Высокопоставленный представитель Пентагона предложил тем, кто считает, что кибербезопасность должна играть более центральную роль в национальной обороне, следует внимательно следить за выпуском Стратегии национальной обороны до 2022 года.

«Мы думаем о роли киберпространства как инструмента в стратегии национальной обороны», - заявила на прошлой неделе в CyberNext DC заместитель помощника министра обороны по киберполитике. «Я думаю, вам всем будет интересно, что мы скажем по этому поводу».

Каждые четыре года по закону министерство обороны должно публиковать Стратегию национальной обороны (ранее известную как Четырехгодичный обзор обороны или QDR). Здесь Министерство обороны смотрит в будущее и обрисовывает в общих чертах то, что оно считает возникающими угрозами; например, QDR 2010 г. был первым случаем, когда департамент определил изменение климата как угрозу национальной безопасности.

В 2018 году, когда название изменилось, новая Стратегия национальной обороны «признала, что мы не можем защитить свой выход от проблемы [киберугрозы]», - сказал Эоян. Именно тогда возникла концепция «защиты вперед» и стратегия постоянного взаимодействия. «В результате кибер-стратегия отдела стала намного яснее».

Она сказала, что у отдела есть три основные задачи в киберпространстве: защита сетей Министерства обороны США, расширение возможностей сети для боевиков и защита нации в целом. «И под этим мы подразумеваем общегосударственные действия».

Еоян отметил, что Министерство обороны сыграло определенную роль в обеспечении безопасности выборов в 2018 и 2020 годах. «Мы были одними из главных игроков, [и] мы должны сделать это снова в 2022 году».

Растущая угроза программ-вымогателей - еще одна область, в которой задействованы кибер-возможности Пентагона, потому что многие злоумышленники либо агенты враждебного национального государства, либо укрываются им.

«Хотя Министерство обороны не несет ответственности за все киберпреступления... когда они поражают инфраструктуру [в США], у нас есть ресурсы, чтобы бороться с ними», - сказал Эоян. «Некоторые из наших противников обладают огромными ресурсами в этой области».

Она сказала, что Пентагон видит, что враждебные страны проводят кибератаки «ниже порога», то есть недостаточно серьезные, чтобы превратиться в акт войны, но что существует растущий риск непредвиденных последствий, если ситуация выйдет из-под контроля.

Eoyang обратился к слушающей лично и онлайн-аудитории с просьбой о том, чтобы оборонные подрядчики помогли министерству повысить кибербезопасность союзников США и международных партнеров.

«В некоторых из этих стран есть компании, которые обладают невероятными возможностями, но… мы должны помочь нашим партнерам и союзникам стать лучше в области киберзащиты», - сказала она. «Я думаю, что во многих случаях [им] было бы более комфортно, если бы они могли работать напрямую с компаниями. [Это бесполезно], если они покупают F-35, но сети, в которых работают F-35», находятся под угрозой». ***(Patience Wait. Cyber policy lead Mieke Eoyang discussed the Defense Department's role in the nation's cybersecurity posture, including in defending elections and countering ransomware attacks // Nextgov (https://www.nextgov.com/cybersecurity/2021/11/pentagon-officials-rethinking-cybers-role-national-defense-strategy/187010/). 22.11.2021).***

***

Створення та функціонування кібервійськ

«Флагманский корабль Шестого флота ВМС США Mount Whitney завершил учения и начал переход из Чёрного в Средиземное море. Об этом сообщили в пресс-службе флота.

10 ноября Минобороны РФ сообщило, что корабли ВМС США прибыли для участия в проводимых объединенным командованием Вооруженных сил США в Европе многонациональных учениях в Черноморском регионе. По данным Минобороны, там находились эсминец с управляемым ракетным оружием Porter, танкер John Lenthall l и Mount Whitney ВМС США.

Как утверждают американские военные, после модернизации плавсредство Mount Whitney стало настоящим «кораблем-хакером». По их словам, сейчас Mount Whitney имеет самое совершенное радиокоммуникационное оборудование среди всех когда-либо существовавших кораблей.

Флагман Шестого флота США может взламывать чужие сети боевого управления, в том числе российские. Таким образом американские военные якобы могут получать доступ к огромным объемам разведданных, перехватывать контроль над вооружением, а также парализовать оборонные системы противника.

Например, оборудование Mount Whitney может взламывать системы управления вооружением, перехватывать данные, разрывать связь операторов с беспилотниками, а также загружать вредоносное ПО в аппаратуру противника». ***(Американцы отправили в Черное море «корабль-хакер» // SecurityLab.ru (https://www.securitylab.ru/news/526528.php). 15.11.2021).***

***

Захист персональних даних

«Менее чем через месяц после того, как израильские официальные лица предупредили о волне попыток кибератак на сектор здравоохранения страны, хакерская группа Black Shadow, которая якобы связана с Ираном, по сообщениям, утекла конфиденциальные медицинские записи почти 300000 пациентов израильской сети медицинских центров.

2 ноября местное СМИ The Times of Israel сообщило, что на прошлой неделе Black Shadow выложила утечку украденных медицинских карт примерно 290 000 пациентов из базы данных Machon Mor, которая управляет почти 30 медицинскими клиниками в Израиле.

Обнародованные данные включают в себя информацию об анализах крови пациентов, лечении, назначениях, сканировании медицинских изображений, колоноскопии и вакцинации, а также переписку от пациентов относительно запросов на прием к врачу, а также о необходимости процедур и результатов анализов, сообщает Times of Israel.

Махон Мор не сразу ответил на запрос Information Security Media Group о комментарии.

Ранее в тот же день, когда произошла утечка информации о Macon Mor, Black Shadow опубликовала то, что, по ее утверждению, было полной базой данных личной информации о пользователях для десятков тысяч людей с веб-сайта Atraf, службы знакомств и индекса ночной жизни ЛГБТ, сообщает Times of Israel.

Утечка данных о пользователях Atraf включала их местонахождение и, в некоторых случаях, информацию о ВИЧ-статусе, которую пользователи имели в своих профилях, сообщает Times of Israel.

Black Shadow, как сообщается, загрузила данные на канал в приложении для обмена сообщениями Telegram после того, как требование выкупа в размере 1 миллиона долларов в цифровой валюте для предотвращения утечки, по-видимому, не было оплачено организацией, согласно Times of Israel.

Группа первоначально взломала Cyberserve - израильскую хостинговую компанию - в конце октября, отключив ее серверы и ряд сайтов, в том числе Atraf, сообщает Times of Israel.

Прочие атаки

После октябрьской кибератаки на Cyberserve национальный кибернетический массив Израиля выпустил публичный совет, призывающий пострадавших граждан «проявлять бдительность в отношении подозрительных электронных писем и сообщений, менять пароли и внедрять двухэтапную проверку во всех приложениях, таких как социальные сети и приложение банка».

В последние месяцы нападения на некоторые другие израильские организации приписывают Black Shadow.

Сообщается, что в марте группа заявила, что взломала израильскую компанию по финансированию автомобилей KLS Capital и украла данные клиентов, а в декабре 2020 года произошла утечка тысяч документов, содержащих личную информацию о клиентах израильской страховой компании Shirbit.

Лучшие цели

Не все убеждены в предполагаемой роли Black Shadow в этих инцидентах.

«Трудно понять, за что законно несет ответственность группа. В кибер-мире любой может «спрятаться» или «представиться» под любым именем, которое выберет», - отмечает Амир Магнер, президент и соучредитель израильской службы безопасности здравоохранения. фирма CyberMDX.

«Это означает, что имя «Черная тень» может одновременно использоваться несколькими, не связанными между собой группами, решившими идентифицировать себя под одним и тем же именем», - говорит он.

Общая характеристика некоторых из этих последних вымогателей инцидентов злоумышленники, использующих тактику двойного вымогательства.

«Перед тем как зашифровать базы данных жертвы, злоумышленники извлекают большие объемы конфиденциальной коммерческой информации и угрожают опубликовать ее, если не будет выплачен выкуп, что оказывает дополнительное давление на предприятия, заставляя их выполнять требования хакеров». - говорит Магнер.

Он добавляет, что поставщики медицинских услуг во всем мире осознают, что они являются главными целями для таких кибератак.

«Это не временная тенденция, это то, что должно остаться.

«Мы видим очень высокую мотивацию атаковать организации здравоохранения во всем западном мире. Нет сомнений в том, что каждая успешная атака, при которой злоумышленники видят широкий эффект, который она производит, побуждает их продолжать атаковать большее количество организаций здравоохранения», - говорит он.

Как отмечает Магнер, Израиль, как и другие развитые страны мира, имеет развитую систему здравоохранения со множеством подключенных устройств Интернета вещей и медицинской информацией, передаваемой в цифровом виде.

«Те же методы, которые эффективны для злоумышленников, нацеленных на медицинские учреждения в Дюссельдорфе, Сингапуре или Сан-Диего, также могут работать против медицинских организаций в Израиле».

Очевидное нарушение медицинских записей сотен тысяч пациентов Махон Мор произошло всего через несколько недель после того, как несколько израильских

поставщиков медицинских услуг, в том числе Медицинский центр Хиллеля Яффе в городе Хадера, подверглись кибератакам в октябре.

Израильские кибернетические чиновники выпустили предупреждения об этой деятельности в прошлом месяце, и израильские власти в то время подозревали, что эти атаки были связаны с китайскими хакерскими группами.

«Хотя вполне возможно, что нападения на израильские медицинские учреждения имеют политический мотив, лучше не задумываться над этой тенденцией», - говорит Сарью Найяр, генеральный директор поставщика средств безопасности Gurucul.

Она добавляет, что больницы являются частью критически важной инфраструктуры страны, и существует множество потенциальных векторов атак, которые можно использовать.

«Мы наблюдаем рост количества программ-вымогателей в сфере здравоохранения в США и других частях мира, отчасти потому, что ИТ-системы здравоохранения сложны и включают в себя записи пациентов и сотрудников, системы выставления счетов, уровень удовлетворенности пациентов и взаимосвязанные медицинские устройства», Найяр говорит». ***(Marianne Kolbasuk. Black Shadow Group Leaks Israeli Patient Records, Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/black-shadow-group-leaks-israeli-patient-records-data-a-17866). 08.11.2021).***

***

«Онлайн-атака привела к отключению системы здравоохранения в самой восточной провинции Канады, нарушила обслуживание пациентов и привела к краже личных данных многих жителей, включая медицинскую информацию.

30 октября представители здравоохранения провинции Ньюфаундленд и Лабрадор сообщили, что системы здравоохранения были нарушены в результате «киберинцидента». Хотя официальные лица не использовали слово «программа-вымогатель», эксперты по безопасности говорят, что эта атака имеет признаки эпидемии криптоблокирующего вредоносного ПО.

Расследование нападения продолжается. «Это развивающаяся ситуация», - сказал премьер-министр Ньюфаундленда и Лабрадора Эндрю Фьюри на пресс-конференции во вторник.

Фьюри сказал, что следователи обнаружили, что личная информация некоторых жителей, в том числе информация о здоровье, была раскрыта более чем за десять лет, как и личная информация сотрудников системы здравоохранения.

«Для пациентов информация состоит из базовой информации, которая обычно регистрируется или используется для посещения пациента, такой как имя, адрес, номер медицинского учреждения (MCP), кого вы посещаете, причина посещения, ваш врач, номер телефона и т.д. дата рождения, адрес электронной почты для уведомлений, стационарное или амбулаторное лечение, девичья фамилия матери и семейное положение», - говорится в сообщении правительства провинции в обновлении системы безопасности.

«Для нынешних и бывших сотрудников информация включает имя, адрес, контактную информацию и номер социального страхования».

Чиновники говорят, что они не верят, что банковские реквизиты сотрудников были раскрыты.

Правительство не опубликовало никаких данных о количестве пострадавших, но население провинции составляет около 520 000 человек.

Королевская канадская конная полиция ведет уголовное расследование инцидента при поддержке Канадского центра кибербезопасности, который является публичным подразделением Управления безопасности связи страны и руководителем национального реагирования на инциденты. CSE является дочерним агентством по радиосвязи Агентства национальной безопасности США и британской GCHQ.

Официальные лица провинции говорят, что они также уведомили о нарушении Управление по информации и конфиденциальности Ньюфаундленда и Лабрадора.

«Мы глубоко сожалеем о том, что произошел этот инцидент, и принимаем меры для защиты конфиденциальности наших сотрудников, пациентов и других членов нашего сообщества», - заявляют официальные лица.

Хотя правительство провинции заявляет, что планирует предложить жертвам мониторинг кражи кредитов или личных данных, оно еще не сделало этого. Вместо этого официальные лица до сих пор возлагают бремя на жертв: «Если вы заметили необычную активность в каких-либо счетах или выписках по своим счетам, пожалуйста, как можно скорее обратитесь к соответствующему поставщику услуг, например, в ваш банк», - говорят они.

Сбои в хирургии, химиотерапия

Атака привела к постоянным сбоям в обслуживании в дополнение к раскрытым данным. Провинция состоит из четырех региональных органов здравоохранения, хотя данные не были украдены у всех из них: Western Health - данные не были украдены, Central Health - данные неясны, Eastern Health - данные раскрыты за 14 лет, и Labrador- Гренфелл - данные за 9 лет раскрыты.

Официальные лица говорят, что они пытаются восстановить системы из резервных копий, и что этот процесс продолжается и еще не завершен.

Например, в четверг общественная телекомпания CBC сообщила, что, хотя больница Центра медицинских наук в городе Сент-Джонс восстановила свою систему Meditech, которая обрабатывает информацию о здоровье пациентов и финансовые данные, она включала только информацию, полученную до атаки.

Каждый орган здравоохранения публикует свои собственные обновления о продолжающихся сбоях, с которыми он продолжает сталкиваться.

По крайней мере, в среду, например, Western Health отметила, что будут продолжаться только некоторые назначения, включая назначения химиотерапии «с ограниченными возможностями».

Кроме того, «будут проводиться только срочные и неотложные визиты для хирургии, эндоскопии, сбора крови, медицинской визуализации, амбулаторной ЭКГ и клиник переломов», - говорится в сообщении. «Western Health приложит все усилия, чтобы связаться со всеми людьми, чьи встречи продолжаются. Все остальные встречи будут перенесены».

Угроза национальной безопасности

Эксперты по безопасности заявили, что очевидная атака с использованием программ-вымогателей еще раз подчеркнула, какое влияние такое преступление может оказать на национальную безопасность, в том числе на общественное здоровье.

«Программы-вымогатели представляют собой серьезную угрозу не только для частных лиц или предприятий, но и для национальной безопасности, нашей экономики и общества», - сказал The Canadian Press консультант по кибербезопасности Брайан Хонан, возглавляющий базирующуюся в Дублине BH Consulting.

Например, в мае операция вымогателя Conti ударила по Национальной службе здравоохранения Ирландии, нарушив работу здравоохранения на несколько месяцев, несмотря на то, что ирландское правительство мобилизовало свои вооруженные силы, чтобы помочь больницам стереть и восстановить системы.

Такие группы, как Conti, иногда обещают никогда не поражать определенные типы целей, например, больницы, и, если они это сделают, предоставить «бесплатный дешифратор». Но эксперты говорят, что, как и все преступники, злоумышленники, использующие программы- вымогатели, регулярно лгут. Кроме того, исправление систем, которые криптоблокируются вредоносными программами, в идеале путем их очистки и восстановления, может быть дорогостоящим и длительным процессом.

Учитывая эту угрозу, некоторые правительства стали более агрессивно противодействовать ей…». ***(Mathew J. Schwartz. Hackers Disrupt Canadian Healthcare and Steal Medical Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/hackers-disrupt-canadian-healthcare-steal-medical-data-a-17881). 10.11.2021).***

***

«Новая шпионская кампания позволила неизвестному злоумышленнику получить доступ к данным, включая средства связи и услуги, на тысячах устройств, принадлежащих южнокорейцам, сообщает Азим Ясвант, аналитик вредоносного ПО для Android из компании Zimperium, занимающейся мобильной безопасностью.

Злоумышленники использовали шпионское ПО под названием PhoneSpy на мобильных устройствах жертв в рамках текущей кампании, отмечает в своем блоге группа исследования мобильных угроз Zimperium, zLabs.

Zimperium заявляет, что уведомила и предоставила все неотредактированные данные исследований соответствующим властям США и Южной Кореи.

Мотив атаки может включать шпионаж и кражу интеллектуальной собственности с целью использования личной информации для выкупа и фишинга, говорит бывший аналитик ЦРУ по киберугрозам Роза Смотерс, старший вице-президент по кибероперациям в компании по безопасности KnowBe4.

«Тот факт, что он ориентирован на граждан Южной Кореи - конечно, их северный сосед является очевидным подозреваемым», - сказала она ISMG.

Шпион в твоем телефоне

По словам Ясванта, PhoneSpy, хотя и похож на шпионское ПО Pegasus от NSO Group с точки зрения возможностей, которые оно предоставляет злоумышленникам, не использует уязвимости в мобильных устройствах или операционных системах, и его также нет в магазинах приложений для Android, включая сторонние или региональные магазины. «Злоумышленники используют методы распространения, основанные на перенаправлении веб-трафика или социальной инженерии», - говорит он.

По словам исследователей, PhoneSpy - это усовершенствованный троян для удаленного доступа, который подключен к командному серверу, от которого он получает все свои команды выполнения. Исследовательская группа выявила 23 приложения, несущие вредоносное ПО, замаскированное под приложения, предлагающие такие услуги, как потоковая передача ТВ, управление фотографиями и обучение йоге, добавляют они.

По словам исследователей, в большинстве приложений, обнаруженных исследователями, приложение запрашивает разрешения после установки и открывает фишинговую страницу, которая имитирует страницу входа в популярное южнокорейское приложение для обмена сообщениями KakaoTalk, чтобы украсть учетные данные.

По словам исследователей, злоумышленники используют KakaoTalk, потому что функция единого входа платформы может использоваться для входа в другие службы в Южной Корее. «Таким образом они получают доступ к большинству других приложений и соответствующих данных», - добавляет Ясвант.

По словам Ясванта, злоумышленники могут использовать доступ к:

Эксфильтровать данные, включая электронные письма и другую конфиденциальную информацию;

Извлечь полный список установленных приложений и украсть учетные данные с помощью фишинга;

Запись или прямая трансляция видео или аудио;

Просмотр SMS-сообщений, включая сообщения двухфакторной аутентификации;

Отправлять SMS-сообщения как владелец устройства;

Редактировать контактную информацию в адресной книге;

Включите переадресацию звонков на любой номер или устройство, которое выберет злоумышленник;

Просмотр GPS-местоположения устройства.

Исследователи отмечают, что все команды эксфильтрации и выполнения отправляются сервером C&C, который также имеет веб-интерфейс и защищен механизмом аутентификации с использованием учетных данных. Всего существует 33 различные команды и соответствующие действия, добавляют они.

Например, команда 33 отправляет на устройство фишинговый URL-адрес, как показано на изображении ниже, а PhoneSpy загружает страницу. Учетные данные, введенные в эти формы, отправляются обратно на сервер C&C, где они хранятся без ведома пользователей, говорят исследователи.

Команда Zimperium сообщает ISMG, что она неоднократно сообщала об узле C&C сервера и предлагала властям помощь в отключении вредоносных сервисов.

Последствия сбора данных

По словам исследователей, злоумышленники, ответственные за PhoneSpy, собрали значительный объем личной и корпоративной информации о своих жертвах, включая личные сообщения и фотографии. Хотя Zimperium не смог установить прочную связь между подтвержденными жертвами, «возможность загружать списки контактов и отправлять SMS-сообщения от имени жертвы повышает вероятность того, что злоумышленники нацелятся на контакты и связи текущих жертв с помощью фишинговых ссылок», исследователи добавляют.

«Многие люди доверяют безопасности и конфиденциальности приложений чата [таких как KakaoTalk], которые обещают сквозное шифрование. Однако, когда жертва явно разрешает установку вредоносного ПО из других источников, а не из официальных магазинов приложений, и, скорее всего, обманутые на предоставление значительных разрешений в процессе, эти средства защиты шифрования, вероятно, будут обойдены, давая злоумышленникам доступ к этим разговорам», - говорит Эрих Крон, защитник осведомленности в кибербезопасной фирме KnowBe4.

«Эта информация может быть использована против жертв, чтобы вымогать у них деньги или выполнять задание для киберпреступников. Имея доступ к этим разговорам, злоумышленники могут даже вымогать деньги у людей, чьи телефоны даже не были зараженными, "он говорит ISMG.

Предупредительные меры

Zimperium перечислил индикаторы взлома и хэши SHA-256 соответствующих вредоносных приложений в своем блоге, чтобы помочь быстро идентифицировать шпионское ПО.

Люди должны больше осознавать риски предоставления абсурдно широких разрешений, запрашиваемых приложениями, говорит Крис Клементс, вице-президент по архитектуре решений в компании Cerberus Sentinel, занимающейся кибербезопасностью.

«Требуется гораздо больше согласованных кампаний по информированию пользователей об этих рисках. Ожидать, что нетехнические люди по своей сути поймут нюансы этих рисков, не имеет смысла. четкое понимание рисков, связанных с их устройствами», - сказал Клементс ISMG.

Кроме того, Google / Android могут сделать больше, чтобы подчеркнуть риск предоставления разрешений приложению, не проверенному официальными магазинами, и представить более жесткое предупреждение, когда приложение запрашивает разрешения, особенно если они кажутся слишком широкими, добавляет он». ***(Mihir Bagwe. Pegasus-Like Spyware Targets South Korean Citizens // Information Security Media Group, Corp. (https://www.govinfosecurity.com/pegasus-like-spyware-targets-south-korean-citizens-a-17882). 10.11.2021).***

***

«Robinhood, самая популярная торговая платформа на основе приложений для непрофессиональных инвесторов, подтвердила, что на прошлой неделе произошла утечка данных, которая потенциально скомпрометировала миллионы имен и адресов электронной почты. Похоже, что злоумышленники могли преследовать несколько избранных учетных записей,

однако, поскольку платформа сообщает, что дополнительная контактная информация была раскрыта для 310 ее клиентов.

Утечка данных имеет ряд сходств с взломом Twitter в 2020 году, начиная с использования социальной инженерии, чтобы убедить сотрудника Robinhood предоставить доступ к системам обслуживания клиентов.

Торговую платформу вымогали после того, как злоумышленник получил доступ по телефону

В сообщении в блоге Robinhood говорится, что утечка данных произошла 3 ноября. Торговая платформа утверждает, что злоумышленнику были раскрыты адреса электронной почты примерно пяти миллионов человек и полные имена другой группы из примерно двух миллионов человек. Более ограниченное количество клиентов, около 310 человек, получили дополнительную личную информацию из своих регистрационных профилей (например, дату рождения и почтовый индекс).

Торговая платформа сообщила, что около 10 клиентов предоставили «более обширную» информацию, но не уточнила. Тем не менее, в начале поста говорилось, что номера социального страхования и финансовых счетов не были раскрыты ни в одном из этих случаев.

Гэри Гардинер, руководитель отдела безопасности APAC и Японии Check Point Software, подробно описывает риски, с которыми пользователи Robinhood могут столкнуться в результате этой утечки данных: «Утечка информации является конфиденциальной и плохой новостью для сообщества Robinhood. Вредоносные хакеры могут использовать просочившуюся информацию для проведения дополнительных атак на жертв, таких как целевые фишинговые электронные письма, поскольку имена и даты рождения часто могут использоваться для проверки личности человека. Мы призываем пользователей Robinhood немедленно изменить свои пароли, включить двухфакторную аутентификацию и следить за любыми подозрительными электронными письмами в своих почтовых ящиках. Согласно нашему исследованию, в этом году 58% вредоносных файлов в США были доставлены по электронной почте».

Как и в случае с утечкой данных в Twitter в прошлом году, атака началась со звонка в службу поддержки клиентов, который был расширен (неуказанными способами) для доступа к некоторым системам поддержки клиентов торговой платформы. Robinhood сообщает, что злоумышленник сразу же попытался вымогать их после получения доступа, и в это время они наняли охранную фирму Mandiant, чтобы помочь с исправлением ситуации. Торговая площадка также сообщила, что к этому причастны правоохранительные органы.

Сообщение в блоге Robinhood не указывало конкретно, были ли миллионы записей успешно удалены злоумышленником, или у них просто был доступ к этому количеству во время окна утечки данных. Торговая платформа заявила, что требование о вымогательстве поступило после того, как нарушение было зафиксировано, и что она будет уведомлять всех затронутых лиц. Robinhood предлагает многофакторную аутентификацию, но до утечки данных она не была включена по умолчанию.

Нарушение данных усугубит проблемы Robinhood в 2021 году; социальная инженерия поражает другую важную платформу

Хотя большинство из семи миллионов человек, затронутых утечкой данных Robinhood, не увидят значительного риска от ограниченной информации, которая была получена, им следует ожидать последующих атак, которые, по всей видимости, исходят от торговой платформы.

Утечка данных также завершает тяжелый год для Robinhood, который начался с того, что в начале 2021 года он сыграл центральную роль в продвижении акций GameStop, что значительно превысило ожидания ритейлера видеоигр. Некоторые пользователи обвинили торговую платформу в том, что они встали на сторону институциональных инвесторов и замедлили или остановили торговлю, когда хедж-фонды должны были слишком много потерять от розничных инвесторов, которые скоординировали свои действия с целью «кратковременного сжатия»; В сентябре против Robinhood был подан иск на 10 миллиардов долларов, и внутренние электронные письма, которые появились во время процесса обнаружения, указывают на то, что торговая платформа может быть в некоторых проблемах.

В июне компания получила самый крупный штраф, когда-либо наложенный Управлением по регулированию финансовой отрасли, в общей сложности 57 миллионов долларов США плюс более 12 миллионов долларов США в виде прямых возмещений клиентам из-за того, что они не сообщили о жалобах клиентов в агентство, а также из-за многочисленных случаев показа клиентам неправильных сведений. информация в приложении (например, неверный отрицательный остаток денежных средств). Ранее в этом году торговая платформа подала частный иск из-за связанных проблем со счетом, когда молодой трейдер покончил с собой, ошибочно полагая, что он потерял 730 000 долларов на сделке, и что он смог связаться с любым сотрудником компании, чтобы обсудить ее.

У Mandiant не было идентификационной информации о злоумышленнике, стоящем за взломом Robinhood, но заявили, что это был тот, кого они опознали по аналогичной деятельности в последние месяцы. Фирма ожидает от преступника дальнейших действий.

В течение прошлого года программы-вымогатели были в заголовках газет, поскольку атаки блокируют критически важную инфраструктуру на несколько дней, но социальная инженерия стала отправной точкой для некоторых громких инцидентов. Самой крупной из них была атака на Твиттер в июле 2020 года, совершенная подростками, стремящимися завладеть крупными учетными записями и запустить мошенничество с криптовалютой. Twitter не раскрыл подробных сведений о том, как произошла утечка данных, но подтвердил, что «небольшое количество» сотрудников было настроено на социальную инженерию по телефону и предоставило злоумышленникам доступ к административным инструментам, которые обеспечивали практически неограниченный доступ к учетным записям пользователей; даже многофакторную аутентификацию можно было обойти.

Джош Явор, CISO из Tessian, отмечает, что социальную инженерию нельзя упускать из виду как путь входа, особенно когда представители службы поддержки клиентов имеют доступ к внутренним административным инструментам, которые могут поставить под угрозу всю платформу: «Это напоминание о том, что люди с

внешними ролями, такими как Служба поддержки клиентов, продажи и набор персонала нуждаются в дополнительной поддержке со стороны служб безопасности, поскольку они обязаны общаться с незнакомцами в рамках своей повседневной работы, а также имеют доступ к конфиденциальным данным о бизнесе и клиентах. Мы можем ожидать, что злоумышленники будут продолжать нацеливаться на людей, занимающих эти должности, и вкладывать средства в более изощренные меры социальной инженерии, чтобы получить привилегированную точку опоры в организациях, на которые они нацелены. Компаниям следует пересмотреть свои процессы, чтобы убедиться, что есть адекватная проверка, когда люди пишут или звонят,

Эрих Крон, защитник осведомленности о безопасности в KnowBe4, добавляет некоторые мысли о том, как обучить сотрудников распознавать эти попытки и справляться с ними: «Злоумышленники, стоящие за этими атаками, часто высококвалифицированы и очень убедительны, когда получают потенциальную жертву на линии. К сожалению, технология не способна остановить эти атаки, поэтому лучшая защита от этих попыток - образование и обучение. Сотрудники должны быть обучены обнаруживать и сообщать о атаках социальной инженерии и фишинга с помощью коротких целевых учебных модулей, а организации должны иметь политику, указывающую сотрудникам, как сообщать об этих атаках».

OneLogin считает, что даже компаниям, которые уже проводят тренинги по предотвращению попыток социальной инженерии, необходимо активизировать и совершенствовать свои усилия: «Обучение кибербезопасности должно происходить более одного раза в год в форме самостоятельного онлайн-обучения. Его необходимо распространять в течение года - проводить учения, рассылать поддельные фишинговые электронные письма, попросить кого-нибудь вытащить USB-накопители, использовать эти типы тактик, чтобы научить сотрудников, с чем они могут столкнуться, за что им следует быть начеку и как для обработки различных сценариев. Большинство людей лучше всего учатся на практике. В качестве второй формы защиты сотрудники должны быть ограничены в том, к чему они имеют доступ. Принципы минимального доступа следует применять везде, особенно когда речь идет о данных о клиентах. Таким образом, если злоумышленник сможет обойти сотрудника и обмануть его, то, к чему он будет иметь доступ, будет ограничен». ***(SCOTT IKEDA. Data Breach of Robinhood Trading Platform Blamed on Social Engineering, Similar to 2020 Twitter Breach // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/data-breach-of-robinhood-trading-platform-blamed-on-social-engineering-similar-to-2020-twitter-breach/). 15.11.2021).***

***

«По мере того, как операции на спортивных стадионах становятся все более зависимыми от центров обработки данных и онлайн-сетей, а показатели производительности и данные о состоянии здоровья спортсменов становятся более уязвимыми для незаконного воздействия или изменения, индустрия соревновательных видов спорта стоимостью 80 миллиардов долларов становится все более уязвимой для кибератак. Как и многие другие

предприятия в разных отраслях, они генерируют большие деньги и большие данные, и оба эти направления являются основными целями для хакеров.

Меньше бдительности, больше атак

За последние полтора года во многих отраслях промышленности наблюдался рост киберугроз и атак из-за использования более географически рассредоточенной рабочей силы и уязвимостей распределенных сетей. Однако теперь, когда такие вертикали, как спорт и развлечения, возвращаются, уязвимости становятся все более критическими. Атаки веб-приложений и атаки типа «отказ в обслуживании» подвергаются все более высокому количеству бит в секунду в спортивной индустрии, при этом атаки социальной инженерии также становятся все более заметными. Злоумышленники стараются отвлечь внимание аудитории во время этих спортивных мероприятий - пользователи теряют бдительность и редко ставят под сомнение подлинность электронных писем или веб-страниц, к которым они могут получить доступ во время просмотра игры или мероприятия.

Кризис подпитывает киберпреступность

Контент в индустрии спорта и развлечений настолько популярен, насколько это возможно. Таким образом, он представляет собой привлекательную цель для киберпреступников и хактивистов, стремящихся монетизировать его или получить известность за счет утечки данных. Социальные сети имеют решающее значение для того, чтобы помочь талантам взаимодействовать с поклонниками, а бренды - в создании сообществ для проведения маркетинговых кампаний. Но это также подвергает их риску взлома аккаунтов, что может серьезно подорвать репутацию компаний и звезд спорта и шоу-бизнеса. Цифровые активы, такие как потоковые порталы, сайты продажи билетов и внутренние приложения, предоставляют гораздо больше возможностей для атак для киберпреступников, хорошо разбирающихся в поиске скрытых уязвимостей.

Основное планирование безопасности для всех организаций

Обучение по вопросам безопасности жизненно важно для снижения воздействия фишинга, повышения безопасности паролей и сведения к минимуму рисков, связанных с использованием общедоступного Wi-Fi. Многофакторная аутентификация (MFA)дополнительно поможет защитить учетные записи сотрудников и талантов, как внутренние, так и в социальных сетях или публичных платформах. Политики доступа с наименьшими привилегиями гарантируют, что люди могут получить доступ только к тому, что им нужно для выполнения своей работы, и ничего более, закрывая больше возможностей для атак. Безопасность конечных точек необходима для защиты домашних или удаленных сотрудников. Регулярное тестирование на проникновение и быстрое исправление любых обнаруженных уязвимостей, особенно в веб-приложениях, еще больше уменьшат поверхность атаки. Соответствующие меры безопасности на предприятии требуются в сети, на гибридном облачном сервере, конечной точке, а также через электронную почту или веб-шлюзы.

Выявление уязвимостей позволяет организации исправлять слабые места до того, как хакер сможет их использовать. Результаты теста на проникновение могут помочь в управлении бюджетом на безопасность и расстановке приоритетов в расходах; Тестирование на проникновение - это лучшая практика не зря. Пора

перестать откладывать это и начать думать о будущем своего бизнеса. В связи с ростом числа хакерских атак и других киберпреступлений все компании должны серьезно относиться к кибербезопасности. Защита систем, сетей и устройств имеет важное значение в гонке против киберпреступности.

Любая организация, у которой нет выделенной ИТ-группы, также может извлечь выгоду из управляемых решений кибербезопасности, будь то оценка уязвимостей, предотвращение и защита вашего бизнеса от атак или обнаружение и реагирование на них. Инвестирование в эти экспертные услуги может обеспечить душевное спокойствие и свести к минимуму риски для вашей операционной, информационной и технологической инфраструктуры. Они также позволяют вашим сотрудникам сосредоточиться на основных обязанностях.

Учитывая заголовки новостей о программах- вымогателях, ваша лучшая защита от программ-вымогателей - это полный план реагирования на инциденты. Сказать, что программа-вымогатель вызывает технические трудности, - значит ничего не сказать. Без надлежащей подготовки атака может привести к полной остановке вашего бизнеса и поставить под угрозу вашу критически важную информацию. К счастью, атак программ-вымогателей можно избежать и сдержать, следуя основным методам обеспечения безопасности и аварийного восстановления.

Цифровая трансформация и опора на технологии

Спортивные организации, как и любой другой бизнес, полагаются на технологии, большинство из которых инвестируют в веб-сайты, несколько учетных записей в социальных сетях, доступ к электронной почте, облачные серверы, онлайн-банковские счета и базы данных, а также цифровые технологии для модернизации своих предложений. Основные кибератаки, от которых спортивные организации должны защищаться, - это компрометация корпоративной электронной почты, фишинговые атаки, мошенничество и кампании вымогателей, используемые для отключения систем критических событий и стадионов - четверть вредоносных атак, нацеленных на спортивные организации, как утверждается, связаны с программами-вымогателями.

Кибербезопасность - важный фактор практически для каждого бизнеса, независимо от отрасли.

Цель обеспечения безопасности организации - это обеспечение надежного обслуживания клиентов, операционное превосходство, цифровая трансформация и цифровая устойчивость. Кибербезопасность - это командный вид спорта». ***(Bindu Sundaresan. Cybersecurity for Sports and Entertainment // Techstrong Group Inc. (https://securityboulevard.com/2021/11/cybersecurity-for-sports-and-entertainment/). 15.11.2021).***

***

«Согласно недавнему отчету компании ESET, занимающейся кибербезопасностью, с момента вступления в силу в мае 2018 г. Общего регламента защиты данных (GDPR) орган по защите данных Венгрии наложил четвертое по величине количество административных штрафов в ЕС за Нарушения GDPR.

Согласно отчету ESET, общее количество штрафов в ЕС превысило 650 на общую сумму более 280 миллионов евро. Самый крупный штраф до сих пор был наложен на Amazon Europe Core S.a RL в Люксембурге (746 миллионов евро - не включены в общую сумму, поскольку она оспаривается в суде).

Венгрия занимает четвертое место после Испании, Италии и Румынии с 43 штрафами на общую сумму почти 812 000 евро. Средняя сумма штрафа в Венгрии составляет примерно 19 000 евро, и типичные причины наложения штрафов в Венгрии связаны с нарушениями GDPR, связанными с хранением данных, управлением информацией и кибербезопасностью». ***(Hungary ranks fourth on the list of European countries with the highest number of GDPR fines // KINSTELLAR (https://www.kinstellar.com/insights/detail/1553/hungary-ranks-fourth-on-the-list-of-european-countries-with-the-highest-number-of-gdpr-fines). 10.11.2021).***

***

«Ниже приводится краткое изложение судебного решения, вынесенного Верховным судом 10 ноября 2021 г. по делу Ллойд против Google LLC [2021] UKSC 50 как потенциально одного из наиболее важных и ожидаемых на сегодняшний день решений о конфиденциальности данных.

Ключевые выводы

Представительский иск может быть предъявлен по искам о нарушении законодательства о защите данных, но только для установления ответственности. Любые убытки должны рассматриваться отдельно в рамках группового иска или индивидуальных претензий.

Ущерб не возмещается за простую «потерю контроля» над личными данными после нетривиального нарушения Закона о защите данных 1998 года (DPA 1998), даже если имело место неправомерное использование частной информации. Ущерб может быть присужден только в том случае, если субъект данных понес материальный ущерб в той или иной форме, например, финансовый убыток или бедствие.

Если бы убытки от потери контроля были доступны, иск г-на Ллойда не мог бы быть подан в качестве представительного иска, поскольку все равно было бы необходимо оценить степень предполагаемого неправомерного использования данных в каждом отдельном случае.

Фон

Этот длительный судебный процесс в английских судах касался обходного пути Google Safari, который, как утверждалось, в 2011-2012 годах обходил настройки конфиденциальности и позволял Google отслеживать интернет-активность миллионов пользователей Apple iPhone и использовать собранные таким образом данные для в коммерческих целях без ведома и согласия пользователей. Это якобы позволило Google собирать или выводить информацию, касающуюся привычек и местоположения пользователей в Интернете, их интересов, возраста, пола и другой личной информации, а затем предлагать групповые ярлыки подписывающимся рекламодателям для целевого маркетинга.

В 2012 году Google согласился выплатить гражданский штраф в размере 22,5 миллиона долларов США для урегулирования обвинений, предъявленных

Федеральной торговой комиссией США на основании обвинений, а затем 17 миллионов долларов США для урегулирования исков потребителей, возбужденных против него в Соединенных Штатах.

В Англии и Уэльсе три человека подали в суд на Google в июне 2013 года, выдвинув те же обвинения и потребовав компенсации в соответствии с Законом о защите данных 1998 года (DPA 1998) и в связи с неправомерным использованием частной информации. После спора о юрисдикции эти претензии были урегулированы до того, как Google выступил в защиту.

В настоящем иске истец, г-н Ллойд, не просто требовал возмещения убытков от своего имени. Скорее, он утверждал, что представляет каждого из 4 миллионов или около того пользователей iPhone, проживающих в Англии и Уэльсе в соответствующее время, чьи данные были получены Google без их согласия. В отличие от США (и других юрисдикций, таких как Канада и Австралия) коллективные иски, как правило, не разрешены, за исключением ограниченных обстоятельств в определенных областях. Г-н Ллойд попытался преодолеть эту трудность с помощью репрезентативной процедуры. Это позволяет подавать иск одним или несколькими лицами (в качестве других представителей), которые имеют «одинаковые интересы» в иске. Мистер. Ллойд согласился с тем, что эту процедуру нельзя использовать для требования компенсации от имени других пользователей iPhone, если компенсация, которую может взыскать каждый пользователь, должна оцениваться индивидуально. Он утверждал, что в такой индивидуальной оценке нет необходимости, поскольку компенсация может быть присуждена за «потерю контроля» над личными данными без необходимости доказывать, что истец понес какие-либо финансовые потери или психические расстройства в результате нарушения в форме «униформы». сумма »в размере 750 фунтов стерлингов (чуть более 1000 долларов США) без необходимости расследовать какие-либо обстоятельства, характерные для их конкретного дела. Умноженное на количество людей, которых, как утверждал Ллойд, представлял, это дало бы компенсацию ущерба в размере порядка 3 миллиардов фунтов стерлингов (чуть более 4 миллиардов долларов США). Он утверждал, что в такой индивидуальной оценке нет необходимости, поскольку компенсация может быть присуждена за «потерю контроля» над личными данными без необходимости доказывать, что истец понес какие-либо финансовые потери или психические расстройства в результате нарушения в форме «униформы». сумма »в размере 750 фунтов стерлингов (чуть более 1000 долларов США) без необходимости расследовать какие-либо обстоятельства, характерные для их конкретного дела. Умноженное на количество людей, которых, как утверждал Ллойд, представлял, это дало бы компенсацию ущерба в размере порядка 3 миллиардов фунтов стерлингов (чуть более 4 миллиардов долларов США). Он утверждал, что в такой индивидуальной оценке нет необходимости, поскольку компенсация может быть присуждена за «потерю контроля» над личными данными без необходимости доказывать, что истец понес какие-либо финансовые потери или психические расстройства в результате нарушения в форме «униформы». сумма »в размере 750 фунтов стерлингов (чуть более 1000 долларов США) без необходимости расследовать какие-либо обстоятельства, характерные для их конкретного дела. Умноженное на количество

людей, которых, как утверждал Ллойд, представлял, это дало бы компенсацию в размере порядка 3 миллиардов фунтов стерлингов (чуть более 4 миллиардов долларов США).

Поскольку Google является корпорацией штата Делавэр, г-ну Ллойду требовалось разрешение английского суда для подачи формы иска в Google за пределами юрисдикции. Google оспорил это на том основании, что у иска не было реальных шансов на успех, поскольку: (1) убытки не могут быть присуждены в соответствии с DPA 1998 за «потерю контроля» над данными без доказательств того, что это вызвало финансовый ущерб или бедствие; и (2) претензия в любом случае не подходит для рассмотрения в качестве представительского действия.

Решение Верховного Суда

Верховный суд вынес решение в пользу Google по основным вопросам, кратко изложенным ниже.

Возможность требовать возмещения убытков в представительском иске ограничена.

Лорд-судья Леггатт постановил, что представительный иск был законным средством удовлетворения малоценных претензий, касающихся прав потребителей. Однако возможность требовать возмещения убытков в представительном иске была ограничена компенсационным характером убытков как средства правовой защиты по общему праву, учитывая, что убытки обычно требуют «индивидуальной оценки, которая не вызывает общих проблем и не может быть справедливо или эффективно проведена без участие в судебных разбирательствах соответствующих лиц». Этого нельзя было добиться репрезентативным действием.

Однако репрезентативный иск мог быть использован для установления того, нарушал ли Google DPA 1998, и, если это так, можно было запросить заявление о том, что любой член представляемого класса, которому был причинен ущерб в результате нарушения, имел право на выплаченная компенсация. Затем отдельные лица будут добиваться возмещения убытков отдельно, путем индивидуальной оценки на основе их собственных обстоятельств. Хотя требование г-на Ллойда могло быть выдвинуто с использованием этого раздвоенного (двухэтапного) процесса, это не был принятый подход.

Никаких убытков за потерю контроля

Лорд Леггатт считал, что, хотя представительный иск мог включать иск о возмещении ущерба, когда все представленные члены класса понесли одинаковые убытки, например, если все они были переплачены на одинаковую сумму, такие ситуации были редкостью.

Г-н Ллойд попытался доказать, что все члены класса понесли одинаковую потерю из-за нетривиального нарушения их прав как субъектов данных, и что это дало начало праву на компенсацию за «потерю контроля» над личными данными. Он стремился установить новое правовое основание, расширив принципы, установленные в предыдущих делах (в частности, Gulati v MGN Ltd [2017] QB 149), которые применимы к оценке ущерба за деликт от неправомерного использования частной информации в общем праве, до оценки компенсация в соответствии с разделом 13 (1) DPA 1998. Он утверждал, что «ущерб» выходит за рамки материального ущерба и включает в себя как бедствие, как было решено в деле

Видал-Холл против Google Inc [2016], так и «потерю контроля» над личными данными (пункт 108).

Верховный суд признал, что ущерб, нанесенный «потерей контроля», был нанесен в результате правонарушения, связанного с неправомерным использованием частной информации (после Gulati v MGN). Однако он постановил, что такие убытки не были доступны в соответствии с DPA 1998. Раздел 13 требовал «доказательства материального ущерба или бедствия всякий раз, когда контролер данных совершает нетривиальное нарушение любого требования Закона в отношении любых личных данных, из которых это субъект - это человек». Таким образом, Верховный суд отклонил аргумент г-на Ллойда, посчитав его принципиально несовместимым с формулировкой статьи 13, учитывая, что законодательство ЕС (действовавшее на момент подачи иска) не давало оснований для придания более широкого значения термину «ущерб». 'в этом разделе, чем было указано Апелляционным судом в иске о неправомерном использовании частной информации вВидаль-Холл против Google. Раздел 13 не может быть разумно истолкован как предоставление права на компенсацию субъекту данных за любое нетривиальное нарушение со стороны контроллера данных без требования к субъекту данных доказывать (i) нарушение; и (ii) нарушение причинило материальный ущерб или страдания заинтересованному лицу.

Поскольку действия и бездействие, послужившие основанием для претензий, произошли в 2011 и 2012 годах, они предшествовали Общему регламенту ЕС по защите данных (GDPR) и регулировались UK DPA 1998 года, который реализовал предыдущую Директиву ЕС о защите данных. Хотя стороны ссылались на GDPR, Верховный суд отказался принять это во внимание при толковании соответствующих положений. Тем не менее, раздел 13 DPA 1998 и статья 82 GDPR (в которой излагаются права субъектов данных на компенсацию и ответственность контроллеров данных) в принципе схожи. Следовательно, аналогичного результата можно ожидать в будущих делах в соответствии с GDPR Великобритании.

Потребность в индивидуальных доказательствах неправомерного использования

Верховный суд установил, что даже если бы убытки «потеря контроля» были доступны в соответствии со статьей 13, представительный иск был бы недопустимым, потому что «все равно было бы необходимо установить степень незаконной обработки в его или ее индивидуальном деле.»

Следующие факторы были приведены в качестве примеров необходимых соображений при количественной оценке убытков (если таковые имеются), которые должны быть присуждены:

Период времени, в течение которого Google отслеживал историю посещений пользователем Интернета.

Количество данных, которые были обработаны незаконно.

Была ли какая-либо незаконно обработанная информация конфиденциальной или частной.

Использование Google информации и коммерческая выгода (если таковая имеется), полученная Google от такого использования.

(1) Требование "наименьшего общего знаменателя"

Г-н Ллойд утверждал, что можно определить «неснижаемый минимальный ущерб», понесенный каждым членом класса, для которого может быть предоставлена единообразная сумма убытков (называемая «наименьшим общим знаменателем» всех индивидуальных требований). Даже при предположении, что представленные лица не будут ущемлены индивидуально в связи с требованием представителя только о минимальной части компенсации, которую могут потенциально потребовать лица, Верховный суд счел такой подход проблематичным. Если бы никакие индивидуальные обстоятельства не принимались во внимание, то предполагаемых фактов было бы недостаточно для установления того, что любой член группы имел право на возмещение ущерба. Так было бы, даже если бы не было необходимости доказывать какой-либо материальный ущерб или страдания физическому лицу.

(2) Факты, общие для каждого отдельного случая

Верховный суд постановил, что факты, выдвинутые против Google, в целом не могут свидетельствовать о том, что какое-либо лицо будет иметь право на компенсацию. Чтобы установить право лица на возмещение ущерба, необходимо, как минимум, показать, что в отношении этого конкретного лица имела место незаконная обработка. Недостаточно просто установить, что каждый заявитель является членом класса, продемонстрировав, что у соответствующего лица был iPhone с соответствующей версией интернет-браузера Apple Safari, который в соответствующий момент участвовал в рекламной службе Google DoubleClick.

Если бы в разделе 13 имелась какая-либо форма «ущерба», такой ущерб нельзя было бы охарактеризовать как более чем незначительный. Что придало этому иску видимость существа, так это утверждение о том, что Google в течение нескольких месяцев тайно отслеживал интернет-активность миллионов пользователей Apple iPhone и использовал полученные данные в коммерческих целях. Но, как постановил Верховный суд, истец пытался взыскать убытки, не пытаясь доказать, что это утверждение было правдой в отношении какого-либо конкретного лица и, следовательно, не мог переступить порог для присуждения компенсации за ущерб. Это произошло потому, что истец, чтобы подать иск в качестве представителя о возмещении ущерба, оцениваемого снизу вверх, сознательно решил не полагаться на какие-либо факты об интернет-активности любого отдельного пользователя iPhone, помимо тех фактов, которые были тогда представлены в класс.

(3) Убытки пользователей на основе наименьшего общего знаменателя

Верховный суд также отклонил иски о возмещении ущерба, присуждаемые на основе пользователей - плату, которую каждый член класса мог бы разумно взимать или согласовал бы в ходе гипотетических переговоров. Он заявил, что целью присуждения компенсации пользователю является компенсация истцу за неправомерное использование актива, защищенного нарушенным правом. Отправной точкой для оценки является определение масштабов неправомерного использования. Только после этого можно оценить, какая сумма денег могла быть разумно взыскана за такое использование или, другими словами, за освобождение правонарушителя от обязанностей, которые он нарушил при неправомерном использовании актива.

По утверждению г-на Ллойда, это могло быть достигнуто путем оценки гипотетической платы за лицензию на размещение файла cookie DoubleClick Ad на телефоне отдельного пользователя в качестве стороннего файла cookie и без освобождения Google от обязательств не собирать и не использовать какие-либо файлы. информация об истории этого человека в Интернете. Верховный суд придерживался мнения, что такая лицензия будет «бесполезной и что сбор, который может быть разумно начислен или согласован за нее, будет равен нулю».

Таким образом, Верховный суд не разрешил г-ну Ллойду подавать иски против Google за пределами юрисдикции судов Англии и Уэльса, фактически завершив рассмотрение его иска.

Подразумеваемое

Это очень важное решение для Google не в последнюю очередь из-за количества субъектов данных и потенциального ущерба. Это имеет более широкие последствия для всех контроллеров данных, особенно когда они сталкиваются с потенциальными претензиями в результате утечки данных. Истцы часто утверждают, что потеря контроля над своими личными данными достаточна сама по себе, не указывая подробностей любого ущерба в виде финансовых потерь или бедствий. Эти претензии в настоящее время имеют гораздо меньше шансов на успех, поскольку утверждение о нарушении Закона о защите данных 2018 года представляется чрезвычайно сложной задачей. Кроме того, в соответствии с ранее вынесенным в июле 2021 года решением Высокого суда Англии по делу Уоррен против DSG Retail Ltd, объем исков, основанных на злоупотреблении доверием, неправомерное использование частной информации и халатность (которые часто объединяются с исками о нарушении GDPR и законодательства Великобритании о защите данных) также были значительно ограничены. Контроллеры данных, очевидно, по-прежнему несут значительную потенциальную ответственность за утечки данных, которые приводят к финансовым потерям или какой-либо форме бедствия, но есть некоторое утешение в том, что простой факт нарушения не обязательно приведет к автоматическим выплатам». ***(Huw Beverley-Smith, Paige Izquierdo. UK Supreme Court Rules in Google's Favor in Data Privacy Group Litigation with Major Implications for Data Breach Cases // Faegre Drinker Biddle & Reath LLP. (https://www.faegredrinker.com/en/insights/publications/2021/11/uk-supreme-court-rules-in-googles-favor-in-data-privacy-group-litigation-with-major-implications-for). 15.11.2021).***

***

«Злоумышленники использовали вредоносные электронные письма, чтобы атаковать более 125 человек с известными учетными записями TikTok, пытаясь украсть информацию и заблокировать их.

Недавно обнаруженный фишинговый мошенник попытался захватить более 125 известных учетных записей пользователей в TikTok. По словам исследователей, эта кампания знаменует собой одну из первых серьезных атак на «влиятельных лиц», обнаруженных на платформе социальных сетей TikTok.

Исследователи облачной службы безопасности электронной почты Abnormal Security обнаружили мошенничества, которые пытались захватить учетные записи

людей, отправляя электронные письма, выдавая себя за TikTok, и прося пользователей подтвердить свои данные для входа.

Кампания, отслеживаемая 2 октября и 1 ноября, была разослана людям по всему миру. Согласно отчету, опубликованному во вторник, подготовленному Abnormal Security, у каждой цели был большой объем учетных записей TikTok «всех видов и в разных регионах».

«Среди типичных агентств по поиску талантов и фирм-консультантов по брендам, которые мы ожидаем увидеть, этот актер отправлял сообщения в студии по производству социальных сетей, влиятельные фирмы и производителей контента всех типов», - сказала Рашель Шуинар, аналитик по анализу угроз в Abnormal Security, написал в отчете.

Игра за выдачу себя за другое лицо

Электронные письма пытались обмануть пользователей, чтобы они отправили информацию для входа в систему злоумышленникам одним из двух способов, каждый из которых требовал дальнейших действий со стороны цели. В обоих случаях злоумышленники сделали вид, что связываются с пользователями из TikTok, принадлежащего китайской компании ByteDance.

Одно из электронных писем, отправленных в рамках кампании, проинформировало пользователя о том, что его или ее учетная запись нарушила авторские права TikTok, и попросило пользователя ответить на электронное письмо, чтобы подтвердить учетную запись, пригрозив удалить учетную запись в течение 48 часов, если не будут приняты меры.

Во втором электронном письме, в котором ложно утверждается, что оно отправлено «официальными лицами TikTok», владельцы учетных записей проинформировали, что учетная запись имеет право на «проверенный значок», и попросили их ответить на это письмо, чтобы учетная запись могла быть должным образом проверена.

«Кампания охватила всех, от известных цифровых медиа-каналов до отдельных актеров, моделей и фокусников, до создателей контента по всему миру», - написал Шуинар. «Несколько электронных писем были отправлены не в ту компанию с тем же названием в той же стране, и многие из использованных адресов электронной почты, похоже, были взяты непосредственно из социальных сетей».

Связь со злоумышленниками

Исследователи повернули тактику злоумышленников против них, выдав себя за влиятельных лиц, ответив на фишинговое письмо, на которое был получен ответ электронной почты, содержащий сокращенную ссылку под названием «Подтвердить мою учетную запись», которая направила исследователей в чат в WhatsApp, объяснила она.

«В ходе разговора в WhatsApp нас попросили подтвердить номер телефона и адрес электронной почты, связанные с целевой учетной записью TikTok», - написал Шуинар.

Затем злоумышленник, выдающий себя за «должностных лиц TikTok», попросил исследователей подтвердить свое право собственности на учетную запись, предоставив шестизначный код, который они отправили, демонстрируя, как они

обходят многофакторную аутентификацию, чтобы получить доступ к учетной записи.

После этого связь со злоумышленниками прекратилась, поскольку злоумышленники, вероятно, проверили учетную запись TikTok, которую использовали исследователи, что показало, что «наша вовлеченность аудитории была ниже номинальной», - написал Шуинар. Abnormal Security пыталась найти влиятельного человека, который разрешил бы использовать его или ее учетную запись для эксперимента, но безуспешно, сказала она.

Мотив неясен

По сообщениям исследователей, в результате кампании у некоторых из них были удалены или захвачены их учетные записи, а их данные украдены. Однако, помимо этого, исследователи не видели явных мотивов для кампании, которая могла бы принести пользу злоумышленникам, пишет Шуинар.

Однако злоумышленники нередко нацелены на высокопоставленных пользователей учетных записей социальных сетей - чаще всего на людей, которые являются так называемыми «влиятельными лицами» в Instagram и Facebook, - чтобы вымогать деньги у владельцев учетных записей, чтобы вернуть их, отметила она.

«Прошлый таргетинг на учетные записи социальных сетей на других платформах предлагает несколько вариантов», - написал Шуинар. «Аккаунты в социальных сетях становятся все более ценными в последние годы, создавая стимул для выкупа их первоначальным владельцам за изрядную плату».

Пользователи Instagram действительно стали мишенью кампании угроз со стороны турецкоязычных киберпреступников, раскрытой в августе 2020 года. Злоумышленники нацелились на сотни знаменитостей, владельцев стартапов и других лиц с большим количеством подписчиков на платформе, пытаясь украсть учетные данные Instagram и электронной почты.

Этот вид деятельности стимулировал «подпольную экономику», предлагающую запрет как услугу, манипулируя механизмами сообщения о злоупотреблениях, чтобы преследовать и подвергать цензуре других пользователей, в первую очередь в Instagram, добавил Шуинар». ***(Elizabeth Montalbano. Phishing Scam Aims to Hijack TikTok 'Influencer' Accounts // Threatpost (https://threatpost.com/phishing-scam-tiktok-influencer/176391/). 17.11.2021).***

***

«Минцифры РФ планирует заняться мониторингом утечек персональных данных россиян в интернете и будет реагировать на уровне государства на каждый инцидент.

«По каждой утечке будет проводиться работа по сверке ее с базой утечек подрядчика (очень часто это старые утечки, которые перепродаются). Также будет проводиться работа по обнаружению источника утечки. При определении примерной даты утечки и места утечки с целью расследования инцидента министерство будет взаимодействовать с федеральными органами исполнительной власти (ФОИВами), откуда была зафиксирована утечка информации. Цель мероприятия - проводить мониторинг и реагировать на уровне государства на каждый инцидент", - отметили в министерстве.

Согласно данным портала госзакупок, Минцифры был опубликован тендер на сбор информации об утечках персональных данных. Начальная цена контракта - 68,3 млн рублей. Подать заявку желающие могут до 19 ноября. Как следует из техзадания, мониторинг должен проводиться на киберкриминальных форумах, в Telegram-каналах и тематических чатах, мошеннических блогах, на веб-сайтах и новостных ресурсах». ***(Минцифры займется мониторингом утечек персональных данных граждан в интернете // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5861887-Mincifry-zajmetsya-monitoringom-ute.html). 15.11.2021).***

***

«Эксперты по кибербезопасности оценивают недавнюю утечку данных GoDaddy, в результате которой были обнаружены данные 1,2 миллиона клиентов.

Взлом произошел после того, как неавторизованный человек использовал взломанный пароль для получения доступа к системам GoDaddy.

Анураг Кахол, исполнительный директор Bitglass, говорит, что из-за того, что многие интернет-пользователи имеют десятки учетных записей в различных сервисах, им стало труднее запоминать многочисленные сложные пароли.

«К сожалению, повторное использование пароля стало обычным явлением, которое увеличивает вероятность взлома учетной записи при утечке одного набора учетных данных пользователя», - говорит он.

«Более 80% взломов связаны с утерянными или украденными учетными данными, и теперь очевидно, что одних паролей недостаточно, когда дело доходит до аутентификации пользователей».

Кахол говорит, что потребители и компании должны работать вместе, чтобы обеспечить конфиденциальность корпоративных и личных данных.

«Для правильной проверки личности своих сотрудников и клиентов компании должны улучшить свои протоколы безопасности, установив непрерывную контекстно-зависимую безопасность на протяжении всего процесса входа в систему», - объясняет он.

«Такие решения, как многофакторная аутентификация (MFA) и единый вход (SSO), не требуют от пользователей запоминания множества паролей, а также снижают риск взлома учетной записи.

«На потребительском уровне пользователи могут защитить свою цифровую идентичность, узнав о рисках повторного использования паролей, следуя передовым методам кибербезопасности и оставаясь в курсе растущих угроз», - говорит Кахол.

«Поскольку сейчас мы живем в то время, когда наша повседневная жизнь вращается вокруг Интернета и наших различных учетных записей в нем, осведомленность об управлении идентификационной информацией как никогда важна.

Дэнни Лопес, исполнительный директор Glasswall, говорит, что сообщения о хакерах, получающих доступ к таким компаниям веб-хостинга, как эта, вызывают беспокойство, учитывая объем данных, хранящихся у таких компаний, и возможные последствия, если они попадут в чужие руки.

«Организациям необходимо внедрить надежные процессы для адаптации и увольнения сотрудников и аффилированных лиц, которые могут получить доступ к ключевым информационным системам», - говорит он.

«Жизненно важно контролировать привилегированный доступ и отслеживать тех, кто пользуется такими привилегиями администратора. Обеспечение применения многофакторной аутентификации везде, где это возможно, является жизненно важной защитой, когда учетные данные пользователей попадают в общественное достояние.

«Это поможет ограничить радиус взрыва и в большинстве случаев предотвратить утечку данных».

Лопес говорит, что подобные атаки демонстрируют, что традиционный подход к сетевой безопасности, основанный на замках и рвах, оставляет организации незащищенными.

«Безопасность с нулевым доверием видит мир по-другому. По умолчанию никому не доверяют, вне зависимости от того, находятся ли они внутри или вне сети», - говорит он.

«В мире, где данные могут храниться среди нескольких облачных провайдеров, критически важно усилить все процессы, связанные с проверкой доступа. Без подхода нулевого доверия организации рискуют получить свободу действий злоумышленников в сети, когда они окажутся внутри». ***(Shannon Williams. Cybersecurity experts weigh in on GoDaddy data breach // Techday Ltd (https://securitybrief.com.au/story/cybersecurity-experts-weigh-in-on-godaddy-data-breach). 23.11.2021).***

***

«…Apple подала в суд на израильскую компанию NSO Group из-за того, что она продавала программное обеспечение правительствам, которое позволяло им взламывать свои устройства и, по сути, считывать доступные данные. Сюда входят сообщения, списки контактов, любые сохраненные номера социального страхования или кредитных карт и т.д. и т.д. В общем, это вся информация, которую нельзя никому передавать без явного согласия. Apple, по сути, была компанией, которая в последнее время наделяла пользователей такой безопасностью. Функции отслеживания / прозрачности компании, запущенные с iOS 14 в 2020 году, по существу не позволили сторонним приложениям и компаниям перекачивать любые пользовательские данные без явного согласия вовлеченных пользователей. Это было встречено бурными аплодисментами со стороны пользовательской базы потребителей и, естественно, критикой со стороны таких компаний, как Meta, которые извлекают выгоду из сбора пользовательских данных.

Судебный процесс влечет за собой запрет Apple NSO Group использовать любое из ее программного обеспечения. Первый также требует от второго более 75 000 долларов США в качестве компенсации за ущерб. В официальном заявлении Apple по этому поводу говорилось, что она примет все меры против того, что по сути является вопиющей атакой на спонсируемое государством программное обеспечение, которое используется в качестве оружия против широких масс. Это не единственное нарушение законодательства, с которым NSO Group столкнулась за

последнее время. Министерство торговли США внесло в черный список NSO Group право использовать любое американское программное обеспечение в своих собственных целях. Этот конкретный бюрократический аппарат может даже помочь Apple в деле против израильской компании, поскольку это также американская компания». ***(Arooj Ahmed. Apple Is Suing Israeli Company NSO Group Over The Latter's Selling Governments Software That Can Hack Into Consumer Devices // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/apple-is-suing-israeli-company-nso.html). 25.11.2021).***

***

«Бразильская компания по разработке программного обеспечения для управления Wi-Fi оказалась в центре инцидента, в результате которого были обнаружены данные различных известных компаний и миллионов их клиентов.

Речь идет о компании WSpot, которая предоставляет программное обеспечение, которое позволяет предприятиям защищать свои локальные сети Wi-Fi и предоставлять своим клиентам беспарольный онлайн-доступ. Облучение было обнаружено исследовательской фирмой SafetyDetectives.

Исследователи обнаружили неправильно настроенную корзину S3 Amazon Web Services (AWS) WSpot, которая была оставлена открытой и предоставила общественности 10 ГБ данных. Обнаружив конфиденциальные данные 2 сентября, исследователи связались с фирмой-разработчиком программного обеспечения 7 сентября. WSpot зафиксировал нарушение на следующий день.

Исследователи отметили, что в ходе инцидента было обнаружено около 226000 файлов, включая личную информацию примерно 2,5 миллионов человек, которые подключились к общедоступным сетям Wi-Fi, предоставляемым клиентами WSpot. В клиентский портфель компании входят Pizza Hut, поставщик финансовых услуг Sicredi и медицинская фирма Unimed.

Согласно SafetyDetectives, набор раскрытой информации включал детали, предоставленные отдельными лицами для доступа к услуге Wi-Fi, предоставляемой компаниями. Это включает полное имя, адрес электронной почты, полный адрес и регистрационный номер налогоплательщика - в дополнение к учетным данным для входа, созданным в процессе регистрации.

WSpot подтвердил инцидент ZDNet, заявив, что проблема была вызвана «отсутствием стандартизации в управлении информацией [хранящейся] в конкретной папке». Бразильская компания подтвердила, что работает над решением этой проблемы с тех пор, как с ней связались по этому поводу до завершения технических процедур 18 ноября.

WSpot заявляет, что его серверы остаются нетронутыми и не подвергались вторжению злоумышленников, утверждая, что нет никаких доказательств того, что к раскрытым данным были получены киберпреступники. Однако компания, занимающаяся разработкой программного обеспечения, также заявила, что наняла охранную компанию для полного расследования любых последствий в связи с утечкой данных в результате инцидента.

WSpot заявляет, что проблема затронула 5% его общей клиентской базы, и ни у одного из ее клиентов не было скомпрометированной деловой и / или конфиденциальной информации. Кроме того, он повторил, что он не собирает финансовую информацию, такую как данные кредитной карты или учетные данные для доступа к другим службам.

Неясно, будет ли компания информировать об инциденте лиц, подвергшихся воздействию.

По словам представителя WSpot, Национальное управление по защите данных еще не связывалось по поводу инцидента, однако «все юридические вопросы, связанные с этим делом, решаются WSpot как можно тщательнее, особенно для определения следующих шагов». ***(Angelica Mari. Data from millions of Brazilians exposed in Wi-Fi management software firm leak // ZDNet (https://www.zdnet.com/article/millions-of-brazilians-exposed-in-wi-fi-management-software-firm-leak/). 22.11.2021).***

***

«…Согласно последнему отчету OAIC об утечках данных за период с января по июнь 2021 года, сектор финансовых услуг занял второе место по количеству утечек данных во всех отраслях промышленности (после сектора здравоохранения).

Важно отметить, что в отчете OAIC говорится, что, хотя человеческая ошибка была наиболее распространенным источником утечки данных в Австралии, злонамеренные или криминальные атаки были наиболее распространенным источником утечек данных в секторе финансовых услуг, на которые приходилось две трети из зарегистрированных. В секторе также зарегистрировано наибольшее количество утечек данных в результате сбоев системы.

Рост числа злонамеренных или преступных атак и роли человеческой ошибки согласуется с выводами нашего шестого ежегодного отчета о кибербезопасности «Перспективы киберрисков», согласно которым 70% всех зарегистрированных инцидентов были вызваны фишинговыми сообщениями (распространенным предшественником атак программ-вымогателей).).

В ответ на киберугрозы, с которыми сталкивается сектор финансовых услуг, регулирующие органы, включая Австралийское управление пруденциального регулирования (APRA), ввели стандарты и руководства. Они нацелены на обеспечение применения соответствующих мер безопасности для защиты конфиденциальности потребителей, а также для защиты стабильности сектора (и, в более широком смысле, экономики).

Это в дополнение к множеству нормативных актов, включая Закон о конфиденциальности 1988 г. (Cth), Закон о корпорациях 2001 г. (Cth), Закон о конкуренции и защите прав потребителей 2010 г. (Cth) и (для некоторых австралийских организаций) Общий европейский регламент защиты данных.. Дальнейшие изменения на горизонте с поправкой к законодательству о безопасности (критическая инфраструктура) и законопроектами о платежах за программы-вымогатели, которые в настоящее время находятся на рассмотрении Федерального парламента.

Поэтому сектору финансовых услуг, от исполнительного до операционного, необходимо понимать серьезную угрозу, которую представляют атаки программ-вымогателей. Организациям необходимо внедрять процессы и технологии, а также культуру безопасности, чтобы подготовить и защитить их в рамках этой быстро развивающейся нормативной базы.

На этом фоне MinterEllison недавно провел круглый стол для представителей сектора финансовых услуг, на котором была изучена «анатомия атаки программ-вымогателей». В нем приняли участие участники дискуссии Эндрю Корнелл, Эшли Джонс, Лия Муни и наш руководитель отдела кибернетики Пол Калленбах.

Группа рассмотрела, как может выглядеть типичная атака программ-вымогателей, как их предотвратить или снизить риск, и рассмотрела нормативно-правовую среду для организаций финансовых услуг, управляющих киберрисками.

Программы-вымогатели постоянно развиваются. У участников возникло несколько уместных вопросов о том, как справиться с этой продолжающейся проблемой. Ниже мы исследуем некоторые из этих вопросов.

Как развивались атаки программ-вымогателей?

Банды киберпреступников становятся все более изощренными.

Команды программ-вымогателей нацелены на гораздо более крупные организации, чем в прошлом. Это известно как «охота на крупную дичь». Кроме того, киберпреступники больше не просто блокируют данные, но и воруют их.

Еще один аспект этой эволюции - «программа-вымогатель как услуга». Бригады программ-вымогателей моделируют себя как законные компании, занимающиеся предоставлением программного обеспечения корпоративного уровня. Они создали широкие сети внештатных специалистов, что еще больше усложняет защиту от атак.

Те же киберпреступники проникают в организации, предлагая сотрудникам денежные стимулы для установки вредоносного ПО или внутреннего запуска процесса вымогательства.

Поэтому доверенные сотрудники могут представлять повышенный риск.

Каковы шансы вернуть данные организации после атаки?

Эксперты пришли к выводу, что в их совокупном опыте шансы получить данные обратно невелики.

В прошлом программа-вымогатель заключалась в блокировке компьютера и предназначалась для отдельных лиц. Выплата выкупа обычно позволяет жертве разблокировать свой компьютер. В последние несколько лет это превратилось в более изощренные атаки против юридических и физических лиц.

Появляется все больше свидетельств того, что не только атаки программ-вымогателей блокируют компьютеры людей, но и штаммы программ-вымогателей теперь обладают способностью кражи данных. Следовательно, злоумышленники используют два, а иногда и три уровня вымогательства.

Первый уровень направлен против целевой организации, которая ищет платеж для разблокировки скомпрометированной системы. Второй уровень — это попытка вымогательства с целью возврата украденных данных, включая угрозу раскрытия данных, если организации отказываются платить. И третий, наиболее неудачный

слой, направлен на людей, которых они находят в этих данных - затронутых лиц - и включает попытки вымогать их индивидуально.

В конце концов, поскольку организации имеют дело с преступниками, доверять им обязательство уничтожить данные организации - рискованное предложение.

Законно ли оплачивать запрос от вымогателя?

В Австралии в настоящее время нет специального закона, запрещающего оплату запроса на вымогательство.

Однако в законодательстве Содружества, штатов и территорий есть положения, запрещающие платежи в обстоятельствах, когда лицо проявляет неосторожность или небрежность в отношении того, будут ли деньги использоваться в качестве орудия преступления.

Например, если организация осуществляет платеж с помощью программы-вымогателя синдикату программ-вымогателей, вполне возможно, что синдикат может реинвестировать часть этих денег в свое преступное предприятие - и, следовательно, в содействие преступлению с использованием программ-вымогателей. Хотя в некоторых случаях может быть доступна защита от принуждения, в конечном итоге это серая зона.

Помимо уголовных норм, касающихся орудий преступления, выплата выкупа может также противоречить законам, запрещающим выплаты подпадающим под санкции организациям и террористическим группам.

Поэтому крайне важно, чтобы любая организация, рассматривающая вопрос о выплате выкупа, проводила надлежащую проверку организации или лица, добивающегося выплаты (что не всегда практично или возможно).

По возможности, правительство и правоохранительные органы (а также участники дискуссии) советуют не платить выкуп.

Кто принимает решение о том, платить ли выкуп?

Решение о том, платить ли выкуп, может приниматься многими людьми - членами совета директоров, руководителями и даже теми, кто не работает в организации. Также может потребоваться поговорить с третьими сторонами (например, со страховщиками), чтобы определить, может ли выплата выкупа покрываться полисом киберстрахования.

Эти соображения должны быть продуманы и задокументированы в политике платежей с использованием программ-вымогателей задолго до того, как произойдет атака с использованием программ-вымогателей, а не «на лету», когда событие разворачивается. Политика в отношении программ-вымогателей должна документировать:

возможные сценарии вымогательства, с которыми может столкнуться организация (включая различные классы уязвимых данных и систем);

общая позиция организации в отношении выплаты выкупа (с учетом финансовых, операционных и репутационных соображений);

обстоятельства, при которых организация заплатит выкуп (и максимальные суммы, которые она может заплатить, включая эскалацию и уровни полномочий).

Как защитить организации от атак программ-вымогателей?

Эксперты рекомендовали организациям вернуться к основам. Это означает обеспечение исправления компьютеров, включение многофакторной аутентификации и создание безопасной и информированной культуры безопасности в организации.

Они рекомендовали три шага, которые помогут организациям защитить себя.

Совместите с внешним каркасом

Согласуйте с внешними структурами, такими как ASD Essential Eight или NIST Cybersecurity Framework.

Организациям также следует тщательно сосредоточиться на снижении риска цепочки поставок путем проведения надлежащей комплексной проверки, аудита и улучшения договорных отношений с поставщиками.

Проводите учения по плану реагирования на утечки данных и регулярно обновляйте план

Организации должны регулярно проверять свои планы реагирования на утечки данных. У большинства организаций теперь есть план реагирования на утечки данных (80%, согласно нашему Cyber Report). Однако только 55% говорят нам, что они регулярно тестируют и обновляют свои планы.

Планы реагирования на утечки данных следует регулярно обновлять в свете быстрых изменений в ландшафте угроз и нормативных требований.

Обучать и обучать

Человеческая ошибка играет ключевую роль в подавляющем большинстве случаев утечки данных. Сотрудники нуждаются в соответствующем обучении тому, как выявлять фишинговые электронные письма и другие атаки и реагировать на них.

Каковы передовые методы реагирования на атаки программ-вымогателей?

Для организаций, ставших жертвами атаки программ-вымогателей, есть несколько важных моментов.

Рассмотрите пострадавших людей

Лучшие тематические исследования о том, как управлять кибератаками, получены от организаций, которые ставят затронутых лиц в центр расследования, а не рассматривают его как минимальное упражнение по соблюдению нормативных требований. Организации должны учитывать положение пострадавшего на всех этапах, в том числе при составлении уведомлений об утечке данных и определении возможных мер по исправлению положения.

Уведомления должны быть вовремя

Организации должны тщательно продумать время принятия решения об уведомлении. Слишком раннее уведомление - до того, как станут известны все относящиеся к делу факты - может нанести ненужный вред пострадавшим. Схема нарушения данных, подлежащая уведомлению в соответствии с Законом о конфиденциальности, направлена на минимизацию вреда для людей. Это включает в себя ущерб, связанный с уведомлением.

Привлекайте третьих лиц заранее

У организаций должен быть список прошедших предварительную проверку сторонних экспертов, с которыми они могут связаться в случае атаки программы-вымогателя и которые могут помочь организации принять объективные, беспристрастные и основанные на доказательствах решения. В случае атаки

программы-вымогателя организация должна обеспечить своевременное привлечение этих экспертов». ***(Paul Kallenbach, Leah Mooney. Is it legal to pay a ransomware demand – and other critical questions // MinterEllison (https://www.minterellison.com/articles/is-it-legal-to-pay-a-ransomware-demand-and-other-critical-questions). 17.11.2021).***

***

«Комиссия по защите персональных данных Сингапура (PDPC) оштрафовала туристическую компанию Commeasure на 74000 сингапурских долларов (54456 долларов США), которая управляет веб-сайтом бронирования путешествий RedDoorz, который раскрыл данные 5,9 миллиона клиентов - крупнейшее нарушение данных, обработанное Комиссией с момента ее создания.

PDPC объявила о наказании за «непринятие разумных мер безопасности для предотвращения несанкционированного доступа и кражи личных данных клиентов, размещенных в облачной базе данных».

RedDoorz начала свою деятельность в Индонезии, а затем переехала в Сингапур, откуда собирает данные о бронировании бюджетных отелей в избранных городах Юго-Восточной Азии. Пользователь выбирает бюджетный отель в RedDoorz по фотографиям, площади и цене, не всегда зная фактическое название или местонахождение отеля. Когда путешественник прибывает, номер в отеле переименовывается в RedDoorz и сопровождается определенными гарантированными услугами, такими как Wi-Fi, телевидение и питьевая вода.

Commeasure узнала об утечке данных его клиентов RedDoorz еще в сентябре 2020 года, когда компания по кибербезопасности из Атланты уведомила материнскую компанию о взломе и предложила услуги по исправлению положения. В течение недели туристическая компания проинформировала PDPC.

Похищенные данные включали имена, контактные телефоны, адреса электронной почты, дни рождения, зашифрованные пароли учетных записей RedDoorz и информацию о бронировании. Согласно постановлению PDPC, в базе данных не было номеров кредитных карт. Добычу выставили на продажу на хакерском форуме.

Ошибка, из-за которой были украдены данные, восходит к временам запуска компании, когда ключ доступа к AWS был встроен в пакет приложения Android (APK), общедоступный для загрузки из Google Play Store. APK, созданный в 2015 году и последний раз обновленный в январе 2018 года, был ошибочно отмечен разработчиками как «тестовый» ключ. Он оставался видимым, несмотря на то, что считался «несуществующим», пока компания не была уведомлена о нарушении в 2020 году.

Имея в руках ключ доступа к AWS, злоумышленники могут получить доступ и украсть записи клиентов, размещенные в облачной базе данных Amazon RDS. RedDoorz действительно предпринимал попытки защитить данные - например, нанимая компании по кибербезопасности и используя инструмент обфускации Java Proguard для предотвращения обратной инженерии APK - но все это было напрасно, потому что соответствующий файл никогда не оценивался…

Commeasure сообщил PDPC, что неспособность реализовать достаточно надежные процессы для управления запасами ключей доступа к инфраструктуре была связана с высокой текучестью кадров. Это не понравилось Комиссии. Тем не менее, регулирующий орган сказал, что он принял во внимание совместное поведение компании, корректирующие действия, неэффективные, но регулярные проверки безопасности и неудачные обстоятельства того, что гостиничный бизнес в разгар пандемии, когда он принял решение о финансовом наказании.

Комиссия предоставила Commeasure 30 дней для выплаты до начала выплаты процентов». ***(Laura Dobberstein. Singaporean regulator punishes biggest-ever data breach: Almost 5.9 million hotel customers' info exposed // The Register (https://www.theregister.com/2021/11/18/redoorz_fined_for_massive_data_leak/). 18.11.2021).***

***

«Согласно отчету Центра ресурсов по кражам личных данных и исследовательской компании DIG.Works, немногие потребители принимают решительные меры для защиты своей конфиденциальности и личности после получения уведомления об утечке данных.

Отчет, основанный на опросе 1050 взрослых потребителей в США, показал, что 16 процентов участников исследования не предприняли никаких действий после получения уведомления об утечке данных, затрагивающей их учетные записи. Информация из взломанных учетных записей может быть использована для мошенничества с идентификационными данными или для того, чтобы сделать работодателей уязвимыми для кибератак, включая мошенничество с использованием программ-вымогателей и компрометации корпоративной электронной почты (BEC).

Более того, менее половины участников (48 процентов) изменили пароли к учетным записям, затронутым взломом, и только 22 процента изменили все свои пароли после того, как были уведомлены об атаке.

«Когда мы спросили 16 процентов, почему они не предприняли никаких действий, когда получили уведомление об утечке данных, 26 процентов ответили, что их данные уже доступны, и они ничего не могут с этим поделать», - сказала Ева Веласкес, президент и генеральный директор ITRC, некоммерческая организация из Сан-Диего, основанная для оказания помощи жертвам кражи личных данных и просвещения потребителей.

«Но есть действия, которые они могут предпринять, в зависимости от того, какие данные были скомпрометированы, которые помогут им свести к минимуму свой риск», - сказала она TechNewsWorld. «Мы не очень хорошо объясняем это».

Невежество и апатия

Веласкес добавил, что 17 процентов потребителей, которые не действовали, когда получили уведомление о нарушении, не знали, что им делать, когда они его получили, а 14 процентов сочли переписку мошенничеством.

«Когда мы смотрим на эти причины, это позволяет нам понять, что то, как мы уведомляем людей, как мы представляем эту информацию, совершенно

неэффективно, и нам необходимо пересмотреть то, как мы информируем людей о том, что их данные были скомпрометированы в результате взлома», она сказала.

Еще 29 процентов из тех, кто не действовал в соответствии с уведомлением о нарушении, полагали, что решение проблемы должна решать организация. «Это неправда, - заметил Веласкес, - поэтому необходимо больше общаться о том, где эта ответственность начинается и заканчивается».

«Получение уведомления о том, что ваши личные данные были украдены, пугает, но, по-видимому, недостаточно, чтобы сделать что-либо существенное с этим», - пошутил Сарью Найяр, генеральный директор Gurucul, компании по разведке угроз в Эль-Сегундо, Калифорния.

«Часть этой проблемы, - сказала она TechNewsWorld, - заключается в том, что пользователи по умолчанию думают, что с их учетными записями не случится ничего плохого».

Рэй Пью, менеджер по безопасности Expel, SOC в качестве поставщика услуг в Херндоне, штат Вирджиния, согласился с тем, что незнание и апатия могут сыграть роль в игнорировании уведомлений об утечке данных.

«Некоторые пользователи могут не полностью понимать, что на самом деле означает уведомление об утечке данных и каковы последствия, - сказал он TechNewsWorld, - в то время как другие понимают масштабы, но стали безразличными к этой теме».

Растущий цинизм

Количество потребителей, игнорирующих уведомления об утечке данных, не должно вызывать удивления из-за отсутствия обучения по этому вопросу, утверждает Джеймс Маккуигган, защитник осведомленности в KnowBe4, учебном центре по вопросам безопасности в Клируотере, штат Флорида.

«Если они пострадают от взлома, большинство пользователей сочтут себя бессильными и могут не знать, с кем связаться», - сказал он TechNewsWorld.

«Без надлежащей подготовки или осведомленности - которые нелегко найти, если они не работают в организации, которая их предоставляет - многие люди не ищут эти навыки», - сказал он TechNewsWorld.

Джон Гилмор, директор по исследованиям Abine, компании, занимающейся решениями для обеспечения конфиденциальности, из Бостона, отметил, что выводы ITRC / DIG согласуются с аналогичными исследованиями, опубликованными в этом году.

«Около 85 процентов потребителей скажут, что они чрезвычайно обеспокоены конфиденциальностью в Интернете, и всегда есть 15–20 процентов, которым просто все равно», - сказал он TechNewsWorld.

Он добавил, что опросы также показывают, что конфиденциальность неуклонно снижается по мере того, как потребители переходят от осведомленности к действию. Таким образом, 85 процентов скажут, что они обеспокоены конфиденциальностью, но только 79 процентов скажут, что они готовы действовать для защиты своей конфиденциальности, и около 50 процентов фактически будут действовать в соответствии с их проблемами конфиденциальности.

Когда дело доходит до потребителей, которые активно защищают свою конфиденциальность, продолжает он, стрелка идет еще дальше: около 30 процентов.

«Люди очень скептически относятся к этим вещам», - сказал он. «Они потратят время на изменение настроек конфиденциальности, но в то же время скажут, что не думают, что это имеет большое значение».

«Это часть растущего цинизма в обществе по поводу искренности институтов делать то, что они обещают делать», - добавил он.

Как избежать замораживания кредита

Опрос ITRC / DIG также показал, что после уведомления о нарушении только три процента респондентов заявили, что они заморозили кредитование, чтобы заблокировать создание новых учетных записей, требующих проверки кредитоспособности, таких как новые кредиты, кредитные карты и другие крупные покупки.

Веласкес признал, что аккаунты не нужно замораживать при каждой утечке данных.

«Если вы являетесь участником взлома, когда имена пользователей и пароли являются данными, которые были взломаны, вашим первым шагом не должно быть замораживание вашего кредита», - сказала она. «В этом нет никакого смысла. Вашим первым шагом будет изменение ваших имен пользователей и паролей».

«С другой стороны, - продолжила она, - если номера социального страхования и все данные, необходимые для открытия нового финансового счета на ваше имя, были взломаны, то замораживание счетов должно быть выше в вашем списке дел».

Пью отметил, что потребители могут уклоняться от замораживания кредита, потому что считают его ненужным и неудобным.

«Они могут думать, что в взломе участвовали тысячи людей, и что они предпочли бы сделать ставку на то, что информация не будет использована, чтобы навредить им лично», - сказал он.

«Замораживание учетных записей может быть больше проблем, чем оно того стоит, потому что в какой-то момент вам придется вернуться и разморозить учетные записи, и с этим связана целая чушь», - добавил Гилмор.

«Большинство людей готовы бросить кости», - продолжил он. «Это не стоит времени».

Повторное использование паролей

Что касается паролей, исследователи ITRC / DIG обнаружили, что только 15 процентов респондентов утверждают, что используют уникальные пароли для каждой из своих учетных записей.

Остальные 85% признались, что повторно использовали пароли для нескольких учетных записей, хотя некоторые утверждали, что использование вариантов одного и того же пароля в разных учетных записях все еще остается рискованным.

Кроме того, только восемь процентов респондентов заявили, что они тщательно охраняют свои пароли, чтобы предотвратить кражу личных данных и мошенничество.

«Удобнее и проще использовать один и тот же пароль, чем запоминать разные пароли», - отметил Маккуигган.

«Пользователей просят создавать надежные пароли и всегда проверять ссылки, но это чужая для них привычка», - пояснил он. «Они также считают, что их,

вероятно, не взломают, потому что у них нет ничего, что киберпреступники хотели бы украсть».

«Сложные пароли трудно запомнить, а сброс забытого пароля - это боль, которой занятые люди стараются избежать», - добавил Пью.

Однако дни взломанных паролей могут быть сочтены.

«В общем, концепция пароля находится в стадии разработки, - сказал Гилмор. «Он существует слишком долго, и сейчас многие люди ищут способы его заменить». ***(John P. Mello Jr. Many Consumers Fail To Protect Privacy After Receiving Data Breach Notice // ECT News Network, Inc. (https://www.technewsworld.com/story/many-consumers-fail-to-protect-privacy-after-receiving-data-breach-notice-87346.html). 23.11.2021).***

***

«Одна из крупнейших частных авиакомпаний Ирана, Mahan Air, объявила об инциденте, связанном с кибербезопасностью, в результате чего ее веб-сайт отключился и потенциально потерял данные.

Как компания объявила в Твиттере, для них нет ничего необычного в борьбе с хакерскими атаками, поэтому, даже если был нанесен некоторый ущерб, расписание полетов не изменится.

Таким образом, даже несмотря на то, что люди не могут получить доступ к веб-сайту Махана, все международные и внутренние рейсы выполняются в обычном режиме без изменений и задержек.

Более того, компания утверждает, что атака была успешно пресечена в короткие сроки, преуменьшая ее значимость и игнорируя какое-либо реальное воздействие.

«После новостей о кибератаке на системы Mahan Airlines сообщается, что в связи с положением Mahan Airlines в авиационной отрасли страны, такие атаки совершались против этой компании много раз и в разное время, так что они могут быть повреждены», - говорится в переведенном твите Mahan Airlines.

«Это считается нормальным явлением, и команда кибербезопасности Махана всегда действовала разумно и своевременно и предотвращала эти атаки. Поэтому настоящим она объявляет, что все рейсы Махана будут выполняться в соответствии с расписанием, а будущие рейсы будут выполняться в соответствии с к предыдущему расписанию».

Атака на объект санкций

Mahan Air была добавлена в санкционный список США в 2011 году за поддержку членов Корпуса стражей исламской революции (КСИР).

В 2019 году Казначейство США опубликовало заявление о деятельности Mahan Air, в котором подробно излагалось следующее:

«Mahan Air перевезла боевиков, оружие, оборудование и средства КСИР-QF за границу в поддержку региональных операций КСИР-QF, а также перевезла оружие и персонал для «Хизбаллы».

«С начала сирийской гражданской войны Mahan Air регулярно доставляла истребители и технику в Сирию, чтобы поддержать режим Асада, который способствовал массовым зверствам и перемещению гражданского населения».

Хотя операции Махана противоречат американским стратегическим интересам, которые привели к реальным военным действиям в июле 2020 года, хакеры, ответственные за последний инцидент, похоже, не являются американцами.

Актер, который взял на себя ответственность за кибератаку на Mahan Air, - «Хушьяран Ватан», который считает КСИР своим врагом и заявляет, что борется за права меньшинства Ахваз (иранское арабское меньшинство).

Хакеры утверждают, что украли конфиденциальные документы, раскрывающие, как Mahair Air работала с КСИР, и пригрозили опубликовать имена, номера и доказательства деятельности Махана.

«Взлом Mahan Airlines — это первый шаг программы, направленной на прекращение грабежей и посягательств коррумпированного корпуса на город и жителей Ахваза и Хузестана. С помощью конфиденциальных документов, которые мы получили из внутренней сети Mahan Airlines, мы докажем наше заявление о причастности Махана к преступной деятельности КСИР, и мы также покажем, что силы Кудса грабят деньги и ресурсы людей и страны Иран среди повстанческих групп», - говорится в переведенном тексте предполагаемых хакеров.

«И иностранная милиция растрачивает деньги и в то же время использует тех же угнетенных людей в качестве прикрытия для воздушных перевозок оружия, снаряжения и боеприпасов».

Как писали актеры в своем Telegram-канале, у них есть доказательства того, что авиакомпания скрывала военные грузы на гражданских рейсах, чтобы обезопасить их от атак.

Напряженность Ирана в отношениях с западным миром

На прошлой неделе произошел всплеск сообщений об иранских хакерах, нацеленных на американские, израильские и европейские организации. В то же время Microsoft опубликовала отчет, в котором указаны шесть различных иранских хакерских групп, которые, по всей видимости, спонсируются государством.

Кульминацией этого сообщения стало предъявление обвинения двум иранским кибер-актерам, которые пытались повлиять на американских избирателей в период с сентября по ноябрь 2020 года, распространяя ложную информацию под одеждой «гордых парней».

Оба идентифицированных участника предположительно работали в компании по кибербезопасности, которая оказывала услуги правительству Ирана». ***(Bill Toulas. Hackers hit Iran's Mahan airline, claim confidential data theft // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-hit-irans-mahan-airline-claim-confidential-data-theft/). 22.11.2021).***

***

«Национальный центр кибербезопасности Великобритании (NCSC) сообщает, что предупредил владельцев более 4000 интернет-магазинов о том, что их сайты были взломаны в результате атак Magecart с целью кражи платежной информации клиентов.

В атаках Magecart (также известных как веб-скимминг, цифровой скимминг или электронный скимминг) злоумышленники внедряют скрипты, известные как скиммеры кредитных карт (также известные как скиммеры платежных карт или веб-

скиммеры), в скомпрометированные интернет-магазины для сбора и кражи платежа и / или личная информация, предоставленная покупателями на странице оформления заказа.

Позже злоумышленники будут использовать эти данные для различных схем финансового мошенничества и мошенничества с кражей личных данных или продавать их по самой высокой цене на хакерских или карточных форумах.

Жертвы призывают обновлять свое программное обеспечение

«Национальный центр кибербезопасности - часть GCHQ - до конца сентября проактивно идентифицировал 4 151 взломанный интернет-магазин и предупредил розничных продавцов об этих уязвимостях», - заявило британское агентство по кибербезопасности

«Большинство интернет-магазинов, используемых для скимминга, идентифицированных NCSC, были взломаны с помощью известной уязвимости в Magento, популярной платформе электронной коммерции».

NCSC контролировал эти магазины с апреля 2020 года и выдавал предупреждения владельцам сайтов и малым и средним предприятиям (МСП) после обнаружения взломанных сайтов электронной коммерции с помощью своей программы Active Cyber Defense.

Затронутым интернет-магазинам было настоятельно рекомендовано поддерживать Magento - и любое другое программное обеспечение, которое они используют - в актуальном состоянии, чтобы блокировать попытки злоумышленников взломать их серверы и скомпрометировать их интернет-магазины и информацию о клиентах во время Черной пятницы и Киберпонедельника.

«Мы хотим, чтобы малые и средние интернет-магазины знали, как предотвратить использование своих сайтов оппортунистическими киберпреступниками в период пикового количества покупок», - сказала Сара Лайонс, заместитель директора NCSC по экономике и обществу.

«Важно обеспечить максимальную безопасность веб-сайтов, и я настоятельно призываю всех владельцев бизнеса следовать нашим указаниям и следить за тем, чтобы их программное обеспечение обновлялось».

Также доступны инструкции для покупателей

Агентство также предоставляет рекомендации для отдельных лиц и семей, которые хотят делать покупки в Интернете безопасно, советуя им делать покупки только в надежных интернет-магазинах, использовать кредитные карты для онлайн-платежей и всегда следить за подозрительными электронными письмами и текстовыми сообщениями с предложениями, которые кажутся слишком хорошими для быть правдой.

Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) также предоставляет советы по безопасности, как оставаться в безопасности при совершении покупок в Интернете.

Советы Центра жалоб на Интернет-преступления (IC3) ФБР также могут помочь избежать преследований при совершении покупок в Интернете. Консультации ФБР включают действенные советы о том, что делать, если вы станете жертвой мошенничества с покупками в Интернете или атаки Magecart.

«В Черную пятницу и киберпонедельник хакеры будут стремиться украсть деньги покупателей и навредить репутации компаний, превратив их веб-сайты в кибер-ловушки», - сказал Стив Барклай, канцлер герцогства Ланкастер.

«В связи с тем, что все больше и больше торговых операций перемещается в онлайн, крайне важно защитить свой бизнес и своих клиентов, следуя указаниям Национального центра кибербезопасности и Британского консорциума розничной торговли». ***(Sergiu Gatlan. UK govt warns thousands of SMBs their online stores were hacked // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/uk-govt-warns-thousands-of-smbs-their-online-stores-were-hacked/). 22.11.2021).***

***

«Министерство обороны Израиля резко сократило список стран, которым израильским компаниям разрешено продавать свои кибертехнологии. Причиной послужил скандал вокруг израильского производителя коммерческого шпионского ПО NSO Group.

Как сообщает новостное издание Calcalist, если ранее в список входили 102 страны, то теперь он сократился до 37. В частности, из него были исключены новые союзники Израиля Марокко и ОАЭ, в которых известны случаи нарушений прав человека.

Кроме того, израильским компаниям теперь запрещено продавать свои кибертехнологии Саудовской Аравии и Мексике. Правительство Саудовской Аравии обвиняется в использовании разработанного NSO Group шпионского ПО Pegasus для слежки за журналистом Washington Post Джамалем Хашогги, убитого в консульстве Саудовской Аравии в Стамбуле в 2018 году. Правительство Мексики также использовало Pegasus для слежки за журналистами и активистами.

Тем не менее, Индия, которую также уличили в злоупотреблении технологий NSO для слежки за журналистами, политическими оппозиционерами и активистами, по-прежнему остается в списке.

Новые правила окажут огромное влияние на израильскую индустрию кибертехнологий...» ***(На фоне скандала с NSO Израиль заявил о запрете продажи кибертехнологий в 65 странах // SecurityLab.ru (https://www.securitylab.ru/news/526892.php). 25.11.2021).***

***

«Индонезийская полиция расследует заявления хакера, заявившего о похищении на этой неделе персональной информации тысяч полицейских.

На своей странице в Twitter (в настоящее время уже заблокированной) хакер, предположительно из Бразилии, сообщил, что ему удалось получить доступ к серверам Национальной полиции Индонезии и похитить данные 28 тыс. полицейских. Скомпрометированные данные включают: имена, домашние адреса, электронные адреса, телефонные номера и сведения о группе крови.

"В настоящее время мы занимаемся этим вопросом, который рассматривается отделом по борьбе с киберпреступностью", - сообщил пресс-секретарь управления полиции Деди Прасетьо (Dedi Prasetyo) индонезийским СМИ.

Инцидент последовал за атакой на Агентство кибербезопасности и шифрования Индонезии (BSSN), осуществленной в прошлом месяце тем же хакером.

Атаки являются ярким свидетельством того, в каком плачевном состоянии пребывает кибербезопасность госорганов в Индонезии, которая является одним из крупнейших мировых online-рынков.

В августе нынешнего года из-за уязвимости в приложении Министерства здравоохранения Индонезии для отслеживания больных COVID-19 произошла утечка персональных и медицинских данных 1,3 млн человек. На той же неделе также был скомпрометирован сертификат вакцинации президента страны.

Спустя месяц полиция подтвердила факт расследования предположительного взлома группировкой Mustang Panda разведывательного агентства Индонезии и десяти министерств.

В нынешнем году число кибератак на Индонезию существенно увеличилось - с января по август было зафиксировано 888 млн попыток кибератак». ***(Домашние адреса тысяч индонезийских полицейских стали известны преступникам // SecurityLab.ru (https://www.securitylab.ru/news/526722.php). 19.11.2021).***

***

Кібербезпека Інтернету речей

«Великобритания представила законопроект о безопасности продуктов и телекоммуникационной инфраструктуре (PSTI), который обещает защитить устройства IoT.

Многие «умные» устройства не соответствуют своему названию, когда речь идет о безопасности. Поскольку производители стремятся идти в ногу со спросом на устройства IoT, безопасность слишком часто оказывается второстепенной…

Среди обычных приемов обеспечения безопасности - использование паролей по умолчанию.

Вам не нужно быть опытным хакером, чтобы получить доступ к странице входа на чье-то устройство и использовать пароль по умолчанию для таких целей, как кража секретов компании, шантаж, вторжение в частную жизнь, сбор конфиденциальных данных и многое другое.

Опытные хакеры могут сканировать уязвимые устройства и использовать пароли по умолчанию, чтобы добавлять их в бот-сети, такие как печально известный Mirai.

IoT-устройства, которые становятся жертвами Mirai, идентифицируются путем асинхронной отправки TCP SYN-зондов на псевдослучайные IPv4-адреса на TCP-портах telnet 23 и 2323. Если устройство IoT отвечает, выполняется попытка установления telnet-соединения с использованием заранее определенных пар имени пользователя и пароля из списка известные учетные данные по умолчанию.

Такие бот-сети используют беспрецедентные объемы широко распределенного трафика, который устройства Интернета вещей предоставляют

службам DDoS, и наносят огромный ущерб. Одна громкая атака на DNS-провайдера Dyn в октябре 2016 года привела к отключению нескольких известных веб-сайтов, включая GitHub, Twitter, Reddit, Netflix, Airbnb и многие другие.

Счет PSTI запрещает использование паролей по умолчанию. Все устройства должны поставляться с уникальными паролями и не могут быть сброшены на какие-либо универсальные заводские настройки.

Производители также будут обязаны предупреждать клиентов в точках продажи и держать их в курсе о том, как долго продукт будет получать важные обновления безопасности и исправления. Если таких планов нет, это также должно быть раскрыто.

Еще одно ключевое правило состоит в том, что необходимо предоставить контактную информацию, чтобы исследователям безопасности и другим лицам было проще сообщать об обнаружении недостатков и ошибок в продуктах.

Правоприменение будет осуществляться еще не определенным регулирующим органом, который будет иметь право штрафовать компании за несоблюдение требований в размере до 10 миллионов фунтов стерлингов или четырех процентов их глобального оборота. Они также смогут оштрафовать до 20 000 фунтов стерлингов в день за продолжающиеся правонарушения.

На любой «подключаемый» продукт будут распространяться новые правила. Единственное существенное исключение - для настольных и портативных компьютеров, поскольку они обслуживаются развитым рынком антивирусного программного обеспечения…

После того, как законопроект получит королевское согласие, соответствующим игрокам отрасли будет дано не менее 12 месяцев на соблюдение новых правил». ***(UK introduces PSTI bill to protect IoT devices // National Cyber Security News Today (https://nationalcybersecuritynews.today/uk-introduces-psti-bill-to-protect-iot-devices-cybersecurity-cyberattack/). 26.11.2021).***

***

Кіберзлочинність та кібертероризм

«Отчет о ландшафте угроз ENISA (ETL) отображает ландшафт киберугроз, чтобы помочь лицам, принимающим решения, политикам и специалистам по безопасности определять стратегии защиты граждан, организаций и киберпространства.

Эта работа является частью годовой рабочей программы Агентства ЕС по кибербезопасности по предоставлению стратегической информации заинтересованным сторонам.

Содержание отчета собрано из открытых источников, таких как статьи в СМИ, мнения экспертов, разведывательные отчеты, отчеты об анализе инцидентов и исследованиях безопасности; а также через интервью с членами рабочей группы ENISA Cyber Threat Landscapes (рабочая группа CTL).

Отчет ENISA Threat Landscape 2021 (ETL) - это годовой отчет Агентства ЕС по кибербезопасности, ENISA, о состоянии ландшафта угроз кибербезопасности.

Вышедшее сегодня 9-е издание охватывает отчетный период с апреля 2020 года по июль 2021 года.

Угрозы кибербезопасности растут. Программы-вымогатели считаются основной угрозой за отчетный период. Для каждой из выявленных угроз наряду с рекомендациями указываются методы атак, заметные инциденты и тенденции. В новом отчете также представлен список тенденций, касающихся злоумышленников.

Атаки цепочек поставок занимают одно из первых мест среди основных угроз из-за значительного потенциала, который они могут вызвать катастрофические каскадные эффекты. Риск таков, что ENISA недавно подготовила специальный отчет о ландшафте угроз для этой конкретной категории угроз.

9 основных угроз, выявленных в связи с их заметной материализацией за отчетный период:

Программы-вымогатели;

Вредоносное ПО;

Криптоджекинг;

Угрозы, связанные с электронной почтой;

Угрозы данным;

Угрозы доступности и целостности;

Дезинформация - дезинформация;

Безвредные угрозы;

Атаки на цепочку поставок.

Ключевые тенденции

Кризис COVID-19 создал возможности для противников, которые использовали пандемию в качестве основной приманки в кампаниях, например, для атак по электронной почте. Монетизация, по-видимому, является основной движущей силой такой деятельности.

Техники, к которым прибегают злоумышленники, многочисленны. В неполном списке ниже представлены некоторые из наиболее распространенных угроз, выявленных в отчете, по всем угрозам:

Бизнес-модели типа «программа-вымогатель как услуга» (RaaS);

Множественные схемы вымогателей;

Компрометация деловой электронной почты (BEC);

Фишинг как услуга (PhaaS);

Бизнес-модель «дезинформация как услуга» (DaaS); и т.п.» ***(The 9th edition of the ENISA Threat Landscape Report // European Commission (https://digital-strategy.ec.europa.eu/en/news/9th-edition-enisa-threat-landscape-report). 09.11.2021).***

***

«По словам исследователей, группа продвинутых постоянных угроз Lyceum, известная своей нацеленностью на организации в энергетическом и телекоммуникационном секторах на Ближнем Востоке, расширила свою текущую шпионскую деятельность, включив в нее интернет-провайдеров или интернет-провайдеров.

По данным Accenture Cyber Threat Intelligence, или ACTI, и Prevailion Adversarial Группа контрразведки, или ПАКТ.

«По крайней мере, два из выявленных компромиссов считаются продолжающимися, несмотря на предварительное публичное раскрытие индикаторов компрометации», - отмечают исследователи.

Исследователи отмечают, что телекоммуникационные компании и интернет-провайдеры являются высокоуровневыми целями для кибершпионажа, поскольку они предоставляют доступ к ряду организаций и подписчиков, а также к их собственным внутренним системам, которые могут быть использованы для дальнейшего использования злонамеренных действий.

По словам исследователей, компании в этих отраслях могут использоваться злоумышленниками или их спонсорами для наблюдения за интересующимися людьми. Они добавляют, что объекты - такие как, например, министерство иностранных дел в Африке - очень востребованы, поскольку они содержат ценную информацию о текущем состоянии двусторонних отношений между странами и понимание будущих деловых отношений.

По словам Касперского, деятельность лицея, также известного под названиями Hexane, Spirlin и Siamesekitten, началась с 2018 года. В ее цели также входят критически важные системы, такие как нефтегазовые организации на Ближнем Востоке, в Африке и Центральной Азии, сообщает компания, занимающаяся кибербезопасностью.

Группа, как полагают, связана с иранскими группировками, согласно исследователям охранной фирмы ClearSky.

«Поставщики телекоммуникационных услуг могут усилить свою защиту от таких атак, обучая сотрудников социальной инженерии. Электронная почта является наиболее распространенным средством для таких атак, но иранские злоумышленники также часто используют LinkedIn для разведки и в качестве среды для социальной инженерии. Социальная инженерия является распространенным компонентом об исходных векторах атак, которые обычно используют иранские кибершпионажные группы, в том числе Lyceum, - говорит Пол Прюдомм, глава советника по анализу угроз IntSights, компании Rapid 7.

«Иранские злоумышленники часто вкладывают больше средств в относительно сложные схемы социальной инженерии, чем другие спонсируемые государством субъекты. В случае Lyceum эта группа ранее использовала социальную инженерию для получения первоначального доступа к учетным записям и машинам сотрудников целевых компаний, либо представляя в качестве рекрутеров с предложениями работы в другой компании или путем взлома подлинных учетных записей в той же компании и использования этих учетных записей для рассылки вредоносных программ большему количеству сотрудников», - отмечает Прюдомм.

Как работает лицей

Первоначальный вектор атаки группы включает доступ к системам организации с использованием учетных данных, полученных с помощью распыления паролей или атак грубой силы, и доставку вредоносных вредоносных программ с помощью целевого фишинга от скомпрометированных учетных записей к целевым руководителям, персоналу отдела кадров и ИТ-персоналу, по данным службы безопасности. провайдер Secureworks.

«Получатель с большей вероятностью откроет сообщение, если оно отправлено с внутреннего адреса», - отмечается в блоге.

Исследователи из ACTI и PACT определили операторов лицеев, использующих два основных семейства вредоносных программ, получивших название Shark и Milan, но также известных вместе как James. По их словам, эти бэкдоры могут обмениваться данными через DNS и HTTP (S) для связи C2.

«Лицей, вероятно, обновляет свои бэкдоры в свете недавних публичных исследований своей деятельности, чтобы попытаться опередить защитные системы. Группа продолжала нацеливаться на компании, имеющие национальное стратегическое значение», - отмечают исследователи.

Бэкдор Shark - это 32-битный исполняемый файл, написанный на C # и.NET. По словам исследователей, он настраивает файлы, содержащие хотя бы один домен C2, который используется с алгоритмом генерации домена для туннелирования DNS или HTTP C2.

Milan - это 32-битная RAT, написанная на Visual C ++ и.NET, и, по словам исследователей, она «извлекает данные, генерируя запросы с использованием жестко заданного домена, а затем запрашивая один из ряда активных URL-путей, связанных с страницами сервера»..

«Когда команда ACTI и PACT запросила в наборе данных Prevailion известные, жестко закодированные URL-пути, наблюдаемые в образцах в Милане, команда заметила, что в октябре продолжалась передача маяков с IP-адреса, который был разрешен оператору связи в Марокко», - отмечают они.

Они определили, что сигнализация, возможно, является новой лазейкой, исходящей из телекоммуникационной компании в Тунисе, а также из министерства иностранных дел в Африке.

«Синтаксис URL-адреса недавно перенастроенного бэкдора аналогичен синтаксису, созданному в более новой версии Milan. Однако, поскольку синтаксис URL-адреса настраивается, вполне вероятно, что операторы Lyceum перенастроили синтаксис URL-адреса, используемый Milan для обхода систем обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), которые были закодированы для обнаружения синтаксиса предыдущего Миланского маяка», - говорят они.

Ожидается, что Lyceum продолжит использовать бэкдоры Shark и Milan, и с некоторыми изменениями группа, вероятно, сохранит плацдарм в сети жертв, несмотря на публичное раскрытие IOC, по мнению исследователей.

«Важно напомнить компаниям, что никто не застрахован от преследований. Государственный и частный секторы должны инвестировать сейчас, чтобы усилить профилактику и обнаружение, а также повысить устойчивость. Мы можем встречать пожар огнем», - говорит Сэм Карри, директор службы безопасности в Cybereason.

«Конечно, злоумышленник может проникнуть внутрь, но что с того? Мы можем сделать так, чтобы это ничего не значило. Мы можем замедлить их. Мы можем ограничить то, что они видят. Мы можем обеспечить быстрое обнаружение и выброс. Короче говоря, мы можем сделать материал «Бреши устарели. Мы можем уберечь их от попадания в замок, заранее спланировав и проявив смекалку и создав правильную оборону», - отмечает Карри…». ***(Prajeet Nair. Lyceum APT Group Adds***

ISPs to Its Target List // Information Security Media Group, Corp. (https://www.govinfosecurity.com/lyceum-apt-group-adds-isps-to-its-target-list-a-17883). 10.11.2021).

***

«Основные угрозы киберпреступности, с которыми сталкиваются организации в Европе и за ее пределами, включают в себя партнерские программы с программами-вымогателями, более сложные мобильные вредоносные программы и множество различных типов онлайн-мошенничества, а также другие виды преступлений.

Так утверждает Европол, правоохранительное агентство ЕС, в своей последней оценке угрозы организованной преступности в Интернете. В ежегодно выпускаемом отчете подробно описываются основные тактики и тенденции киберпреступности за последние 12 месяцев.

IOCTA этого года основывается на наблюдениях, собранных в результате опроса всех 27 стран-членов ЕС; Исландия, Норвегия, Швейцария и Великобритания, которые являются ассоциированными членами Целевой группы ЕС по киберпреступности; Консультативные группы Европола; и внутренние эксперты Европола.

Один из основных выводов прошлогоднего отчета IOCTA заключался в том, что «киберпреступность - это эволюция, а не революция», - сказал Information Security Media Group Филипп Аманн, руководитель отдела стратегии Европейского центра киберпреступности Европола после публикации прошлогоднего отчета.

В этом году главный вывод заключается в том, что экстремальные явления могут способствовать еще более быстрой эволюции киберпреступности, как это сделала продолжающаяся пандемия COVID-19, - говорит Катрин Де Болле, исполнительный директор Европола.

Рост партнерской модели программ-вымогателей

Например, в прошлом году был отмечен стремительный рост экосистемы вымогателей как услуги, в которую вовлечены разработчики, предоставляющие вредоносное ПО с криптоблокировкой аффилированным лицам, которые используют вредоносное ПО для заражения жертв в обмен на согласованную часть суммы каждого выкупа.

«Партнерские программы программ-вымогателей позволяют большей группе преступников атаковать крупные корпорации и государственные учреждения, угрожая им многоуровневыми методами вымогательства», - говорит Де Болле. Эти методы вымогательства, отмечает она, могут включать не только угрозы назвать имена жертв и опозорить их, но и уничтожить их с помощью распределенных атак с отказом в обслуживании.

Ухудшение сексуальной эксплуатации детей

По ее словам, еще одной тенденцией к ускорению является рост сексуальной эксплуатации детей, в том числе с целью получения прибыли.

«Дети, проводящие больше времени в Интернете, сделали их более восприимчивыми к уходу, что привело к увеличению количества самодельных

материалов для эксплуатации», - говорит Де Болле, добавляя, что «в этих материалах все чаще используются дети младшего возраста».

Кроме того, «резко возросла активность онлайн-ухаживания в социальных сетях и на игровых онлайн-платформах», - говорит Европол, причем часто взрослые выдают себя за сверстников несовершеннолетних, которых они преследуют для жестокого обращения.

Преступники часто торгуют материалами эксплуатации через темные веб-сайты, доступные только через анонимный браузер Tor, что, по словам полиции, может затруднить их идентификацию или отслеживание.

Атаки на цепочки поставок и вредоносное ПО для мобильных устройств

Для злоумышленников из национальных государств, а также для преступников, стремящихся получить незаконную прибыль, цепочки поставок остаются главной целью преступников. По словам Европола, за последние 12 месяцев атаки SolarWinds и Microsoft Exchange, а также атаки программ-вымогателей на программное обеспечение разработчика управляемых ИТ-сервисов Касеи продемонстрировали, что масштабы и серьезность таких атак увеличиваются.

По словам Европола, еще одна давно существующая угроза, которая становится все более изощренной и разрушительной, - это мобильные вредоносные программы и особенно банковские трояны, которые работают на устройствах Android и предназначены для кражи учетных данных пользователей.

«Ряд семейств вредоносных программ для мобильного банкинга реализовали на устройстве новые возможности для совершения мошенничества, манипулируя банковскими приложениями на устройстве пользователя с помощью модулей системы автоматизированного перевода на базе Android Accessibility Service», - говорится в сообщении. «Банковские трояны, такие как Cerberus и TeaBot, также способны перехватывать текстовые сообщения, содержащие одноразовые коды доступа, отправленные финансовыми учреждениями и приложениями для двухфакторной аутентификации, такими как Google Authenticator».

Другой банковский троянец под названием FluBot чрезвычайно популярен, особенно в США и Европе, и распространяется через фишинговые текстовые сообщения с зараженного устройства всем, кто находится в его списке контактов, сообщает Европол. «Ключевой частью функциональности вредоносного ПО является его способность устанавливать оверлеи дисплея для проверки в Google Play и различных банковских приложений, что позволяет кражу учетных данных жертв - банковских, кредитных карт и криптокошельков», - говорится в сообщении.

Мошенничество в самых разных формах

В то время как программы-вымогатели часто оказываются в центре внимания киберпреступлений - не в последнюю очередь из-за массовых сбоев, которые они могут вызвать, - полиция заявляет, что мошенничество продолжает оставаться серьезной угрозой. По словам официальных лиц, мошенничество с доставкой - например, текстовые сообщения с якобы имевшей место «пропущенной доставкой» - резко возросло во время пандемии и, как правило, пытается обманом заставить жертву отправить средства непосредственно злоумышленнику.

Ведущие виды мошенничества включают взлом корпоративной электронной почты и мошенничество со стороны генерального директора - атаки, в которых преступники пытаются обманом заставить жертв перевести им деньги.

Но, прежде всего, «инвестиционное мошенничество стало наиболее распространенным типом мошенничества за последние 12 месяцев», - заявляет Европол, жертвы которого часто становятся мишенью для получения возможности инвестировать в криптовалюту с предположительно гарантированной высокой доходностью.

«Подлинно выглядящие рекламные кампании, незаконное использование знаменитостей и даже личные рекомендации через схемы онлайн-знакомств - все это помогает привлечь ничего не подозревающих жертв на эти поддельные платформы», - говорит Европол. «Кроме того, преступники становятся все более профессиональными, управляя местными центрами обработки вызовов для разных языков, создавая более легитимные веб-сайты, используя программное обеспечение удаленного доступа для захвата учетных записей жертв и управляя сложными сетями денежных мулов».

Criminals Market Услуги преступникам

К сожалению, экосистема киберпреступности как услуги делает ряд вредоносных сервисов и инструментов доступными для легкого доступа, включая возможность доступа к центрам обработки вызовов, поскольку не только мошенники с криптовалютой, но и операции с программами-вымогателями продолжают атаковать или связываться с жертвами.

Начинающие преступники, которые могут не обладать глубокими техническими знаниями, также могут покупать готовые к использованию штаммы программ-вымогателей и других вредоносных программ, подключаться к защищенным хостинг-сайтам или арендовать ботнеты для помощи в своих атаках, а также обращаться за советом на форумы по борьбе с киберпреступностью.

Европол отмечает, что для борьбы с этим правоохранительные органы продолжают нацеливаться на так называемую «серую инфраструктуру», имея в виду услуги, которые преступники продают другим преступникам. «Услуги серой инфраструктуры включают в себя пуленепробиваемые хостеры, мошеннические обмены криптовалютой и виртуальные частные сети, которые обеспечивают безопасное убежище для преступников», - говорит Европол (см. «Подожди, смотри, срывай: как полиция продолжает преследовать киберпреступность»).

Хотя такие услуги не всегда могут быть прерваны, полиция продолжала делать это во многих случаях. Например, за последний год Европол помог скоординировать удаление сервисов DoubleVPN и Safe-Inet VPN и связанных с ними надежных хостинг-провайдеров, а также арестовать преступных пользователей криптофонных сервисов.

Преступники все чаще полагаются на виртуальную валюту для получения выкупа и отмывания своих доходов, полученных незаконным путем, и внедрения большего количества сохраняющих конфиденциальность цифровых монет, таких как монеро, банкноты Европола. Однако и здесь возможны сбои, хотя часто и за пределами правоохранительных органов, на более политическом или дипломатическом уровне. Финансовые регуляторы США, например, вносят в

черный список криптовалютные биржи, которые не соблюдают требования «знай своего клиента» и противодействие отмыванию денег, что делает их использование преступлением». ***(Mathew J. Schwartz. Pace of Cybercrime Evolution Is Accelerating, Europol Warns // Information Security Media Group, Corp. (https://www.govinfosecurity.com/pace-cybercrime-evolution-accelerating-europol-warns-a-17902). 12.11.2021).***

***

«Похоже, что многочисленные киберпреступные группы нацелены на относительно новых участников рынка с помощью фишинговых атак.

Согласно новому отчету из Сингапура, в том, что аналитики называют «каннибалистическим подходом», эти банды выдают себя за подпольные карточные магазины, такие как Joker's Stash, BriansClub, Unicc, Ferum Shop и ValidCC, чтобы обмануть новичков с целью получения денежной выгоды. кибербезопасная компания Group-IB.

Дмитрий Шестаков, руководитель отдела исследования киберпреступности Group-IB, рассказал Information Security Media Group: «Среди воров нет чести. Киберпреступники часто обманывают друг друга, время от времени происходят взломы подпольных рынков - это довольно распространенная практика. Ничего особенного. не дает кардерам играть грязно, поскольку «жертвы» - в данном случае также кардеры - не могут предпринимать юридических действий».

Фишинговые сайты, которые Руслан Чебесов и Сергей Кокурин из Group-IB в своем отчете называют «фальшивыми магазинами», в основном были созданы тремя группами, которые аналитики идентифицируют как UniFake, JokerMantey и SPAGETTI.

В сообщении говорится, что сетевая инфраструктура, созданная тремя бандами, включает тысячи доменных имен, используемых для фишинга. Он добавляет, что SPAGETTI имеет самую большую известную сеть, в которой работает более 3000 доменных имен.

Карточные магазины и связанные с ними торговые площадки

В отчете карточные магазины и связанные с ними рынки в подполье называются амазонками и eBays темной сети для банковских данных. Аналитики добавляют, что они являются основными ресурсами, используемыми более мелкими преступниками, участвующими в мелкомасштабном мошенничестве, таком как мошенничество с банковскими картами или кардинг, мошенничество и рассылка спама.

«Карточные магазины - это разновидность подпольного рынка. Они используются для продажи украденных данных банковских карт в виде полных записей о держателях карт (включая имя, номер карты, CVV, дату истечения срока действия) или свалок: копий магнитной полосы банковской карты.», - говорят аналитики.

Скомпрометированные данные, не относящиеся к банковским картам, обычно не продаются в карточных магазинах, добавляют они.

Аналитики сообщили Information Security Media Group, что для того, чтобы быть участником настоящих подпольных карточных магазинов и рынков,

пользователи должны платить за активацию учетной записи в размере от 20 до 200 долларов и / или вносить деньги на свои счета для покупки скомпрометированных данных.

В отчете отмечается, что поддельные магазины используют процесс предоплаты, чтобы ввести в заблуждение киберпреступников.

Мошенники добавляют уровень подлинности, используя названия существующих подземных ресурсов и полностью копируя их дизайн, говорят аналитики, добавляя, что, когда пользователи тратят свои деньги в этих фальшивых магазинах, операторы собирают платежи в свои собственные криптокошельки.

В отчете отмечается, что поддельные магазины не создаются один за другим - они обычно создаются большими кластерами. «Чтобы привлечь больше потенциальных покупателей скомпрометированных данных банковских карт, создатели фальшивых магазинов размещают рекламу на подпольных форумах и в чатах Telegram и обманом заставляют пользователей посещать свои ресурсы. Как бы иронично это ни звучало, это наносит ущерб репутации оригинальных веб-сайтов», - аналитики говорят и отмечают, что в качестве альтернативы более мелкие поддельные сайты объединяются в более крупные сети.

СПАГЕТТИ

Аналитики отмечают, что в SPAGETTI, крупнейшую из трех обнаруженных сетей, было совершено более 9 200 входящих транзакций на различные кошельки с криптовалютой. Они обнаружили, что полученная сумма была в основном в биткойнах (23 BTC) и составила более 1,2 миллиона долларов по обменному курсу на 12 октября 2021 года.

Адреса кошельков с криптовалютами могли измениться с момента создания сети фальшивых магазинов SPAGETTI, поэтому фактическая выручка может быть значительно выше, добавляют аналитики.

Аналитики отмечают, что хотя SPAGETTI имеет несколько независимых фальшивых магазинов, ее главным «активом» является тот, который маскируется под один из старейших и крупнейших карточных магазинов, под названием BriansClub, у которого очень мало клонов на рынке кардочесания. По их словам, создатели SPAGETTI используют фишинговый домен briansclub [.] Ru. Аналитики отмечают, что помимо заработка на мошенничестве с платой за активацию аккаунта, он также распространяет вредоносное ПО через свои веб-сайты.

Согласно отчету, после уплаты платы за активацию поддельного briansclub [.] Ru пользователям отображается сообщение об успешном завершении и предлагается загрузить «защищенное» приложение по ссылке на архив под названием «panelcontrol.rar». " В архиве два файла: «PanelControl.exe» и «LitePanel.exe».

Первый вместо того, чтобы предоставить доступ к панели карточного магазина, запускает стилер под названием Taurus Project, говорят аналитики.

По данным новостной платформы Security Boulevard, вредоносное ПО для кражи информации C / C ++, также известное как Taurus Stealer, широко используется с апреля 2020 года. В отчете говорится, что он, продвигаемый в Telegram-канале и на русскоязычных подпольных форумах, скорее всего, был разработан Alexuiop1337, который также создал вредоносное ПО Predator the Thief.

Описывая действия стилера, аналитики говорят, что «стилер Taurus Project не только собирает информацию из браузеров Chrome, Opera и Firefox, но также получает доступ к камере и собирает данные для входа из нескольких кошельков с криптовалютами, таких как Bitcoin, Ethereum и Bytecoin. Это означает, что после запуска файла неопытный пользователь может потерять данные для входа в свои криптовалютные кошельки, которые использовались для оплаты активации, а также потерять доступ к другим ресурсам, включая другие магазины карт».

UniFake

UniFake, получивший свое название от большинства поддельных доменных имен, олицетворяющих разновидности карточного магазина Unicc, имеет более 100 доменных имен. Из них, по мнению аналитиков, 66 являются вариациями названия Unicc. Аналитики выявили 150 транзакций, совершенных в сети UniFake, на сумму 17 377 долларов США по курсу на 12 октября 2021 года.

Unicc, по мнению аналитиков, является одним из крупнейших подпольных карточных магазинов. «Он был запущен в 2012 году и вскоре стал популярным среди кардеров из-за большого количества обновлений, но также и среди карточных магазинов, которые выступают в качестве посредников и продают данные Unicc за комиссию, используя свои собственные системы API для продажи карт. Эти факторы, скорее всего, способствовали появлению (сайта) ", - говорят они.

Большинство из этих доменов имеют поразительное сходство с реальным дизайном сайта Unicc, за исключением того факта, что «криптокошельки при активации учетной записи контролируются владельцами фальшивых магазинов», - говорят аналитики.

ДжокерМантей

JokerMantey, сеть поддельных магазинов, которая выдает себя за и фишит от имени популярного карточного магазина Joker's Stash, имеет более 20 поддельных доменных имен, а также включает поддельные магазины, копирующие карточный магазин BriansClub.

Владельцы оригинального тайника Джокера закрыли магазин в феврале 2021 года (см.: Тайник Джокера, как сообщается, прекращает работу).

В отчетах говорится, что именно поэтому киберпреступники используют одно и то же имя для работы в темной сети. Операторы JokerMantey с меньшей вероятностью столкнутся с преследованием со стороны оригинального карточного магазина, даже если их злонамеренные действия будут обнаружены, поскольку первоначальный карточный магазин уже закрыт, говорится в сообщении. «Это делает его прибыльным», - добавляют аналитики.

Аналитики также идентифицировали два связанных биткойн-кошелька: один Litecoin и другой Dash, которые они получили из платежной формы на фишинговом сайте.

Аналитики отмечают, что до октября 2021 года JokerMantey получил в общей сложности 304 транзакции в связанных криптовалютных кошельках на сумму 220 587 долларов США по обменному курсу того же месяца.

Последствия поддельных магазинов

«Некоторые новички-кардеры, которых обманули, уходят из этого незаконного бизнеса, в то время как другие учатся на своих ошибках, становятся

более осторожными и продолжают кардочесальную деятельность», - сказал Шестаков ISMG.

Он говорит, что исходные незаконные кардинговые сайты явно страдают репутацией. «Обманутые кардеры рассказывают о своем негативном опыте на подпольных форумах, не осознавая, что стали жертвами фальшивых магазинов. Такие отзывы вызывают недоверие как среди постоянных пользователей карточных магазинов, так и среди партнеров, что приводит к потере прибыли для оригинальных карточных рынков. попытка предотвратить потерю клиентов и нанесение ущерба их репутации, заходит так далеко, что публикует списки фальшивых магазинов, которые выдают себя за них ".

Тем не менее, говорит Шестаков, эти поддельные магазины будут продолжать существовать, потому что «у владельцев карточных магазинов нет законных средств, чтобы закрыть поддельные магазины, выдающие себя за них».

Он говорит, что поддельные магазины влияют на исследования в области безопасности и информацию об угрозах, потому что они могут вызывать ложные срабатывания. «Не зная, что они имеют дело с фальшивым магазином, - говорит Шестаков, - специалисты по анализу угроз могут предупреждать клиентов и общественность неточной и вводящей в заблуждение информацией». ***(Mihir Bagwe. Cybercriminals Target Newbie Bad Actors With Phishing Sites // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cybercriminals-target-newbie-bad-actors-phishing-sites-a-17810). 01.11.2021).***

***

«Агентство Европейского Союза по кибербезопасности (ENISA) заявляет, что количество кибератак на сектор здравоохранения увеличилось почти на 50%.

В 2020 году ENISA получила в общей сложности 742 сообщения об инцидентах, связанных с кибербезопасностью, которые существенно повлияли на критическую инфраструктуру в соответствии с Директивой о безопасности сети и информационных систем (Директива NIS). В секторе здравоохранения в 2020 году количество таких инцидентов увеличилось на 47% по сравнению с предыдущим годом.

Атаки кибербезопасности на здравоохранение могут угрожать жизни и повлиять на всю цепочку поставок здравоохранения с разрушительными последствиями для всех заинтересованных сторон, таких как граждане, государственные органы, регулирующие органы, профессиональные ассоциации, отрасли, малые и средние предприятия.

Количество киберугроз на протяжении многих лет в настоящее время растет пропорционально растущей популярности новых технологий, таких как Интернет вещей (IoT), искусственный интеллект (AI), большие данные, облачные вычисления и множество подключенных устройств, среди прочего.

Роль групп реагирования на инциденты компьютерной безопасности (CSIRT) заключается в развитии возможностей, необходимых для решения таких проблем и реализации положений Директивы NIS. Национальные CSIRT - это организации, отвечающие за реагирование на инциденты в секторе здравоохранения. Хотя

специализированные CSIRT сектора здравоохранения по-прежнему являются исключением в государствах-членах, сотрудничество CSIRT в конкретных секторах развивается.

ENISA заявляет, что у операторов основных услуг в ЕС отсутствует культура безопасности. Поскольку скорость обновлений быстро опережает темпы развития ИТ-технологий, когда медицинское оборудование обычно имеет срок службы в среднем 15 лет, уязвимости, как правило, накапливаются по мере устаревания ИТ-уровня в течение жизненного цикла оборудования и цифровых устройств. Еще одна проблема, с которой сталкивается сектор здравоохранения, - сложность систем из-за увеличения количества подключенных устройств, что ведет к увеличению потенциальной поверхности атаки.

Ключевой движущей силой развития возможностей CSIRT по реагированию на инциденты является информация, связанная с требованиями безопасности и обязанностями организаций для каждого сектора. Общие рамки для классификации инцидентов и моделирования угроз, образовательные мероприятия и сеть, позволяющая общаться между участниками реагирования на инциденты, составляют основные ресурсы и инструменты, поддерживающие в настоящее время развитие возможностей реагирования на инциденты.

CSIRT национального сектора здравоохранения, как правило, предоставляют услуги, более подходящие для этого сектора. Поскольку отраслевые CSIRT в сфере здравоохранения остаются дефицитом в среде, где требуется специализированная поддержка для разработки мероприятий по реагированию на инциденты, ENISA рекомендует содействовать созданию CISRT в секторе здравоохранения, обеспечивая легкий доступ к финансированию и содействуя деятельности по наращиванию потенциала.

По заявлению ENISA, CSIRT в области здравоохранения могли бы помочь операторам основных услуг в развитии их возможностей реагирования на инциденты, установив отраслевые нормативные акты, соглашения о сотрудничестве, каналы связи и государственно-частные партнерства». ***(EU Agency Reports 47% Rise in Cybersecurity Incidents in the Health Sector in 2020 // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/eu-agency-reports-47-rise-in-cybersecurity-incidents-in-the-health-sector-in-2020/). 15.11.2021).***

***

«Хакеры атаковали почтовые серверы Федерального бюро расследований (ФБР), рассылая тысячи фальшивых сообщений, в которых говорится, что их получатели стали жертвами «изощренной цепной атаки»… Электронные письма были первоначально обнаружены The Spamhaus Project, некоммерческой организацией, которая расследует расследование спамеров.

В электронных письмах утверждается, что Винни Троя стоял за фальшивыми атаками, а также ложно утверждается, что Троя связана с печально известной хакерской группой The Dark Overlord - теми же плохими актерами, которые просочились в пятый сезон Orange Is the New Black. На самом деле Троя - известный исследователь в области кибербезопасности, который руководит двумя компаниями по обеспечению безопасности в темной сети, NightLion и Shadowbyte.

…хакерам удалось разослать электронные письма более чем на 100 000 адресов, все из которых были извлечены из базы данных Американского реестра Интернет-номеров (ARIN). В отчете Bloomberg говорится, что хакеры использовали общедоступную систему электронной почты ФБР, из-за чего электронные письма казались еще более законными. Исследователь кибербезопасности Кевин Бомонт также подтверждает законный вид электронного письма, заявляя, что заголовки аутентифицируются как исходящие с серверов ФБР с использованием процесса почтового сообщения с идентификационными ключами домена (DKIM), который является частью системы, которую Gmail использует для наклеивания логотипов бренда на проверенные корпоративные электронные письма.

ФБР отреагировало на инцидент в пресс-релизе, отметив, что это «текущая ситуация» и что «поврежденное оборудование было отключено». Помимо этого, ФБР заявляет, что в настоящее время у него нет дополнительной информации, которой можно было бы поделиться.

По данным Bleeping Computer, спам-кампания, вероятно, была проведена как попытка опорочить Трою. В своем твите Троя предполагает, что атаку мог предпринять человек по имени «Помпомпурин». Как отмечает Bleeping Computer, этот же человек якобы пытался нанести ущерб репутации Трои аналогичными способами в прошлом.

Репортер по компьютерной безопасности Брайан Кребс также связывает Помпомпурина с этим инцидентом - человек якобы отправил ему сообщение с адреса электронной почты ФБР, когда были начаты атаки, со словами: «Привет, его помпомпурин. Проверьте заголовки этого электронного письма, оно действительно пришло с сервера ФБР ». KrebsOnSecurity даже получил возможность поговорить с Помпомпуриным, который утверждает, что взлом был направлен на выявление уязвимостей в системе электронной почты ФБР.

«Я мог бы использовать это на 1000 процентов, чтобы отправлять больше законных электронных писем, обманывать компании для передачи данных и т.д.», - сказал Помпомпурин в заявлении для KrebsOnSecurity. Этот человек также сообщил изданию, что они воспользовались брешь в безопасности на портале правоохранительного предприятия ФБР (LEEP) и сумели зарегистрировать учетную запись, используя одноразовый пароль, встроенный в HTML-код страницы. Оттуда Помпомпурин утверждает, что они смогли манипулировать адресом отправителя и телом электронной почты, выполнив масштабную спам-кампанию.

При таком доступе атака могла быть намного хуже, чем ложное оповещение, которое ставило системных администраторов в состояние повышенной готовности. Ранее в этом месяце президент Джо Байден поручил исправить ошибку, требующую от гражданских федеральных агентств исправления любых известных угроз. В мае Байден подписал распоряжение, направленное на улучшение киберзащиты страны после разрушительных атак на Colonial Pipeline и SolarWinds». ***(Emma Roth. The FBI's email system was hacked to send out fake cybersecurity warnings // Vox Media, LLC. (https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-cybersecurity-warnings). 14.11.2021).***

***

«Новый отчет PhishLabs показывает, насколько распространены угрозы кибербезопасности среди популярных брендов, а также общие тенденции, которым они следуют.

PhishLabs — это компания, занимающаяся анализом кибербезопасности, которая фокусируется на информировании об угрозах и злоумышленниках. Фирма достигает этого несколькими способами. В нем публикуются исследовательские статьи о популярных угрозах кибербезопасности и распространенных привычках злоумышленников.

Угрозы кибербезопасности являются регулярными, о них постоянно слышно, и они наносят слишком большой ущерб, который также часто может быть непоправимым. В наши дни вся важная информация хранится в сети. Данные кредитной карты, личные адреса, номера телефонов и даже номера социального страхования — это лишь часть важной информации и данных, которые мы оставляем в Интернете по мере необходимости. Защита имеет первостепенное значение, и это именно та работа, в которой PhishLabs помогает своим клиентам и пользователям.

В этом текущем отчете, озаглавленном «Ежеквартальный отчет о тенденциях и аналитике угроз за ноябрь 2021 года», подробно рассказывается о том, как возникали угрозы в течение 2021 года, причем сравнения проводятся до 2020 года. Говоря о сравнениях, наша первая метрика делает именно это, показывая, что количество фишинговых атак увеличилось на 32. % в годовом исчислении, а количество связанных с ними атак вишинга за тот же период увеличилось вдвое. Для тех, кто не знает, вишинговые атаки — это просто фишинговые атаки по телефону, в которых задействован голос злоумышленника. Хотя можно было бы ожидать, что с годами количество таких атак снизится из-за в целом повышенной осведомленности о мошенничестве в Интернете, мы не учитываем то, что такие атаки растут и развиваются, как и мы. Как реклама становится умнее, так и хакеры, и киберпреступники готовы более или менее попробовать что угодно, если в конце концов будет получен день выплаты жалованья. Фишинговые атаки больше всего затронули финансовую отрасль и социальные сети: частота составила 55% и 30,5% соответственно.

Отталкиваясь от фишинга в социальных сетях, в отчете показано, что угрозы кибербезопасности в социальных сетях в целом выросли на целых 82% с января этого года. Такие платформы и отрасль остаются средоточием угроз кибербезопасности и часто являются источником многих атак. Социальные сети - это служба, обслуживающая буквально миллиарды людей, и киберпреступники с большой вероятностью (намеренно) столкнутся с людьми, которые не подозревают об угрозах и злоумышленниках и, следовательно, более восприимчивы к ним. Фишинговые атаки по-прежнему остаются гибкими. Хотя скомпрометированные веб-сайты по-прежнему остаются самой популярной формой злоумышленников, электронные письма, короткие URL-адреса, сообщения в социальных сетях и бесплатные услуги хостинга также набирают обороты, и им даже удается находить все более и более широкую аудиторию». ***(Arooj Ahmed. Cybersecurity Report Details Phishing Threats And Their Respective Trends Across 2020 To 2021 // DIGITALINFORMATIONWORLD.COM***

(https://www.digitalinformationworld.com/2021/11/cybersecurity-report-details-phishing.html). 16.11.2021).

***

«Страдание практически от любого вида киберпреступности приведет к тому, что вы почувствуете, что оказались в невыгодном положении, учитывая все обстоятельства, которые были учтены и приняты во внимание. Люди часто предполагают, что именно пожилым людям тяжелее справляться с киберпреступностью и т.п. по той причине, что они могут не обладать нужными знаниями, необходимыми для того, чтобы в конечном итоге защитить себя в сети.

Учитывая все вышесказанное, важно отметить, что данные от StaySafeOnline NCSA показали, что представители более молодого поколения, а именно поколение Z и миллениалы, с меньшей вероятностью сообщат о киберпреступлении после его совершения. против них. Бэби-бумеры чаще всего сообщают о киберпреступлениях, поскольку 64% из них заявили, что они это сделали, а среди миллениалов, которые сообщают о киберпреступлениях только 32% времени, эта доля была намного ниже. Ситуация становится еще более мрачной, если вы посмотрите на поколение Z, в просторечии известное как «зумеры» в Интернете, которые сообщают о киберпреступлениях только в 21% случаев.

Одной из причин этого может быть тот факт, что представители поколения Z и миллениалы, выросшие в Интернете, не осознают, что онлайн-безопасность - это не то, что можно принимать как должное. Очень важно, чтобы представителям молодого поколения была предоставлена возможность узнать о важности кибербезопасности, а также рассказать о том, как сообщение о преступлениях, совершенных против них, может принести им пользу во многих отношениях, если задуматься.

Это становится особенно важным, когда вы понимаете, что пользователи Интернета из поколения Z и поколения миллениалов являются одними из самых уязвимых людей в Интернете, поэтому попытка защитить их - это то, что было бы полезно для будущего всех онлайн-пространств…» ***(Zia Muhammad. Data Shows Younger People Aren't Reporting Cybercrimes // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/data-shows-younger-people-arent.html). 09.11.2021).***

***

«Все получают спам-сообщения с фишинговыми ссылками, и вы можете подумать, что вы слишком умны, чтобы когда-либо нажимать на что-либо подобное. Учитывая все вышесказанное, важно отметить, что 1 из каждых 10 человек нажимал на фишинговую ссылку при использовании своих телефонов, согласно недавнему исследованию, которое было проведено по этому вопросу. Данные выявили довольно неприятную тенденцию, на которую многие хотели бы обратить внимание.

Исследование было проведено Wandera / Jamf, и оно включало анализ полумиллиона защищенных устройств, которые были распределены в 90 разных

странах, включая такие крупные, как США и Китай. По-настоящему тревожная статистика, о которой будут беспокоиться многие люди, - это тот факт, что склонность людей переходить по фишинговым ссылкам на самом деле увеличилась. Число людей, ставших жертвами фишинговых атак, выросло на 160% в годовом исчислении, а это означает, что многие люди, вероятно, не предпринимают необходимых шагов для защиты от подобных ситуаций.

Что еще более примечательно, учитывая все обстоятельства, которые были учтены и приняты во внимание, так это то, что фишинговые атаки исходят не из небезопасных мест. Напротив, подавляющее большинство из них, а точнее 93%, пришли с якобы безопасных доменов. Это означает, что у доменов, вероятно, был замок в строке URL-адреса, из-за чего многие люди начали предполагать, что ссылки были достаточно безопасными, чтобы нажимать на них. Это, мягко говоря, понятно, но это просто показывает, что никогда нельзя быть слишком осторожным, когда речь идет о ссылках, которые вы собираетесь соединить…». ***(Zia Muhammad. Study Shows 10% of People Have Clicked on Phishing Links While on Their Phones // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/study-shows-10-of-people-have-clicked.html). 10.11.2021).***

***

«Целый год исследования, проведенного Imperva, показывает, что пятьдесят семь процентов всех кибератак и атак, наблюдаемых на платформах электронной коммерции, были выполнены ботами в текущем году, по сравнению с тридцатью тремя процентами в остальных отраслях.

Это также указывает на то, что предприятия электронной коммерции являются основными целями для киберпреступников и хакеров данных, что также приводит к огромному разрыву между покупателями и продавцами. Поскольку препятствия и препятствия в международной цепочке поставок затягиваются в сезон отпусков, праздников и праздничных покупок в текущем году, продавцы могут предвидеть дополнительные потрясения и искажения, вызванные кибератаками и вторжениями.

Imperva Research Labs по рискам кибербезопасности, влияющим на электронную торговлю, в опубликованном отчете признает, что они раскрыли ситуацию и условия безопасности в текущем году в отчете по электронной коммерции, который охватывал данные, полученные из их многонациональной сети за весь год, то есть Обобщенный годовой отчет, включающий более трехсот шестидесяти миллионов атак онлайн-приложений на триллионы запросов протокола передачи гипертекста.

Вскоре наступает период праздничных покупок в этом году, и они ожидают, что безопасность по-прежнему представляет собой опасность, и риски будут продолжать расти в текущем месяце, то есть в ноябре текущего года, поскольку покупатели стекаются за покупками для разнообразных и разнообразных закупочных сделок и событий.

Они также утверждают, что, просматривая этот отчет за текущий год, можно накопить полезные идеи и знания о сути и столкновении таких атак и ударов,

нацеленных на его учреждение, помогая всем на переднем крае иммунитета и безопасности веб-сайтов.

Автоматическая активность ботов - серьезная угроза для электронной коммерции. В текущем году процент ежемесячных атак ботами на форумах розничных продавцов увеличился на тринадцать по сравнению с предыдущим годом. Следует отметить, что доля замысловатых ужасных ботов в розничных сетях также выросла в текущем году. Эта модель и разновидность бота, которую сложнее всего предотвратить, потому что они производят и стимулируют движения курсора и действуют аналогично человеку-оператору. Сложные боты ускользают от скромных мер безопасности и несут ответственность только за взлом учетных записей, вымогательство, мошенничество и отказ от инвентаря, из-за которых подлинным и законным потребителям трудно покупать продукты, которые они предпочитают и желают.

Еще одно открытие, которое подчеркивает более непосредственное влияние на клиентов, заключается в том, что тридцать два целых восемь десятых процента всех входов в розничную сеть определили, что в текущем году стремится захватить счета, что на двадцать пять целых пять десятых процента выше, чем стандарт для остальных отраслей…». ***(Arooj Ahmed. More than half of the entire eCommerce cyberattacks and invasions are bot-driven, reveals new report // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/more-than-half-of-entire-ecommerce.html). 10.11.2021).***

***

«Публичные сообщения о компьютерных преступлениях стремительно растут благодаря огромному росту утечек данных, даже несмотря на то, что преследование нарушителей Закона о неправомерном использовании компьютеров сокращается.

Исследование преступности в Англии и Уэльсе показало, что за 12 месяцев, закончившихся в июне 2021 года, было зафиксировано 1,8 миллиона преступлений, связанных с неправильным использованием компьютеров, что соответствует количеству, зафиксированному в 2017 году.

«Это на 85% больше по сравнению с годом, закончившимся в июне 2019 года, в основном за счет увеличения на 161% количества правонарушений, связанных с «несанкционированным доступом к личной информации (включая взлом)», - заявило Управление национальной статистики, которому принадлежит опрос.

Джед Кафец, руководитель отдела тестирования на проникновение в британской компании Redscan, занимающейся информационными технологиями, назвал последнюю статистику «полезным барометром для понимания того, как киберпреступность влияет на граждан Великобритании в их повседневной жизни».

«По оценкам, 1,8 миллиона правонарушений, связанных с неправильным использованием компьютеров, будут лишь долей реального числа, если учесть, сколько деталей утеряно, украдено и продано во время утечки больших данных в течение обычного года», - сказал довольно мрачный Кафец. «Я уверен, что о

хакерских атаках очень мало сообщается, потому что люди все чаще ожидают их в повседневной жизни».

УНС добавило, что согласно проведенному в 2019 году опросу, 68% тех, кто сообщил о том, что они были причастны к утечке данных, заявили, что они «совсем не пострадали» от нее.

За 11 месяцев с июля 2017 года по июнь 2018 года Обследование преступности зафиксировало 1,1 миллиона преступлений, связанных с «неправильным использованием компьютера» в телефонном опросе репрезентативной выборки британцев на национальном уровне, хотя УНС заявило, что эти цифры несопоставимы с телефонным опросом на этой неделе, поскольку Данные старшего возраста включают подростков в возрасте 16–18 лет и не ограничиваются только взрослыми.

Данные опроса отличаются от данных, собранных полицией, потому что, по заявлению УНС, оно собирает информацию о преступлениях, о которых не сообщается в полицию.

Несмотря на резкий рост числа преступлений, связанных с неправильным использованием компьютеров, число судебных преследований, возбужденных в соответствии с Законом о неправомерном использовании компьютеров за аналогичный период времени, снизилось на 20 процентов.

Сообщение в полицию о неправомерном использовании компьютера может иметь разные результаты. В 2019 году мы сообщали, что отчеты о преступлениях в Action Fraud редко делают больше, чем просто добавляются в строку таблицы. В то время как полиция и связанные с ней агентства особенно хороши, в Великобритании отвлекают своенравную молодежь от взлома и в пользу законного выбора в области информационной безопасности, необходимо соблюдать баланс между уклонением от расследований и судебного преследования и обеспечением фактического соблюдения закона». ***(Gareth Corfield. Computer misuse crimes in UK surge to high not seen since 2017 even as prosecutions slump 20% // The Register (https://www.theregister.com/2021/11/08/computer_misuse_crimes_ons_crime_survey/) . 08.11.2021).***

***

«Общественные компьютеры публичной библиотеки округа Толедо Лукас и доступ к Wi-Fi были восстановлены после атаки кибербезопасности, а также ее функции общедоступного каталога.

Библиотечная система сообщила, что расследование атаки продолжается, и если какая-либо конфиденциальная информация была скомпрометирована, она свяжется с любыми затронутыми людьми. Он заверяет общественность, что не хранит информацию о чьих-либо кредитных картах, номерах социального страхования или истории займов.

В пресс-релизе говорилось, что библиотеке необходимо изучить свои системы, прежде чем вернуть все в онлайн.

«Это включает в себя надежную систему каталогов, обслуживающую почти 300 000 держателей карт в 20 местах; 90 серверов; 1500 общественных и служебных компьютеров; веб-сайт, который посещают более 1 миллиона раз в месяц; и сложный

центр обработки данных, который контролируется 24/7 для обработки запросов от наших пользователей и защиты от угроз кибербезопасности», - говорится в релизе. «Всю нашу операцию пришлось отключить, провести расследование на предмет сохраняющихся угроз, а затем тщательно вернуть в оперативный режим, чтобы гарантировать, что уязвимости не сохранятся».

Он добавил, что TLCPL не платила выкуп и не планирует этого делать». ***(Toledo Lucas County Public Library services back online after cybersecurity attack // 13abc.com (https://www.13abc.com/2021/11/15/toledo-lucas-county-public-library-services-back-online-after-cybersecurity-attack/). 15.11.2021).***

***

«Новая волна атак, начавшаяся в конце прошлой недели, взломала около 300 сайтов WordPress для отображения поддельных уведомлений о шифровании, пытаясь обманом заставить владельцев сайтов заплатить 0,1 биткойна за восстановление.

Эти требования о выкупе сопровождаются таймером обратного отсчета, чтобы вызвать чувство срочности и, возможно, паниковать веб-администратором, чтобы он заплатил выкуп.

Хотя спрос на выкуп в размере 0,1 биткойна (~ 6069,23 доллара США) не особенно значителен по сравнению с тем, что мы наблюдаем в случае громких атак программ-вымогателей, для многих владельцев веб-сайтов он все же может быть значительной суммой.

Эти атаки были обнаружены фирмой по кибербезопасности Sucuri, которую наняла одна из жертв для реагирования на инциденты.

Исследователи обнаружили, что веб-сайты не были зашифрованы, а скорее злоумышленники модифицировали установленный плагин WordPress, чтобы отображать записку о выкупе и обратный отсчет, когда помимо отображения записки о выкупе, плагин изменял все сообщения в блоге WordPress и устанавливал их ' post_status 'на' null ', в результате чего они переходят в неопубликованное состояние.

Таким образом, актеры создали простую, но мощную иллюзию, из-за которой все выглядело так, как будто сайт был зашифрован.

Удалив плагин и запустив команду для повторной публикации сообщений и страниц, сайт вернулся к своему нормальному состоянию.

После дальнейшего анализа журналов сетевого трафика Сукури обнаружил, что первой точкой, где появился IP-адрес актера, была панель wp-admin.

Это означает, что злоумышленники вошли в систему как администраторы на сайте, либо путем подбора пароля, либо путем получения украденных учетных данных с рынков даркнета.

Это не была единичная атака, а скорее похоже на более широкую кампанию, которая придает больший вес второму сценарию.

Что касается плагина, который видел Sucuri, это был Directorist, который представляет собой инструмент для создания списков бизнес-каталогов на сайтах.

Sucuri отследила примерно 291 веб-сайт, затронутый этой атакой, при этом поиск в Google показал сочетание очищенных сайтов и тех, которые все еще показывают записки о выкупе.

Все сайты, которые BleepingComputer видит в результатах поиска, используют один и тот же биткойн-адрес 3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc, который не получил никаких выкупных платежей.

Защита от шифрования сайта

Сукури предлагает следующие методы безопасности для защиты сайтов WordPress от взлома:

Проверьте пользователей с правами администратора на сайте, удалите все поддельные учетные записи и обновите / измените все пароли wp-admin.

Защитите свою страницу администратора wp-admin.

Измените пароли других точек доступа (база данных, FTP, cPanel и т.д.).

Разместите свой сайт за брандмауэром.

Следуйте надежным методам резервного копирования, которые упростят восстановление в случае реального инцидента с шифрованием.

Поскольку WordPress часто является целью злоумышленников, также важно убедиться, что все установленные вами плагины работают с последней версией.

Обновление 18 ноября - BleepingComputer получил известие о недавнем исправлении в плагине Directorist, устраняющем ошибку, которая позволяла пользователям с низкими привилегиями запускать произвольный код.

Хотя в отчете Сукури плагин не рассматривается как точка проникновения, существование этой уязвимости имеет смысл в контексте конкретной атаки.

Это также означает, что очистка от инфекции и восстановление сайта не помешают актерам нанести новый удар, пока плагин Directorist остается в более старой уязвимой версии». ***(Bill Toulas. WordPress sites are being hacked in fake ransomware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/wordpress-sites-are-being-hacked-in-fake-ransomware-attacks/). 16.11.2021).***

***

«Центр Microsoft Threat Intelligence Center (MSTIC) представил на CyberWarCon 2021 анализ эволюции нескольких иранских субъектов угроз, и их результаты показывают, что атаки становятся все более изощренными.

С сентября 2020 года Microsoft отслеживает шесть иранских хакерских групп, развертывающих программы-вымогатели и вывозящие данные, чтобы вызвать сбои и разрушения для жертв.

Со временем эти хакерские группы превратились в компетентных злоумышленников, способных вести кибершпионаж, использовать многоплатформенные вредоносные программы, нарушать работу программ-вымогателей и программ-вымогателей, проводить фишинговые атаки и атаки с использованием паролей и даже настраивать сложные операции цепочки поставок.

Все эти группы развертывают программы-вымогатели для достижения своих целей, и их развертывание происходит волнами, обычно с интервалом от шести до восьми недель.

В этом году Microsoft наблюдала, как акторы сканируют множество уязвимостей, в том числе нацелены на Fortinet FortiOS SSL VPN, серверы Microsoft Exchange, уязвимые для ProxyShell, и многое другое.

Подсчитано, что только путем сканирования непропатченных систем Fortinet VPN в этом году участники получили более 900 действительных учетных данных в текстовой форме.

Сбор учетных данных пациента

Еще одна тенденция, проявившаяся в прошлом году, - это повышенный уровень терпения и настойчивости в кампаниях социальной инженерии, что свидетельствует о наличии опытного актера.

Раньше такие актеры, как Phosphorus (Очаровательный котенок), рассылали нежелательные электронные письма с вредоносными ссылками и зашнурованными вложениями - массовая тактика, которая имела ограниченный успех.

Теперь Phosphorus следует по трудоемкому пути «приглашений на собеседование» - методу, введенному северокорейской хакерской группой «Lazarus».

Во время этих атак субъекты Phosphorus вызывают цели и проходят через них, нажимая на страницы сбора учетных данных как часть процесса интервью.

Новая группа, которая придерживается столь же терпеливой тактики, называется «Куриум», и аналитики Microsoft говорят, что этот актер использует обширную сеть поддельных учетных записей в социальных сетях, обычно маскирующихся под привлекательных женщин.

Они связываются с целями и через некоторое время устанавливают взаимопонимание, ежедневно болтают и завоевывают их доверие.

Затем в один прекрасный день они отправляют вредоносный документ, похожий на безобидные файлы, отправленные ранее, что приводит к скрытому удалению вредоносных программ.

Похожую тактику использовала хакерская группа, связанная с ХАМАСом, которая создавала поддельные приложения для знакомств, чтобы заманить Силы обороны Израиля (IDF) на установку мобильных приложений, зараженных вредоносным ПО.

Неясно, связаны ли эти две кампании.

Грубое проникновение внутрь

Хотя некоторые участники действуют более методично, другие предпочитают использовать атаки «грубой силы» для агрессивного получения доступа к учетным записям Office 365.

Одним из таких злоумышленников является DEV-0343, который в прошлом месяце был замечен нацелившимся на американские оборонные технологические компании и проводившим массовые атаки с использованием паролей.

Microsoft сообщает, что DEV-0343 перемещается намного быстрее, чем группы, упомянутые выше, обычно получая доступ к целевым учетным записям в тот же день.

Кроме того, исследователи увидели совпадения, такие как одновременное нацеливание на определенные учетные записи операторами DEV-0343 и «Европиум», явное свидетельство скоординированных действий.

Иранские хакеры продолжают развиваться

Microsoft отслеживает иранских игроков почти десять лет назад, и технологический гигант добился определенного успеха в отключении части своей инфраструктуры.

Несмотря на эти усилия, Phosphorus удалось нанести серьезные удары, ярким примером которых является взлом высокопоставленных чиновников в октябре прошлого года.

Последние наблюдения MSTIC подчеркивают, что Phosphorus не только жив и здоров, но и представляет собой изменяющую форму угрозу, поддерживаемую сторонниками беспрецедентного плюрализма». ***(Bill Toulas. Microsoft warns of the evolution of six Iranian hacking groups // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-warns-of-the-evolution-of-six-iranian-hacking-groups/). 16.11.2021).***

***

«В третьем квартале общее число DDoS-атак увеличилось почти на 23,5% по сравнению с аналогичным периодом 2020 г., а продвинутых (которые часто являются целевыми) – на 31,4%, утверждается в отчете «Лаборатории Касперского». Кроме того, в августе был поставлен рекорд по количеству таких инцидентов в день за последние несколько лет – 8825. Средняя и максимальная продолжительность DDoS-атак снизились и составили 2,84 часа и 339 часов соответственно. Большинство нападений представляли собой SYN-флуд.

В числе крупнейших целей – организации, борющиеся с пандемией, государственные учреждения, разработчики игр и специализирующиеся на кибербезопасности медиа. Больше всего атакованных ресурсов располагалось в США, Гонконге и Китае. Эксперты зафиксировали серию политически мотивированных атак в Европе и Азии, атаки на разработчиков игр и на образовательные ресурсы.

Для проведения некоторых крупных DDoS-атак в третьем квартале использовался новый мощный ботнет Mzris, который состоит из производительных сетевых устройств (преимущественно компании Mikrotik) и использует в атаках технику конвейерной обработки HTTP. С его помощью были атакованы, в том числе два известных медиа по кибербезопасности – блог Krebs on Security и журнал InfoSecurity Magazine.

Также третий квартал принес два новых вектора DDoS-атак, потенциально представляющих серьезную угрозу, в том числе для крупных веб-ресурсов. Группа исследователей из Мэрилендского университета и Колорадского университета в Боулдере нашла способ подделывать IP-адрес жертвы по протоколу TCP. Атака, описанная исследователями, злоупотребляет устройствами безопасности, расположенными между клиентом и сервером (так называемыми мидлбоксами) – брандмауэрами, балансировщиками нагрузки, NAT, DPI (Deep Packet Inspection) и др. Если отправить на такое устройство запрос от имени жертвы на обращение к запрещенному ресурсу, ответ может значительно превосходить его по размеру. Так, исследователи обнаружили более 386 тыс. устройств, дающих фактор амплификации свыше 100, из них более 97 тыс. могут усиливать атаку более чем в 500 раз, а 192 – более чем в 51 тыс. раз.

Вторая атака, описанная компанией Nexusguard и получившая название Black Storm, позволяет злоупотреблять любыми сетевыми устройствами. Злоумышленник может отправлять запросы на закрытые порты устройств в сети поставщика услуг связи (CSP) от имени других устройств, находящихся в той же сети. Устройства-получатели отвечают на такие запросы сообщением о том, что порт недоступен. Эти сообщения потребляют много ресурсов при обработке, в результате устройства-жертвы оказываются перегружены и неспособны принимать легитимные запросы. Исследователи отмечают, что этот метод позволяет злоумышленнику вывести из строя не только отдельные серверы, но и всю сеть провайдера, в том числе крупного». ***(Количество DDoS-атак в третьем квартале выросло на четверть // Компьютерное Обозрение (https://ko.com.ua/kolichestvo_ddos-atak_v_tretem_kvartale_vyroslo_na_chetvert_139362). 12.11.2021).***

***

«Компанія Eset повідомляє про виявлення цілеспрямованих атак на сайти медіа-компаній, державних установ та інтернет-провайдерів. Зокрема цілі кіберзлочинців знаходяться у Європі, на Близькому Сході та в Південній Африці.

У цих атаках зловмисники компрометують сайти, які можуть відвідати потенційні цілі, для подальшого інфікування їхніх пристроїв. Деякі користувачі таких сайтів, ймовірно, стали жертвою атаки через експлойт в браузері. Однак ні експлойт, ні фінальний компонент виявити не вдалося.

Варто зазначити, що скомпрометовані вебсайти використовуються лише як початковий вектор інфікування зловмисниками своїх цілей.

Зокрема цілями кіберзлочинців стали сайти ЗМІ у Великій Британії, Ємені та Саудівській Аравії, а також вебресурси аерокосмічних та військово-технологічних компаній в Італії та Південній Африці.

«Зловмисники також створили фальшивий вебсайт "Всесвітнього медичного форуму MEDICA", який проходив у Німеччині. Найімовірніше, кіберзлочинці не змогли зламати офіційний сайт, тому створили підроблений, щоб вставити свій шкідливий код», – пояснює Матьє Фау, дослідник Eset.

Під час кампанії 2020 року шкідливе програмне забезпечення перевіряло операційну систему та браузер. Оскільки цей процес базувався на програмному забезпеченні для комп'ютерів, кампанія не була націлена на мобільні пристрої. Наступного разу зловмисники, щоб бути трохи непомітнішими, почали модифікувати скрипти, які вже були на скомпрометованих сайтах.

Існує велика ймовірність, що кіберзлочинці є клієнтами компанії Candiru, яка пропонує державним установам інструменти для кібершпигунства.

Активність цієї операції зменшилась наприкінці липня 2021 року невдовзі після повідомлень про діяльність Candiru в блогах Citizen Lab, Google та Microsoft. Ймовірно, кіберзлочинці беруть паузу, щоб удосконалити свої інструменти для уникнення виявлення». ***(Кіберзлочинці атакують державні установи та медіа-компанії через скомпрометовані вебсайти // Компьютерное Обозрение (https://ko.com.ua/kiberzlochinci_atakuyut_derzhavni_ta_novinni_sajti_cherez_skomprometovani_vebsajti_139411). 17.11.2021).***

***

«Специалисты компании Cloudflare нейтрализовали мультивекторную распределенную атаку типа «отказ в обслуживании» (DDoS), максимальная мощность которой составила почти 2 Тбит/с.

Атака продолжалась одну минуту, включала DNS-усиление и UDP-флуд, а также была осуществлена с использованием примерно 15 тыс. ботов. Боты запускали вариант вредоносного кода Mirai на скомпрометированных IoT-устройствах и экземплярах GitLab, содержащих уязвимость CVE-2021-22205. Критическая уязвимость позволяет удаленно запускать код. Проблема получила максимальную оценку в 10 баллов по шкале CVSS. В апреле нынешнего года было выпущено исправление для этой уязвимости, но, по словам исследователей, проблема до сих пор присутствует на тысячах систем.

Как отметили в Cloudflare, общее количество DDoS-атак терабитной мощности увеличилось в третьем квартале года. Количество инцидентов на сетевом уровне выросло на 44% по сравнению с предыдущим кварталом.

Напомним, ранее специалисты компании Microsoft зафиксировали DDoS-атаку мощностью в 2,4 Тбит/с в августе нынешнего года. Атака была нацелена на клиента Microsoft Azure в Европе и на 140% превышала максимальную пропускную способность атаки, зафиксированной Microsoft в 2020 году. Атака длилась более 10 минут с кратковременными всплесками трафика, достигающими пиковой мощности в 2,4 Тбит/с, 0,55 Тбит/с и 1,7 Тбит/с. Azure смогла оставаться в сети на протяжении всей атаки». ***(Cloudflare нейтрализовала мощную многовекторную DDoS-атаку // SecurityLab.ru (https://www.securitylab.ru/news/526605.php). 16.11.2021).***

***

«Второй по величине производитель пива в Испании Damm был вынужден приостановить производство на своей основной пивоварне за пределами Барселоны в результате кибератаки.

Атака на несколько часов «полностью парализовала» завод в Эль-Прат-де-Льобрегат. Об этом сообщила информагентству Reuters глава отдела коммуникаций Damm Ольга Видаль (Olga Vidal).

Видель отказалась сообщать, требовали ли злоумышленники от компании выкуп. Также неизвестно, уведомила ли компания правоохранительные органы об инциденте.

Помимо всемирно известного бренда Estrella Damm, испанская пивоварня Damm производит несколько других брендов пива (Voll-Damm, Xibeca, Estrella Levante). Пивоварня смогла выполнить все поставки в бары, рестораны и супермаркеты только благодаря имеющимся запасам». ***(Кибератака нарушила производство на заводе крупного испанского производителя пива Damm // SecurityLab.ru (https://www.securitylab.ru/news/526552.php). 15.11.2021).***

***

«42% геймеров в Великобритании сталкивались с кибератаками на свои игровые учетные записи или устройства. К такому выводу пришли специалисты компании NortonLifeLock, опросившие 700 взрослых геймеров.

Согласно исследованию NortonLifeLock, самым распространенным типом атак на любителей компьютерных игр являются атаки на игровые девайсы с использованием вредоносного ПО (20%), похищение цифровой валюты, персонажей и предметов (12%) и неавторизованнй доступ к игровому online-аккаунту (12%). Более трех четвертей (78%) пострадавших признались, что в результате атак потеряли деньги (в среднем J145).

Почти у каждого пятого (19%) заядлого геймера злоумышленники похитили и опубликовали персональную информацию (так называемый doxing или доксинг).

Более четверти респондентов (28%) признались, что сами не прочь взломать игровую учетную запись друга, члена семьи или парня/девушки, если это позволит им получить преимущество в игре. Среди заядлых геймеров этот показатель еще выше и составляет 48%.

43% респондентов не прочь также воспользоваться лазейкой или багом в игре. Треть (34%) не брезгует установкой читов, а 30% согласны покупать чужие учетные записи.

Исследование также показало, что британские геймеры не особо пекутся о безопасности, что делает их уязвимыми к кибератакам. К примеру, около половины респондентов используют одни и те же имена пользователя (54%) и пароли (46%) для нескольких игровых учетных записей. 38% геймеров во время игры используют публичные сети Wi-Fi, 37% раскрывают свои персональные данные (например, имена и даты рождения), 29% используют более дешевые или бесплатные версии игры и еще 29% загружают дополнения (аддоны) с посторонних web-сайтов, не имеющих отношения к дистрибьютору игры». ***(Британские геймеры плюют на безопасность // SecurityLab.ru (https://www.securitylab.ru/news/526585.php). 16.11.2021).***

***

«Министерство цифрового развития, связи и массовых коммуникаций РФ заявило, что на портал «Госуслуг» второй день подряд направлена мощнейшая кибератака, говорится в сообщении официального Telegram-канала Минцифры.

«Портал госуслуг находится под беспрецедентной кибератакой. «Госуслуги» второй день подвергаются самой мощной за всё время функционирования портала кибератаке. Первая атака мощностью свыше 680 гигабит в секунду была зафиксирована 10 ноября 2021 года. 11 ноября в течение 20 минут некоторые пользователи столкнулись со сложностями входа на портал», — говорится в сообщении министерства, размещенном в его Telegram-канале.

У некоторых пользователей в течение 20 минут возникали проблемы со входом на портал, отметили в ведомстве. Экспериментальный чат-бот Макс какое-то время не по шаблону отвечал на вопросы о вакцинации. На вопрос о том, как получить QR-код для переболевшего, бот ответил, что коронавируса не существует, а факт болезни никем не доказан.

В настоящее время бот функционирует в штатном режиме». ***(Взломанный чат-бот Госуслуг отрицает существование коронавируса // SecurityLab.ru (https://www.securitylab.ru/news/526489.php). 11.11.2021).***

***

«Аналитики компании StormWall зафиксировали всплеск DDoS и других хакерских атак на сектор e-commerce в начале ноября этого года. Из-за ограничений, связанных с COVID-19, популярность онлайн-шопинга в начале ноября выросла, и на эту ситуацию моментально отреагировали хакеры. Злоумышленники стремились создать проблемы в работе сайтов ритейлеров, запуская DDoS-атаки, а также пытались взломать аккаунты пользователей интернет-магазинов с помощью умных ботов.

В основном, DDoS-атаки осуществлялись по протоколу HTTP, а их средняя мощность составляла 100 Гбит/с. Самое большое число DDoS-атак было направлено на онлайн-магазины по продаже техники (45%), одежды и обуви (32%) и косметики (17%). Также хакеры атаковали интернет-магазины по продаже мебели (3%), товаров для дома (2%) и другие (1%). Основным мотивом DDoS-атак являлось вымогательство, но также причиной могла быть конкурентная борьба, которая обычно усиливается в конце года.

Для организации атак с целью взлома аккаунтов пользователей злоумышленники использовали умных ботов, которые обходят большинство традиционных средств защиты. Для защиты от таких ботов необходимо использовать специализированные решения, такие как WAF (Web Application Firewall), позволяющие фильтровать атаки по множеству параметров. Хакеры пытались взломать аккаунты пользователей, желая обогатиться, злоумышленники хотели получить доступ к данным, чтобы потом продать их на черном рынке. Кроме того, хакеры могут использовать данные с целью вымогательства и шантажа.

Эксперты ожидают новых всплесков DDoS-атак и хакерских атак на ритейл в ноябре этого года в связи с предстоящей “черной пятницей” и сезоном распродаж.

Специалисты советуют онлайн-ритейлерам заранее подготовиться к повышенной хакерской активности. По мнению экспертов, для защиты онлайн-ресурсов от кибератак во время распродаж лучше всего использовать профессиональные Anti-DDoS решения вместе с сервисом WAF». ***(В начале ноября 2021 года сектор e-commerce подвергся кибератакам // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5862731-V-nachale-noyabrya-2021-goda-sektor.html). 18.11.2021).***

***

«Больница в Портсмуте, штат Огайо, все еще пытается полностью выздороветь - продолжает отменять и откладывать некоторые услуги по уходу за пациентами - через неделю после того, как она обнаружила, что хакеры получили доступ к некоторым из ее серверов, что, по ее словам, выглядело как «целенаправленная кибератака».

Медицинский центр Южного Огайо (SOMC) сообщил 11 ноября в социальных сетях, что «неавторизованная третья сторона» получила доступ к его серверам и что

больница на 248 коек перенаправляет машины скорой помощи с пациентами скорой помощи в другие больницы, но по-прежнему обслуживает пациентов.

К следующему дню SOMC прекратил отвлекать машины скорой помощи, но в течение недели, включая четверг, по-прежнему отменял или переносил многие услуги по уходу за пациентами, в том числе приемы в лабораторию сна, тесты функции легких и амбулаторную реабилитацию, поскольку он продолжал устранять широко распространенные отключения. включая электронную почту.

«Мы работаем круглосуточно, чтобы получить полную функциональность», - заявил в четверг Information Security Media Group представитель SOMC. Он сказал, что больница надеется на полное выздоровление «как можно скорее», но у него не было графика, когда это может произойти.

Представитель отказался обсуждать, какие ИТ-системы все еще были затронуты, а также подробности атаки, в том числе о том, была ли она связана с программами-вымогателями или злоумышленники требовали выкуп, заявив, что инцидент расследуется.

SOMC, которая обычно предлагает широкий спектр медицинских услуг, включая неотложную, хирургическую, амбулаторную и хосписную помощь, отметила на своей странице в Facebook, что она работает с федеральными правоохранительными органами и охранными фирмами для расследования инцидента.

Подобные атаки

Ситуация с SOMC - одна из растущих жертв недавних кибератак на медицинские учреждения, приведших к критическим отключениям ИТ, что привело к сбою в предоставлении услуг по уходу за пациентами.

В августе медицинская организация Memorial Health System в Мариетте, штат Огайо, пострадала от очевидного инцидента с использованием программы-вымогателя, который нарушил работу служб по уходу за пациентами, что побудило организацию временно перенаправить пациентов неотложной помощи из трех своих больниц в другие медицинские учреждения.

Кроме того, кибератака в июле на DuPage Medical Group, крупнейшую многопрофильную группу специалистов в Иллинойсе, вызвала сбой в работе сетевой системы, что, среди прочего, привело к тому, что пациенты не смогли позвонить в офисы своих врачей и получить доступ к медицинским записям в Интернете.

В сентябре DuPage сообщила федеральным регулирующим органам об утечке данных, затронувшей более 655 000 человек, причастных к инциденту со взломом.

Одной из самых заметных атак в этом году стала майская атака вымогателей на компанию Scripps Health из Сан-Диего, которая привела к отключению системы почти на месяц.

Калифорнийская организация сообщила в августе финансовым регулирующим органам, что инцидент с безопасностью обошелся почти в 113 миллионов долларов, включая 91,6 миллиона долларов потерянной прибыли. Ожидается, что около 21 миллиона долларов будет покрыто страховкой, сообщила компания.

После этого инцидента против Scripps Health было подано несколько предложенных коллективных исков.

В июне Scripps Health сообщила о взломе в Министерство здравоохранения и социальных служб как о нарушении HIPAA, затронувшем более 147 000 человек.

Ярким примером того, как кибератака помешала лечению пациентов, является то, что в прошлом году мать подала иск о злоупотреблении служебным положением против Мобайл, Медицинский центр Спрингхилла в штате Алабама, утверждая, что у ее ребенка возникли осложнения при родах, а затем он умер в результате атаки вымогателя в июле 2019 года. больница, которая, по ее словам, препятствовала доступу врачей к своевременному мониторингу состояния плода и другим системам во время ее родов.

Планировать заранее

Джон Мур, главный специалист по рискам консалтинговой компании Clearwater по вопросам конфиденциальности и безопасности, говорит, что лучшая сторона некоторых из этих недавних громких атак на сектор здравоохранения заключается в том, что за последние шесть месяцев он увидел «видимый рост» числа организаций, укрепляющих свои позиции. их меры безопасности.

«Эта тенденция вызвана продолжающимися атаками программ-вымогателей и фишинговыми атаками, повышенным вниманием инвесторов, советов директоров и высшего руководства, а также ужесточением требований страховщиков кибербезопасности», - отмечает он.

Но плохая новость, по его словам, заключается в том, что он по-прежнему видит, что многие организации по-прежнему отстают в своих средствах контроля, ориентированных на восстановление.

«Самая большая ошибка, которую мы видим, - это отсутствие подготовки и практики до того, как критическая система будет потеряна», - говорит Мур.

По его словам, зачастую организации готовят планы обеспечения непрерывности бизнеса и аварийного восстановления без участия бизнес-подразделений, что приводит к неэффективному распределению и приоритизации ресурсов.

«Планирование и отработка восстановления не могут быть эффективно выполнены силами специалистов по кибербезопасности или ИТ-специалистов. Также должны быть задействованы руководители высшего звена в бизнес-подразделениях.

«Мы видим, что планы и процессы не проходят проверку и терпят неудачу, когда организации пытаются реализовать их под давлением. Мы видим, что организации теряют драгоценное время, потому что управление процессом восстановления не документируется и не практикуется, оставляя вопросы о том, кто за что отвечает».

По словам Мура, процесс планирования непрерывности бизнеса должен начинаться с анализа воздействия на бизнес, чтобы понять критичность систем для бизнеса, влияние или стоимость сбоя этих систем и определенных целей восстановления, включая системы и данные.

Затем, по его словам, отделам кибербезопасности и ИТ необходимо разработать планы обеспечения непрерывности бизнеса и аварийного восстановления, включая стратегию резервного копирования и процессы, которые позволят достичь этих целей.

«Наконец, организации необходимо практиковать реагирование и восстановление, в том числе регулярные настольные упражнения с участием старших руководителей бизнеса и отработку процессов восстановления, чтобы убедиться, что они функционируют, как задумано, и являются эффективными». ***(Marianne Kolbasuk McGee. Ohio Hospital Still Struggling One Week After Cyberattack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ohio-hospital-still-struggling-one-week-after-cyberattack-a-17943). 18.11.2021).***

***

«Правительство США предупредило все предприятия, что они подвергаются повышенному риску сетевых атак во время праздника Благодарения.

«Злоумышленники не планируют такие праздники, как вы», - предупреждает совместное предупреждение ФБР и Агентства по кибербезопасности и безопасности инфраструктуры.

«Недавняя история говорит нам, что это может быть время, когда эти постоянные кибер-игроки на другом конце света ищут способы - большие и маленькие - нарушить работу критически важных сетей и систем, принадлежащих организациям, предприятиям и критической инфраструктуре», - добавляет он.

Подобные предупреждения неоднократно выдавались ФБР и CISA в последние месяцы перед другими праздниками. Как и прежде, Белый дом не сообщил, что у него есть какая-либо конкретная информация о запланированных атаках или о любых злоумышленниках, которые, возможно, уже находятся в корпоративных сетях и готовы сигнализировать о своей вредоносной программе для криптоблокировки, чтобы принудительно зашифровать каждую возможную конечную точку.

«Хотя ни CISA, ни ФБР в настоящее время не выявили каких-либо конкретных угроз, последние тенденции 2021 года показывают, что злоумышленники в киберпространстве начинают серьезные и эффективные атаки программ-вымогателей в праздничные и выходные дни, включая День независимости и выходные дни Дня матери», - говорится в предупреждении.

Действительно, многие крупные атаки продолжают совершаться, когда у предприятий меньше рук. Например, накануне праздничных выходных четвертого июля злоумышленники, использующие программу-вымогатель REvil, также известную как Sodinokibi, воспользовались уязвимостью в программном обеспечении для удаленного управления ИТ, разработанном поставщиком программного обеспечения Kaseya и используемым поставщиками управляемых услуг. Злоумышленники смогли использовать программное обеспечение Kaseya для распространения своего вредоносного ПО клиентам 50 различных поставщиков услуг Интернета, в конечном счете, систем криптоблокировки, используемых до 1500 организаций.

Но злоумышленники не всегда ждут праздников. Например, бангладешский банк подвергся нападению в пятницу - мусульманский день молитвы в стране, - что

привело к убыткам в размере 81 миллиона долларов. Между тем атаки на немусульманские страны часто начинаются в субботу.

Невозможно предсказать, когда злоумышленники, стоящие за каким-либо конкретным инцидентом, могут нанести удар, говорит Девон Акерман, управляющий директор и руководитель службы реагирования на инциденты в Северной Америке в нью-йоркской консалтинговой компании Kroll's по киберрискам. «Но группы злоумышленников, как правило, наносят удары в те сроки, в которых их наименьшая вероятность быть обнаруженными», - говорит он. «Ночью, в выходные дни, во время выходных в США для многих предприятий и корпоративных сетей - неудачное время, чтобы заметить, когда больше людей, скорее всего, находится вдали от своих клавиатур, а не у них».

С чего начать

Эксперты отмечают, что в центре внимания предупреждения CISA и ФБР не говорится, что небо падает. Скорее, они используют склонность злоумышленников как напоминание организациям, чтобы они были готовы.

«Если вы не задумались об этом в преддверии праздников, это должна быть принудительная функция для запуска», - говорит Сэм Карри, руководитель службы безопасности фирмы Cybereason, о последнем сообщении.

В частности, он рекомендует быть готовым к отражению фишинговых атак, финансовых мошенников и поддельных сайтов, особенно в период Черной пятницы. Он также призывает компании иметь хорошо протестированные планы реагирования на инциденты и коммуникационные стратегии, разработанные для работы даже в случае атаки программы-вымогателя, при которой теряется весь доступ к ИТ-инфраструктуре.

В справочнике также рекомендуется:

Назначение ответчиков: «Определите сотрудников ИТ-безопасности на выходные и праздничные дни, которые будут доступны для всплеска в это время в случае инцидента или атаки программы-вымогателя».

Использование MFA: «Реализуйте многофакторную аутентификацию для удаленного доступа и административных учетных записей».

Надежные пароли: «Установите надежные пароли и убедитесь, что они не используются повторно в нескольких учетных записях».

Защита RDP: «Если вы используете протокол удаленного рабочего стола или любую другую потенциально опасную службу, убедитесь, что она защищена и находится под контролем».

Повышение осведомленности: «Напомните сотрудникам не переходить по подозрительным ссылкам и проведите упражнения для повышения осведомленности».

В целях повышения устойчивости бизнеса

Организации с более зрелыми подходами уже делают все эти вещи и пересмотрели свое внимание не только на «киберустойчивость», но и на «устойчивость бизнеса», - говорит Рокко Грилло, управляющий директор по глобальным расследованиям киберрисков и реагированию на инциденты в Нью-Йорке. консалтинговая компания Alvarez & Marsal.

Но непрерывные темпы атак программ-вымогателей и их сбои помогают продемонстрировать, что не у всех есть достаточно хорошие средства защиты, особенно с учетом того, что группы, использующие программы-вымогатели, в течение последних пяти лет продолжали вводить новшества. «Во всяком случае, за последние шесть-12 месяцев это превратилось в эпидемию», - говорит Грилло.

Тем не менее, недавний опрос жертв программ-вымогателей, проведенный Cybereason, показал, что многие из них до сих пор не усовершенствовали свои методы реагирования на инциденты.

Из 1200 опрошенных специалистов по безопасности в организациях, которые ранее подвергались атакам с использованием программ-вымогателей, треть заявили, что, по их мнению, инцидент «прошел успешно, потому что не было плана на случай непредвиденных обстоятельств и реагировало лишь ограниченное количество сотрудников», - говорит Сайберисон. Кроме того, 24% заявили, что атака не привела к тому, что их организация создала новые планы действий в чрезвычайных ситуациях на выходные или праздничные дни, чтобы обеспечить более быстрое реагирование.

Основы: мониторинг, обнаружение, реагирование

Что фирмы могли бы сделать лучше? Не каждую атаку можно остановить сразу, что усиливает потребность в «лучшем мониторинге, лучшем обнаружении и последующем реагировании», - говорит Грилло. «План реагирования не предназначен для предотвращения этого. В некоторых случаях он может - для базовых атак. Но если кто-то попадает в вашу среду, очень важно идентифицировать его, понимать, что происходит, сдерживать это, ограничивать ущерб., сможете восстанавливать и восстанавливать и, надеюсь, вернуться к нормальной работе ".

Эксперты по реагированию на инциденты давно рекомендуют настольные упражнения - также известные как имитация кибератак, - чтобы каждый в организации понимал свои роли и обязанности во время инцидента, когда бы он ни случился.

«Имея правильные системы для быстрого обнаружения, вы должны иметь возможность уверенно реагировать», - говорит Акерман из Kroll. «Были ситуации, когда инциденты обнаруживаются, меры по сдерживанию запускаются, но сейчас 2 часа ночи в субботу, и некому полностью выполнить и оценить воздействие. Крайне важно иметь в наличии соответствующий персонал или подходящих поставщиков, уполномоченных принимать меры. необходимые действия от вашего имени ".

Оттачивание планов реагирования на инциденты

Другими словами, планировщикам необходимо учитывать множество факторов, включая склонность злоумышленников к нанесению ударов в нерабочее время.

«В хорошо разработанных планах реагирования на инциденты предусмотрены непредвиденные обстоятельства для инцидентов, происходящих в нерабочее время или когда ключевые участники находятся в отпуске», - говорит Акерман. «Эти сценарии лучше всего разрабатывать во время настольных упражнений, а затем задокументировать в плане. Да, организации должны иметь возможность реагировать в Черную пятницу, канун Рождества или когда их руководитель ИТ-

отдела находится в отпуске, а план реагирования на инциденты должен подробно описывать, как. "

Список шагов, которые необходимо предпринять организациям, чтобы занять хорошую оборонительную позицию, «не сложен - это просто вещи, которые вы должны делать», - говорит Карри из Cybereason. «Это не просто: «Развернуть элементы управления». Существуют элементы управления, которые могут помочь, и наличие стратегии обнаружения... важно... но это также подготовка бизнеса и резервирование в ИТ. Как долго вы храните резервные копии? Кому вы собираетесь позвонить в экстренной ситуации?»

Ответить на такие вопросы после нападения без хорошо отрепетированного плана может быть сложно.

«Есть компании, которые знают об этом» и также «что-то с этим делают», - говорит Грилло из Alvarez & Marsal. «Или они выясняют свой собственный путь». ***(Mathew J. Schwartz. US Cybersecurity Alert: Hackers Won't Respect Thanksgiving // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-cybersecurity-alert-hackers-wont-respect-thanksgiving-a-17976). 23.11.2021).***

***

«Французская фирма Bureau Veritas, которая специализируется на лабораторных испытаниях, инспекциях и услугах по сертификации, сообщила о кибератаке, которая затронула ее систему кибербезопасности.

Нарушение безопасности было обнаружено 20 ноября.

В качестве превентивной меры компания временно отключила все свои серверы и данные.

В настоящее время проводятся дополнительные расследования и корректирующие процедуры.

В заявлении компании говорится: «Было принято превентивное решение о временном отключении наших серверов и данных для защиты наших клиентов и компании, пока продолжаются дальнейшие расследования и корректирующие меры. Это решение приводит к частичной недоступности или замедлению работы наших сервисов и клиентских интерфейсов».

После кибератаки команды Bureau Veritas при поддержке сторонних ИТ-специалистов в настоящее время сосредоточивают свои усилия на обеспечении непрерывности бизнеса, инициировав процедуру реагирования на инциденты.

Они также прилагают усилия, чтобы уменьшить неудобства для клиентов, сотрудников и партнеров.

Бюро Веритас добавило: «Бюро Веритас также приняло меры к соответствующим органам, которые предоставят нам дополнительную поддержку для возобновления нормальной работы в краткосрочной перспективе. Мы благодарим наших клиентов за понимание и доверие»…» ***(Bureau Veritas hit by cyberattack on cybersecurity system // Verdict Media Limited (https://www.ship-technology.com/news/bureau-veritas-hit-cyberattack/). 23.11.2021).***

***

«Сегодня в мире существует два типа бизнеса. Те, которые подверглись нападению со стороны киберпреступников, и те, которые нет.

Что становится все более очевидным, большинство этих предприятий в настоящее время находятся в уязвимом положении на грани исторического кризиса.

Только в этом месяце, по данным Bleeping Computer, гигант розничной торговли электроникой MediaMarkt пострадал от атаки вымогателя с первоначальным требованием выкупа в размере 240 миллионов долларов. В результате удара были остановлены ИТ-системы и нарушена работа магазинов в Нидерландах и Германии.

Что еще хуже, Hive, группа, стоящая за атакой, угрожает украсть конфиденциальный контент и опубликовать его на своем сайте утечки данных, если выкуп не будет уплачен.

Важно отметить, что этот тип атак - это не просто проблема, угрожающая крупным европейским корпорациям. Во всем мире предприятия любого размера сталкиваются с невиданным ранее уровнем кибератак.

Чтобы узнать больше о проблеме и о том, что можно сделать, мы поручили Coleman Parkes Research провести независимое исследование.

Крупные предприятия, такие как MediaMarkt, обычно имеют бюджет, персонал и другие ресурсы для борьбы с киберпреступностью. Обычно они могут позаботиться о себе сами. Несмотря на то, что этот опыт может быть очень «болезненным» для их репутации и непрерывности бизнеса, у большинства крупных компаний есть средства пережить кибератаки.

Но как насчет кибератак среднего и малого бизнеса? Они так же зависят от вычислительных ресурсов и онлайн-общения, как и любая крупная корпорация. Если подвергнуться кибератаке, это может серьезно повлиять на работу.

В целом, есть ли у малых и средних предприятий технологии и обученный персонал для адекватной защиты от постоянно развивающихся киберугроз? Есть ли у них планы на случай непредвиденных обстоятельств для уменьшения ущерба в случае нападения? Есть ли у них страховые полисы, покрывающие ущерб и расходы на восстановление? Ответы на эти вопросы могут помочь найти подходящие и эффективные средства правовой защиты в текущей ситуации.

Итак, в своем исследовании Коулман Паркс сосредоточился на малых и средних предприятиях. Четыреста руководителей малого и среднего бизнеса в Северной Америке и Европе были опрошены на предмет их текущего состояния готовности к кибербезопасности. Результаты опроса подтвердили, что малые и средние предприятия подвергаются кибератакам, практически не имея практических возможностей защитить себя.

Кроме того, в ходе опроса была обнаружена новая информация об этой развивающейся ситуации и множество полезных статистических данных о кибератаках среднего и малого бизнеса:

24% малых и средних предприятий стали жертвами кибератак за последние 12 месяцев.

Средняя стоимость инцидента кибербезопасности для малого и среднего бизнеса составила около 200 тысяч долларов.

Малые и средние предприятия готовы платить в среднем 6,45 долл. США / 6,40 евро каждый месяц за защиту кибербезопасности». ***(Barry Spielman. Examples of Large & Small Business Cyber Attacks: Fighting for Survival Against a New Wave of Cyber Criminals // Techstrong Group Inc. (https://securityboulevard.com/2021/11/examples-of-large-small-business-cyber-attacks-fighting-for-survival-against-a-new-wave-of-cyber-criminals/). 16.11.2021).***

***

«В прошлом году 86% предприятий подверглись DDoS-атаке (годовой отчет Radware по безопасности). Это означает, что 86% предприятий пострадали от сбоев, которые как минимум повлияли на их сотрудников и, в худшем случае, повлияли на качество обслуживания клиентов и доходы. При выборе технологии безопасности и подхода к ней нельзя допускать ошибок. Предприятиям необходимо убедиться, что выбранный поставщик способен защитить свою сеть и приложения от новейших DDoS-атак и многовекторных атак.

Что происходит с бизнесом без надлежащей защиты?

Вот пример. Банк APAC стал последней целью кампании DDoS-атак, начавшейся в начале сентября. Первоначально атаки затронули основного поставщика услуг банка. Хотя банк развернул облачную службу защиты от DDoS-атак Akamai за несколько дней до атаки, эта служба не смогла выявить и смягчить весь плохой трафик. Плохой трафик «просачивался» из решения Akamai, влияя на межсетевые экраны контрольных точек банка, вызывая дополнительные сбои в обслуживании. К сожалению для банка, эти отключения привлекли внимание общественности.

ИТ-команда банка изначально думала, что сможет справиться с DDoS-атаками с помощью существующих решений. Однако после нескольких безуспешных попыток смягчения последствий, включая разрушительные новости, руководство банка созвало встречу между своей ИТ-командой, Cisco и Radware для разработки решения.

РЕШЕНИЕ

Команда рекомендовала локальное DDoS- устройство Radware для обеспечения улучшенной защиты от новейших векторов атак, с которыми служба Akamai не могла справиться.

В середине сентября первое устройство было развернуто в оперативном режиме, первоначально в режиме отчета. Десять дней спустя ИТ-отделу банка потребовалась помощь в проведении крупномасштабной атаки массового UDP / TCP-флуда с пакетными характеристиками на его VPN. Решение Akamai Cloud DDoS обработало до 100 Гбит / с атаки, но «утекло» еще 2–2,5 Гбит / с плохого трафика, что привело к проблемам с удаленным подключением и нарушению их банковских операций. Утечки трафика продолжались до тех пор, пока Akamai не создал черные списки для плохого трафика.

Устройство защиты от DDoS-атак в режиме отчета немедленно определило векторы атак, которые служба Akamai не смогла идентифицировать и смягчить, включая атаки UDP FRAG и ICMP / UDP / DNS Reflection. Решение Radware DDoS предлагает защиту от продвинутых DDoS-атак, включая Burst-атаки, низкие и

медленные атаки, UDP-фрагментацию и SYN-Flood, которые сервисы облачной очистки не могут обеспечить. Облачные сервисы по определению рассматривают только входящий (входящий) трафик; они не могут защитить от векторов атак, требующих двусторонней видимости трафика.

После того как команда Radware провела тщательный анализ трафика, чтобы убедиться в отсутствии ложных срабатываний, и переместила политики из режима отчета в режим блокировки, банк был полностью защищен. Банк высоко оценил технологию Radware для выявления атак и защиты от них. После инцидента устройство защиты от DDoS-атак Radware было установлено во всех дата-центрах банка. У банка не было дополнительных сбоев, и теперь он пользуется преимуществами защиты от DDoS-атак Radware...

Вопросы, которые следует задать для оценки возможностей поставщика средств защиты

При оценке решений безопасности не забудьте задать поставщику, продукты которого вы оцениваете, следующие вопросы:

Сможете ли вы обеспечить непрерывность бизнеса при атаке?

От каких атак защищает ваше решение?

Используете ли вы алгоритмы поведенческого обучения, чтобы установить «законные» шаблоны трафика?

Как отличить хороший трафик от плохого?» ***(Debra Price. Does Your DDoS Protection Solution Defend Against the Latest Attacks? // Techstrong Group Inc. (https://securityboulevard.com/2021/11/does-your-ddos-protection-solution-defend-against-the-latest-attacks/). 16.11.2021).***

***

«С развитием технологий количество взломов значительно увеличилось. В свете того, что хакеры были такими хитрыми и знали, где и когда атаковать, самой большой целью в прошлом году были компании среднего размера.

Компании среднего размера — это не транснациональные хорошо оснащенные предприятия, но они тоже не очень маленькие. Это бизнес, который сумел зарекомендовать себя в своей сфере деятельности и неплохо зарабатывает.

Coro провела перекрестное исследование безопасности среднего бизнеса, в ходе которого было оценено, что «вероятность того, что компании среднего размера столкнутся с нарушением кибербезопасности к концу этого года, на 490 процентов выше, чем в 2019 году». Отчет включал около 4000 компаний среднего размера, в которых работает от 1000 до 1500 сотрудников из различных сфер бизнеса. Причина, по которой рынок среднего размера является основным объектом атак, заключается в том, что, хотя они хорошо зарабатывают, у них недостаточно финансов или более сильных связей, чтобы защитить себя, как это делают более крупные транснациональные компании. Помимо этого, отрасли защиты кибербезопасности с точки зрения защиты более крупных транснациональных компаний, чем средний бизнес.

Опрос показал, что в период с 2020 по 2021 год во всех секторах средней промышленности наблюдался рост кибератак на 50 процентов, при этом резко возросли масштабы здравоохранения и транспорта. Кроме того, выяснилось, что

кибератаки с большей вероятностью будут расти с наступлением праздничного сезона. Статистические данные за прошлый год показали больший рост случаев атак к концу года по сравнению с первыми кварталами, в то время как в отчете за 2021 год анализируется то же самое.

В отчете также говорится, что из-за пандемии изменились и методы атак. Перед пандемией чаще встречались фишинговые и вредоносные атаки. Однако отрасли, которые становятся все более цифровыми из-за пандемии, во многом меняют образ жизни. Компании среднего размера столкнулись со взломом и атаками в виде бот-атак, Wi-Fi, вредоносных программ в электронных письмах, вредоносных программ в приложениях и т.д.

Большинство компаний среднего размера не инвестируют достаточно средств, чтобы защитить себя, за исключением основных мелких взломов, и, учитывая, что к более серьезным кибератакам они столкнутся, они не готовы. Кроме того, те компании, которые инвестируют средства в защиту, сталкиваются с компромиссом в параметрах защиты.

Компаниям следует широко инвестировать в свою защиту, потому что, только если они защитят себя, они смогут двигаться вперед и прожить более успешные годы в бизнесе». ***(Arooj Ahmed. Mid-Size Businesses more prone to cyberattacks, reveals a new study // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/mid-size-businesses-more-prone-to.html). 23.11.2021).***

***

«Исследование показывает, что 47% онлайн-игроков подверглись атакам кибербезопасности, которые привели к огромным финансовым потерям или другим личным потерям.

Гейминг превратился в огромную индустрию, в которой тысячи людей по всему миру в настоящее время зарабатывают на жизнь, транслируя себя, играя в видеоигры. То, что раньше считалось хобби, но которое не одобряли, теперь стало невероятно прибыльным делом, которое позволяет людям по-настоящему жить своей жизнью. Конечно, не все зарабатывают миллион долларов на этом джазе, но уже давно позади те времена, когда потоковый контент считался бесполезным и несерьезным. Ну, по крайней мере, в нынешнем поколении. Старшие поколения по-прежнему склонны инфантилизировать и покровительствовать таким способам зарабатывания денег, даже когда они отмечают, что 50-летние комментаторы делают то же самое со спортом. С другой стороны, понятие иронии часто упускается из виду. Дело в том, что игры и прямые трансляции - такой же вариант работы, как искусство или наука.

Конечно, онлайн-игры привлекают внимание не тех людей. Интернет-аудитория означает, что вас знает гораздо больше людей, чем средний наемный работник, и такой пьедестал может оказаться разрушительным. Особая форма негативного внимания, о которой я говорю в этой статье, - это то, что предлагают киберпреступники. Конечно, когда я говорю «предложение», я должен также пояснить, что такие захудалые люди не собираются возвращать указанное

индивидуальное внимание. У них есть цель, и теперь они будут целиться в яремную вену.

Исследование, проведенное NortonLifeLock, показывает, что почти половина всех онлайн-игроков пострадали от той или иной угрозы кибербезопасности. В основном такие атаки проводятся в погоне за деньгами. Исследование показывает, что 3 из каждых 4 затронутых стримеров потеряли деньги в процессе проводимой атаки, при этом стримеры в среднем теряют около 744 долларов США на человека. Это уже ужасно, но многие такие киберпреступники ищут и другие, более компрометирующие предметы. Женщины-стримеры часто страдают от людей, которые получают доступ к личным фотографиям и сообщениям с намерением шантажа, личного вуайеризма и просто отвратительной мерзостью в целом. Ой. Пятая часть всей выборки, участвовавшей в исследовании, также показала, что 21% из них в какой-то момент также подверглись доксированию, что является ужасным испытанием…» ***(Arooj Ahmed. A Survey Reveals That Around Half Of All Online Gamers Have Suffered From Cybersecurity Threats And Attacks // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/a-survey-reveals-that-around-half-of.html). 24.11.2021).***

***

«…Proofpoint, компания, занимающаяся цифровой безопасностью предприятий, сообщила во вторник, что ее исследователи наблюдают массовый рост числа мобильных фишинговых атак на тему праздников, также известных как smishing.

Он отметил, что объем мобильных фишинговых сообщений почти удвоился по сравнению с этим периодом прошлого года.

Эти сообщения обещают все, от доставки посылок и подарков до специальных розничных предложений и особых исключений для доставки.

«В последние несколько лет наблюдалась тенденция мошенничества и мошенничества, связанного с праздниками и праздничными темами в четвертом квартале года», - отметила Хасинта Тобин, глобальный вице-президент Proofpoint по операциям Cloudmark.

«Мы наблюдаем стабильный рост наших отчетов о мошенничестве и мошенничестве в США и во всем мире, начиная с октября и заканчивая декабрем», - сказала она TechNewsWorld.

Сезон восприимчивости

Бен Бригитта, директор по операциям SOC на Выгнать, в SOC-как-сервис - провайдере inHerndon, Va. Разъяснено, что фишинговые атаки увеличиваются во время праздников, потому что люди более восприимчивы к социальной инженерии, ориентации их желанию показать свои близкие, они заботятся.

«Это не редкость, когда в это время появляются рекламные объявления, обещающие выгодные предложения, или когда кто-то спрашивает, не хотите ли вы скинуться на крупный подарок», - сказал он TechNewsWorld.

«Злоумышленники могут отправить электронное письмо о сделке, которая слишком хороша, чтобы быть правдой для горячей новой игрушки, и люди на нее повадятся», - сказал он.

«Они могут выдать себя за менеджера, - продолжил он, - и попросить кого-нибудь «забрать подарочные карты для всех в офисе», и это действительно имеет смысл, поэтому люди делают это».

Магни Р. Сигурдссон, старший менеджер по технологиям обнаружения в Cyren, компании по кибербезопасности в Маклине, штат Вирджиния, которая специализируется на защите бизнеса от фишинговых атак и потери данных, отметила, что количество фишинговых SMS-кампаний увеличилось, потому что мобильных пользователей и устройств больше, чем там. были год назад.

«Фишинг - это коммерческое предприятие, поэтому киберпреступники приспосабливаются к изменениям в поведении потребителей так же, как и законные компании», - сказал он TechNewsWorld.

Успех с высоким рейтингом кликов

«Поскольку потребители все больше полагаются на мобильные устройства, вполне естественно, что злоумышленники сосредоточатся на этих платформах», - заметил Джон Бамбенек, главный специалист по поиску угроз в Netenrich, компании, работающей в сфере ИТ и цифровой безопасности в Сан-Хосе, Калифорния.

«Это особенно верно, учитывая, что количество кликов по SMS-атакам намного выше, чем по электронной почте, и тот факт, что на мобильных устройствах гораздо меньше безопасности», - сказал он TechNewsWorld.

«Таким образом, количество нападений абсолютно увеличилось, и они будут продолжать расти», - сказал он.

Хэнк Шлесс, старший менеджер по решениям безопасности Lookout, поставщика мобильных фишинговых решений из Сан-Франциско, отметил значительный рост корпоративного мобильного фишинга в конце 2019 и 2020 годов. С четвертого квартала 2019 года по первый квартал 2020 года объем увеличился 87 процентов, а с четвертого квартала 2020 года по первый квартал 2021 года они подскочили на 127 процентов.

«Интересно то, что с этого момента в 2021 году субъекты угроз не сдавались, и количество столкновений продолжало расти в течение первых трех кварталов 2021 года, показывая, что это серьезная проблема, которая не исчезнет», - сказал он TechNewsWorld..

Служба поддержки поддельных клиентов

В блоге Proofpoint Тобин написал, что киберпреступники охотятся на мобильных пользователей с помощью smishing-атак, которые якобы исходят от уважаемых компаний, включая известных розничных продавцов, бренды электронной коммерции и компании по доставке посылок.

Эти приманки пытаются украсть личную информацию у ничего не подозревающих целей, добавила она.

Многие из этих приманок запрашивают информацию о кредитной карте, чтобы решить проблему, предположительно связанную с покупкой или доставкой несуществующего товара, отметила она.

В других случаях, пишет она, злоумышленники пытаются украсть личную информацию через привлекательный URL-адрес или целевую страницу.

Expel видел аналогичную активность в Интернете. В блоге, опубликованном в понедельник, говорится о мошенничестве с доставкой, когда цель уведомляется о покупке дорогостоящего предмета, который они не купили.

В письме нет интерактивных ссылок - просто номер телефона «службы поддержки», напечатанный ярко-красным шрифтом в нижней части уведомления о покупке.

Когда получатель уведомления звонит по номеру телефона, «представитель службы поддержки клиентов» предлагает решить проблему после сбора необходимой информации об учетной записи для решения проблемы.

В случае успеха этот тип мошенничества приведет к тому, что злоумышленник получит учетные данные учетной записи, номера кредитных карт или другую конфиденциальную личную информацию от соответствующего получателя, пояснил Expel.

«Рост потребительских покупок в период праздников предоставляет злоумышленникам множество возможностей заставить людей раскрыть конфиденциальную информацию», - заметил Рэй Пью, менеджер по операциям с безопасностью Expel.

«Поддельные квитанции о покупках, счета-фактуры и уведомления о доставке особенно часто побуждают получателей нажимать ссылки или звонить по номерам телефонов, указанным в фишинговом письме, поскольку получатели ожидают таких писем в это время года, поэтому призыв к действию является сильным. и шансы злоумышленников на успех особенно высоки во время праздников», - сказал он TechNewsWorld.

Меры предосторожности

В своем блоге Тобин дала несколько советов по безопасности мобильных устройств во время праздников.

Обращайте внимание на подозрительные текстовые сообщения. Преступники все чаще используют мобильные сообщения и SMS-фишинг в качестве вектора атаки.

Будьте осторожны, сообщая свой номер мобильного телефона предприятиям или другим коммерческим организациям.

Каждый раз, когда вы получаете сообщение, в том числе какое-либо предупреждение или уведомление о доставке пакета, содержащее веб-ссылку, не используйте веб-ссылку, указанную в текстовом сообщении. Вместо этого используйте браузер вашего устройства для прямого доступа к веб-сайту отправителя или используйте приложение бренда, если оно у вас уже установлено на вашем устройстве. Сделайте это также для любых кодов предложений, которые вы получаете, вводя их прямо на веб-сайте отправителя из вашего браузера.

Сообщайте о SMS-фишинге и спаме в Службу сообщений о спаме. Используйте функцию отправки сообщений о спаме в своем клиенте обмена сообщениями, если он есть, или пересылайте текстовые сообщения о спаме на номер 7726, что означает «СПАМ» на клавиатуре телефона.

Будьте осторожны при загрузке и установке нового программного обеспечения на свое мобильное устройство. Внимательно прочитайте приглашения на установку, особенно для получения информации о правах и привилегиях, которые может запрашивать приложение.

Не отвечайте на нежелательные корпоративные или коммерческие сообщения от поставщиков или предприятий, которых вы не знаете. Это часто подтверждает, что вы «настоящий человек».

Не устанавливайте программное обеспечение на свое мобильное устройство из любого источника, кроме сертифицированного магазина приложений от поставщика или оператора мобильной сети.

«Потребители должны понимать, что SMS-сообщения более небезопасны, чем электронная почта, и что каждое полученное ими сообщение является подозрительным», - сказал Бамбенек.

«Им следует предпочесть обмен сообщениями на основе приложений, а не текст, - добавил он, - и понять, что если что-то слишком хорошо, чтобы быть правдой, то, вероятно, так оно и есть». ***(John P. Mello Jr. Holidays Fuel Surge of Mobile, Online Phishing Scams // ECT News Network, Inc. (https://www.technewsworld.com/story/holidays-fuel-surge-of-mobile-online-phishing-scams-87348.html). 24.11.2021).***

***

«…В период с 2019 по 2020 год киберпреступность выросла на 158% в национальном масштабе и на 62% во всем мире. Cybersecurity Ventures прогнозирует, что глобальные затраты на программы-вымогатели достигнут 20 миллиардов долларов в 2021 году. От печально известного нарушения колониального трубопровода в мае, которое перекрыло доступ к топливу и нанесло ущерб миллионам американцев восточного побережья, до почти 50 миллионов номеров социального страхования, раскрытых после 21 года. -старому удалось взломать T-Mobile, киберпреступность становится горячей темой. К сожалению, защита от киберугроз остается непонятной, сложной и недоступной для большинства.

Если программы-вымогатели так популярны, почему кибербезопасность не меняется быстрее?

Кибербезопасность нужна всем секторам, и она не может сравниться по популярности с программами-вымогателями, потому что отрасль использует те же методы, инструменты и мыслительные процессы, что и более 20 лет назад. Услуги кибербезопасности предназначены для крупных государственных организаций и крупных корпораций, поэтому продукты, стратегии, роли и услуги были созданы для более крупных предприятий с лучшими ресурсами.

С начала пандемии 94% компаний частично перешли на облачные технологии, и практически все в мгновение ока внедрили приложения SaaS, чтобы модернизировать и повысить эффективность, открыв новые направления атак для киберпреступников. Тем не менее, поставщики, консультативные органы и лидеры мнений мало что сделали для обслуживания средней компании. Они продолжают сосредотачиваться на корпоративном образе мышления снизу вверх, вместо того,

чтобы давать компаниям возможность быстро принимать решения, потому что это то, что они знают, а для многих именно это и есть деньги.

Соблюдение требований не означает безопасность.

Когда дело доходит до безопасности, большинство организаций ориентируются на соответствие требованиям. Они отмечают несколько флажков, чтобы получить необходимые сертификаты, которые соответствуют минимальному уровню, позволяющему продолжать бизнес. Такая практика «галочки» является нормой, потому что, по нашим оценкам, для более чем 80% предприятий это все, что они могут себе позволить. Между тем, 43% всех жертв программ-вымогателей составляют предприятия малого и среднего бизнеса. Эти малые и средние предприятия склонны полагать, что их не заметят, хотя на самом деле они малоизвестны, потому что редко имеют надлежащие системы безопасности.

Кибербезопасность излишне сложна. В результате отрасль сталкивается с явной нехваткой кадров. Эти условия в сочетании с тревожным стоицизмом индустрии кибербезопасности создают идеальный шторм для увеличения числа программ-вымогателей.

Дело не в том, что то, что находится на месте, неправильно. Многие из них хорошо сделаны, хорошо изучены и хорошо выполнены. Просто армия из одного человека не может внедрить системы, которые созданы для команды из 100 человек.

Как выглядит идеальный кибербезопасный мир?

Всем нужен эквивалент iTunes для ИТ и безопасности. iTunes сделал доступ к цифровой музыке возможным одним нажатием кнопки по низкой цене. Нам нужна простая, доступная и быстрая безопасность. Начнем с того, что базовая гигиена безопасности должна быть бесплатной, а не стоить десятки тысяч долларов.

Фирмы должны сделать все аспекты своей безопасности и процессов измеримыми. Использование приложений, обеспечивающих измеримость, должно быть быстрым и простым. Вместо того, чтобы спрашивать и ждать в течение недели, пока они не узнают, уязвимы ли их активы или скомпрометированы киберугрозой, лидеры должны иметь полную видимость, быстро предоставляя контекст вокруг событий в их среде в терминах, которые они могут понять.

Вместо того, чтобы реактивно тратить дни на исправление оконечных устройств постфактум, руководители должны иметь мгновенные ответы на насущные вопросы, например: «Влияет ли угроза на мои ресурсы?»

Руководители должны быть уверены в том, что в случае постоянных кибератак, о которых сообщается в новостях, они проявляют максимальную активность. Когда гигиена на должном уровне, шансы на образование корневого канала низки.

Кто несет ответственность за внесение изменений?

Мы находимся на переломном этапе развития рынка. Отрасль должна отказаться от старых моделей. Все, от поставщиков кибербезопасности и средств массовой информации до правительства и опытных специалистов по безопасности, должны изменить свое мышление.

Поставщики должны предлагать решения, которые будут полезны без чрезвычайно технически подкованной армии. Как отрасль, мы должны объединиться и взяться за достижение ощутимой кибергигиены для предприятий любого размера.

Журналисты и правительство могут посоветовать, как оставаться в безопасности, сотрудничая с экспертами, которые видят необходимость изменений, описывая передовой опыт, который не обязательно должен быть крупным предприятием для внедрения, и рекомендовать инновационные технологии, которые подходят для всех бюджетов, а не только сенсация новостей, выпуск политики и вложение денег в проблему.

Практикам нужно думать иначе, особенно в небольших компаниях. В настоящее время они реагируют на угрозы, а не проактивны; они сосредоточены на восходящих подходах, которые привлекли внимание лучших специалистов в области передачи данных. Им нужно начать думать о реальной безопасности, а не о соблюдении установленных правил.

Эксперты знают, что то, как они применяли кибербезопасность, сегодня не сработает для большинства компаний. Они знают, что это неустойчивая модель. Эксперты должны говорить громче, чтобы помогать будущим поколениям и влиять на поставщиков, чтобы они внесли изменения в их бизнес-модели.

Руководители бизнеса должны знать, чтобы не опережать угрозы; Ключевым моментом является выяснение того, как лучше всего автоматизировать получение информации о вашей компании, связанной с нарушениями, происходящими в мире. Инструменты, которые достигают этого и помогают измерять и укреплять индивидуальную ответственность за безопасность, будут способствовать изменениям, которые можно масштабировать с помощью компании любого размера.

Кибербезопасность отчаянно нуждается в преобразовании, и как отрасль мы сможем сделать это, только если объединимся». ***(Grant Wernick. Cyberattacks Are Sensationalized Daily Without Solutions, And Businesses Continue To Take The Hit // Forbes (https://www.forbes.com/sites/forbestechcouncil/2021/11/24/cyberattacks-are-sensationalized-daily-without-solutions-and-businesses-continue-to-take-the-hit/?sh=57c0c2d77646). 24.11.2021).***

***

«Предприятия по производству биотехнологий в США активно становятся мишенью неизвестной хакерской группы, использующей новый штамм вредоносного ПО.

В новом сообщении об угрозах Центр обмена и анализа биоэкономической информации (BIO-ISAC) сообщил, что первая атака, которая предположительно была запущена с использованием этого нового вредоносного ПО, получившего название «Tardigrade», произошла весной этого года. В то время Tardigrade использовался в кибератаке на крупный завод по производству биопродуктов, хотя второй объект был поражен тем же вредоносным ПО только в прошлом месяце.

Согласно BIO-ISAC, как предприятиям по производству биопродуктов, так и их партнерам «рекомендуется предполагать, что они являются целями», и им следует предпринять необходимые шаги для пересмотра своих позиций в области безопасности и реагирования.

Как сообщили по SiliconANGLE, медленно передвигающийся в основном используются для шпионажа, хотя вредоносные программы также вызывают другие проблемы, о системах заражает в том числе отключения сети.

В отдельном докладе, Wired отметил, что эти недавние нападения могут быть связаны с Covid-19 исследований, как пандемия показала, насколько важно Biomanufacturing исследования при разработке вакцин и других лекарственных средств.

Происхождение кода, используемого в Tardigrade, также вызывает споры, поскольку BIO-ISAC считает, что вредоносная программа основана на Smoke Loader, хотя исследователи безопасности, которые говорили с Bleeping Computer, утверждают, что это форма HTTP-маяка Cobalt Strike, а не полностью новый штамм вредоносного ПО.

Благодаря передовым характеристикам Tardigrade, вредоносное ПО могло быть разработано группой передового обнаружения угроз или даже государственной разведывательной службой.

Независимо от своего происхождения, Tardigrade довольно опасен, и мы, вероятно, узнаем больше об этом новом вредоносном ПО, поскольку исследователи безопасности и даже правительственные агентства углубятся в его код, пытаясь обнаружить его истинное происхождение». ***(Anthony Spadafora. Hackers target biomanufacturing facilities using the Tardigrade malware // Future US, Inc. (https://www.techradar.com/news/hackers-target-biomanufacturing-facilities-using-the-tardigrade-malware). 25.11.2021).***

***

«Анализ спам-сообщений показал, что большинство фишинговых атак, нацеленных на интернет-покупателей, происходит из США (44%) в преддверии праздников.

Цифра основана на анализе данных глобальной телеметрии спама, собранных Bitdefender в период с 1 по 11 ноября 2021 года в преддверии приближающегося сезона праздничных покупок.

Исследование показывает, что, хотя фишеры используют широкую сеть, их внимание сосредоточено на покупателях из США, которые стали наиболее привлекательной целью для злоумышленников, получая наибольшую долю спам-писем, составляющую 44% от всего мирового объема спама.

За США следуют Великобритания (8%), Австралия (6%), Южная Африка (5%), Ирландия (4%), Германия (4%), Швеция (3%), Дания (2%), Франция). (2%), Румыния (1%) и Италия (1%).

«Всего за две недели до самого крупного торгового дня в году нет недостатка в фальшивых предложениях и рекламных акциях, на которые могут влюбиться увлеченные покупатели. Ни один камень не остался незамеченным, от предметов интерьера и розничной торговли до технологий и билетов на самолет», - отметил Bitdefender.

Готовьтесь к большему

Bitdefender утверждает, что его результаты согласуются с недавним опросом, который поставил США на первое место по количеству людей, которые планируют делать покупки в Черную пятницу в этом году.

Неудивительно, что подавляющее большинство спам-сообщений, проанализированных Bitdefender, было написано на английском языке.

Согласно их анализу спама, вознаграждения покупателей и подарочные карты или призы, связанные с фальшивыми опросами и розыгрышами, являются одними из наиболее часто используемых уловок для соблазнения получателей. Кроме того, с ослаблением ограничений на поездки Bitdefender ожидает, что мошенники увеличат использование туристических предложений, чтобы обмануть ничего не подозревающих планировщиков поездок.

«Исследователи спама Bitdefender ожидают, что в ближайшие недели будет больше спамерских кампаний, с пиками в Черную пятницу, Киберпонедельник и зимние праздничные покупки. Мошенники часто используют эти события для распространения фишинговых писем и массовой доставки вредоносного ПО целям», - предупреждает Bitdefender». ***(Mayank Sharma. Most phishing scams targeting online shoppers originate in the US // Future US, Inc. (https://www.techradar.com/news/most-phishing-scams-targeting-online-shoppers-originate-in-the-us). 24.11.2021).***

***

«Arkose Labs опубликовала новые данные о последних тенденциях мошенничества, выявив рост угроз во время праздников, рост числа атак ботов и возобновление атак на туристические компании. По мере того как покупатели заполняют свои онлайн-тележки, атаки по захвату аккаунтов (ATO) и мошенничество с подарочными картами остаются постоянными.

В отчете представлены шесть основных тенденций борьбы с мошенничеством за последние 3 месяца и представлены данные, подчеркивающие, что ни один цифровой бизнес не застрахован от атак. Финансовые отрасли подверглись атакам на 32 процента больше, чем в первой половине 2021 года.

В третьем квартале количество атак на розничную торговлю и туристические компании увеличилось на 63%, а в играх наблюдался поток фальшивых новых учетных записей, созданных в мошеннических целях. В медиа- и потоковых компаниях 60% злонамеренных действий нацелены на вход в систему, и 20% этих атак исходят от ферм, занимающихся мошенничеством людей.

На технологические платформы приходится 91% всех атак, совершаемых ботами. В целом количество атак увеличивается во всех отраслях, и они становятся все более изощренными.

«По мере приближения к 2022 году частота и серьезность мошенничества продолжает угрожать любой организации, ведущей бизнес в Интернете», - сказала директор по маркетингу Arkose Labs Ванита Пандей. «Основываясь на данных, полученных от сети Arkose Labs Network, мы прогнозируем 60-процентное увеличение атак в наступающем сезоне праздничных покупок 2021 года. Ни один цифровой бизнес не застрахован от этой угрозы».

Угрозы нарастают во время праздников

Сезон отпусков - это еще и сезон киберпреступлений. Атаки неуклонно росли в течение 2020 года, становились все более частыми, начинались в более широком масштабе и начинались с большей изощренностью. Цифровым компаниям необходимо понимать, как работают мошенники, и защищать те части своего бизнеса, которые уязвимы для атак.

Предполагается, что во время сезона праздничных покупок 2021 года, который сейчас начнется, будет совершаться восемь миллионов атак ежедневно. Пока мошеннические атаки выгодны для злоумышленников, компании должны проявлять бдительность в своей защите.

Индустрия туризма снова под прицелом. Мир снова путешествует, а это означает, что на туристических сайтах появляется больше онлайн-бронирований. В туристическом секторе объем цифрового трафика увеличился на 40%, что создает прекрасную возможность для атак, который со 2-го по 3-й квартал 2021 года увеличился на 80%.

Особенно сильно пострадал цифровой трафик на туристические сайты США: 66% посещений в Интернете были отмечены как мошенничество или атаки ботов.

Азия является лидером по атакам на планете. Азия вернулась в число основных инициаторов мошеннических атак, при этом на долю Китая приходится почти половина всех атак в третьем квартале. Для сравнения, на США, находящиеся на втором месте, пришлось 19,4 процента атак.

В центре внимания боты. Несмотря на рост числа попыток мошенничества со стороны людей, согласно прогнозам, машинные атаки будут устойчивыми и, возможно, возрастут в период праздников. На ботов сейчас приходится 88% атак.

В 2020 году с октября по декабрь произошло более 2 миллионов бот-атак. В этом году это число, вероятно, будет еще выше, поэтому для предприятий еще более важно усилить контроль за трафиком, предназначенным для нанесения вреда.

У мошенничества новое лицо. Цифровые компании испытывают массовый рост поддельных новых учетных записей. В прошлом квартале было обнаружено 560 миллионов злонамеренных попыток регистрации потоков, что в четыре раза больше, чем на начало года. Эти фальшивые учетные записи открывают двери для последующего мошенничества, которое напрямую влияет на чистую прибыль компаний электронной коммерции.

Внедрение учетных данных продолжает преследовать онлайн-бизнес. По мере того, как все больше клиентов открывают цифровые учетные записи, вскоре последуют попытки захвата учетных записей, подпитываемые масштабным заполнением учетных данных. За последний год было закрыто 3 миллиарда атак по подбору учетных данных, что почти удвоилось за последние 12 месяцев…». ***(As digital shopping surges, researchers predict 8 million daily attacks // Help Net Security (https://www.helpnetsecurity.com/2021/11/22/threats-during-holidays/). 22.11.2021).***

***

«Распределенные атаки типа «отказ в обслуживании» (DDoS) становятся все более изощренными, масштабными и экономически мотивированными. Даже по прошествии 25 лет они по-прежнему представляют собой огромную угрозу безопасности для любого бизнеса. Во многом это связано с тем, что DDoS-атаки относительно просты и дешевы в запуске. Показательный пример: злоумышленники запустили самую крупную DDoS-атаку за всю историю в сентябре 2021 года, продемонстрировав сохраняющуюся жизнеспособность DDoS-атак для недобросовестных сторон, которым есть что от них выиграть.

DDoS-атаки находятся в авангарде войны с цифровым бизнесом, и ни одна компания или отрасль не защищены. DDoS-атаки направлены на перегрузку (или исчерпание) цифровых ресурсов бизнеса и предотвращение их нормальной работы. В худшем случае массовый приток трафика приведет к сбою веб-серверов. DDoS-атаки также могут быть дымовой завесой для утечки данных, пытаясь привлечь внимание ИТ-специалистов к DDoS-атакам, а не к утечке данных. DDoS-атаки с выкупом, когда злоумышленники требуют оплаты за предотвращение или прекращение DDoS-атак, также растут.

Итак, как можно смягчить DDoS-атаки? Их ключ - блокировать как можно больше плохого трафика, сохраняя при этом оптимальную работу приложения или службы. И есть четыре ключевых момента, которые должна учитывать каждая компания, чтобы выбрать правильное решение для защиты от DDoS-атак.

1. Комплексная защита от DDoS-атак.

DDoS-атаки бывают разных форм, но основными типами являются атаки по протоколу соединения, объемные атаки и атаки на уровне приложений:

Атаки по протоколу соединения нацелены на заполнение таблиц соединений граничных устройств, таких как маршрутизаторы, брандмауэры и балансировщики нагрузки, что приведет к отключению сети. Распространенные примеры атак протокола соединения включают лавинную рассылку SYN и UDP.

Объемные атаки пытаются атаковать сеть напрямую и заполнять канал, чтобы предотвратить прохождение законных запросов. Распространенные примеры объемных атак включают наводнения ICMP, фрагментацию IP / ICMP и наводнения IPSec.

Атаки на уровне приложений являются наиболее разрушительным типом DDoS-атак, поскольку они нацелены на тот аспект вашего приложения или службы, который может повлиять на ваших клиентов или сотрудников. Кроме того, у них может быть низкая пропускная способность трафика, что затрудняет их обнаружение. Атаки на уровне приложений, такие как HTTP-потоки GET и усиление DNS, набирают популярность за последние несколько лет.

По-настоящему эффективное решение защиты от DDoS-атак должно быть достаточно комплексным, чтобы смягчить все эти векторы атак.

2. Масштабируемость для отражения крупнейших DDoS-атак

Ключевой вопрос, который следует задать: «Насколько масштабируемым должно быть мое решение защиты от DDoS-атак?» Ответ «очень», потому что объем DDoS-атак увеличивается с каждым днем.

Еще один вопрос, который следует задать: «Следует ли мне использовать облачную защиту от DDoS-атак или защищать свои системы с помощью локального решения?» Локальные устройства имеют ограниченную возможность масштабирования по запросу, поэтому вы должны подготовиться к срокам, связанным с увеличением вашей емкости. Более того, локальные решения для защиты от DDoS-атак могут быть сложными в установке и обслуживании, поэтому потребуется специальная ИТ-группа.

Облачные решения предоставляют простую услугу, которую не нужно устанавливать или обслуживать, и они могут автоматически масштабироваться в зависимости от размера DDoS-атаки. Они предлагают централизованное смягчение

последствий для обеспечения согласованной защиты для всех приложений и сайтов. Глобальное присутствие установленной службы смягчения последствий может обеспечить высокую пропускную способность очистки, защищая вас от массовых DDoS-атак. Когда дело доходит до защиты от DDoS-атак, облачные решения могут многое предложить.

3. Постоянная защита от DDoS-атак по сравнению с защитой по требованию: найти правильный баланс между инвестициями и защитой

Вы предпочитаете, чтобы весь онлайн-трафик всегда перенаправлялся, или вы предпочитаете перенаправлять трафик для очистки только во время атаки? Постоянное обнаружение DDoS-атак обеспечивает постоянную защиту, но также добавляет небольшую задержку к нормальной работе.

С другой стороны, защита от DDoS-атак по требованию будет ежедневно сокращать задержку приложений, но вы будете больше подвержены DDoS-атакам, когда они начнутся и до того, как вы начнете перенаправлять трафик. Решения с постоянным подключением дороже, чем решения по требованию, поэтому для удовлетворения бизнес-требований необходимо найти баланс между защитой и стоимостью.

4. Интегрированная и автономная защита от DDoS-атак: выбор между простотой и сложностью

Автономный подход к защите от DDoS-атак защитит только от DDoS-атак. Вам потребуются дополнительные службы защиты приложений, которые необходимо развертывать и управлять индивидуально, что может значительно усложнить работу. Благодаря интегрированному решению защита от DDoS-атак включает брандмауэры веб-приложений, управление ботами и защиту API, предлагая как комплексную защиту, так и простоту. Вам нужно управлять только одним решением, а не несколькими продуктами от нескольких поставщиков.

Пришло время пересмотреть свое решение для защиты от DDoS-атак

Citrix предлагает комплексное облачное решение для защиты от DDoS-атак с возможностью постоянной работы и по запросу. Он обладает одной из самых больших возможностей очистки для защиты от крупномасштабных DDoS-атак. Решение Citrix для защиты от DDoS-атак доступно как отдельная услуга, а также как интегрированное решение, которое включает брандмауэр веб-приложений, управление ботами и защиту API.

Имея 25-летний опыт работы, ясно, что DDoS-атаки никуда не денутся. И они станут намного больше и более распространенными с появлением 5G и распространением плохо защищенных устройств IoT.

Так что спросите себя сейчас: есть ли у меня правильная защита от DDoS-атак, чтобы помешать им и сохранить мой бизнес в безопасности?» ***(Pankaj Gupta. How to Choose the Right DDoS Protection Solution // Threatpost (https://threatpost.com/how-to-choose-the-right-ddos-protection-solution/176409/). 18.11.2021).***

***

«Злоумышленники нацелены на сотрудников крупных корпораций, базирующихся на Ближнем Востоке, с помощью мошенничества, в котором

используется особый «эфемерный» аспект инструмента управления проектами для ссылки на фишинговые страницы SharePoint.

Как выяснили исследователи, долгосрочная кампания целевого фишинга нацелена на сотрудников крупных корпораций с помощью электронных писем, содержащих PDF-файлы, которые ссылаются на недолговечные приложения Glitch, на которых размещены фишинговые страницы SharePoint для сбора учетных данных.

Исследователи из DomainTools обнаружили подозрительные PDF-файлы, которые сами по себе не содержат вредоносного содержимого, еще в июле, пишет старший исследователь безопасности Чад Андерсон в отчете, опубликованном в четверг.

Вместо этого вредоносная активность, распространяемая PDF-файлами, представляет собой ссылку на приложения Glitch, на которых размещены фишинговые страницы, которые включают обфусцированный JavaScript для кражи учетных данных, написал он. Glitch - это веб-инструмент управления проектами со встроенным редактором кода для запуска и размещения программных проектов, от простых веб-сайтов до крупных приложений.

Похоже, что кампания нацелена только на сотрудников, работающих на Ближнем Востоке, в качестве «единой кампании» в серии аналогичных фишинговых атак на тему SharePoint, пишет Андерсон.

Злоупотребление глюк

«Чтобы понять, как работает кампания, нужно понимать, как работает бесплатная версия Glitch», - пояснил Андерсон. Платформа позволяет приложению работать в течение пяти минут в Интернете с предоставленным Glitch именем хоста с использованием трех случайных слов, написал он.

«Например, один документ направил получателя на адрес hammerhead-resilient-birch.glitch [.] Me, где хранился вредоносный контент», - пояснил Андерсон в своем сообщении. «По истечении пяти минут учетная запись, стоящая за страницей, должна щелкнуть, чтобы снова открыть свою страницу».

Именно эта «эфемерная природа» делает общие пространства Glitch идеальными для злоумышленников, которые хотят размещать вредоносный контент, учитывая, что их трудно обнаружить. Это особенно верно, «потому что домены Glitch уже пользуются доверием и часто разрешены во многих сетях», - пояснил Андерсон.

«Пространства, в которых код может запускаться и размещаться бесплатно, являются золотой жилой для злоумышленников, особенно с учетом того, что многим из базовых доменов безоговорочно доверяют списки блокировок, которые собираются корпорациями», - написал он. «Такое делегирование доверия позволяет злоумышленникам использовать, казалось бы, безобидный PDF-файл, содержащий только ссылку на доверенный базовый домен, для обхода средств защиты и привлечения доверия пользователей».

В этой кампании злоумышленники использовали этот аспект наряду с кражей учетных данных на взломанных сайтах WordPress, чтобы создать цепочку атак, которая может обойти защитные инструменты, пишет Андерсон. Он добавил, что компания DomainTools Research попыталась поговорить с Glitch о возможном злоупотреблении платформой, но пока безуспешно.

Знакомство с кампанией

Исследователи DomainTools обнаружили активность угроз во время регулярного мониторинга и поиска вредоносных документов, связанных с предыдущими кампаниями, пишет Андерсон. В частности, команда наткнулась на PDF-документ, якобы являющийся счетом-фактурой, который включал раздел URI, связанный с внешней страницей - что, как он написал, обычно не вызывает тревогу.

Однако в этом случае адрес электронной почты был добавлен к URL-адресу в виде фрагмента, который обычно ссылается на элемент «id» на странице HTML, но которым также можно управлять с помощью CSS. Более того, адрес электронной почты принадлежал законному сотруднику корпорации, базирующейся в Объединенных Арабских Эмиратах, что, по словам Андерсона, было для исследователей попахившим целевым фишингом.

Исследователи искали похожие документы и обнаружили около 70 документов, датируемых 30 июля, и все они использовали разные URL-адреса для таргетинга на адреса электронной почты реальных людей, работающих в крупных корпорациях, пояснил он.

«Хотя каждый URL-адрес и адрес электронной почты были уникальными, сами документы всегда ссылались на одну и ту же страницу с именем: red.htm», - пишет Андерсон.

Уклонение от обнаружения

Исследователи заявили, что из-за недолговечности страниц, используемых для сбора учетных данных, перед ними стояла задача найти живые страницы, служащие основной полезной нагрузкой кампании. Им пришлось использовать инструмент URLScan, который позволял им выполнять поиск по всем просканированным сайтам за последний месяц.

В конце концов, исследователи обнаружили действующий сайт с помощью службы AnyRun, коммерческой «песочницы» и общедоступного хранилища исполняемых вредоносных программ, которые можно использовать для обнаружения конкретных взаимодействий с вредоносным кодом, пояснил Андерсон. Он написал, что хотя команда все еще не нашла полезную нагрузку следующего этапа, она все же обнаружила снимок экрана с фишинговым логином Microsoft SharePoint, который использовался для заманивания жертвы.

«Хотя содержимое страницы было недоступно, DomainTools Research учла имя документа, а также перенаправление на in.htm в качестве следующей страницы после страницы red.htm в исходном PDF-документе», - пояснил Андерсон..

Исследователи обнаружили ряд совпадающих HTML-документов, привязанных к предыдущим PDF-файлам на VirusTotal - исходным PDF-документам, предназначенным для передачи электронной почты цели в виде фрагмента URL-адреса - с использованием адресов электронной почты, предварительно заполненных на странице, написал он.

Команда также обнаружила «куски» обфусцированного кода JavaScript, которые после раскрытия показали, что адрес электронной почты и пароль отправляются на взломанные сайты WordPress и пересылаются на адрес электронной почты, указанный в теле сценария uzohifeanyi @ outlook [.] Com. Андерсон написал, что после того, как злоумышленники собирают учетные данные, JavaScript

перенаправляет пользователя на URL-адрес его адреса электронной почты». ***(Elizabeth Montalbano. Spear-Phishing Campaign Exploits Glitch Platform to Steal Credentials // Threatpost (https://threatpost.com/spear-phishing-exploits-glitch-steal-credentials/176449/). 18.11.2021).***

***

«Даже при наличии самой совершенной системы сканирования электронной почты и обнаружения фишинга фишинговые электронные письма по-прежнему являются очень распространенным вектором вторжений, который киберпреступники используют для внедрения вредоносных программ, в том числе программ-вымогателей, в корпоративную сеть. Это потому, что 1) все чаще используются легитимные системы; и 2) фишинговые электронные письма также могут быть эффективными, даже если сотрудники высокообразованы и умеют замечать их и сообщать о них.

К счастью, есть тактика для защиты вашей сети, даже если рассылку электронных писем невозможно остановить сразу.

Все более эффективный фишинг

Когда легитимные почтовые системы скомпрометированы и начинают рассылать вредоносные электронные письма из действительного источника, эффективность фишинга возрастает. Именно это произошло на выходных, когда одна из почтовых систем ФБР была взломана, чтобы рассылать фальшивые предупреждения о кибербезопасности тысячам людей.

Хотя в отправленном электронном письме не было никаких фишинговых ссылок, оно показывает, что такие взломы электронной почты могут создать серьезные проблемы безопасности для ИТ-специалистов. Большинство людей, получивших электронное письмо, вряд ли усомнятся в его легитимности - даже если они посмотрят на заголовки электронных писем, - потому что письмо пришло оттуда, откуда, по его словам, оно пришло (в приведенном выше случае - от ФБР).

Такой вид компромисса чрезвычайно опасен; он делает бесполезными такие механизмы аутентификации электронной почты, как DMARC, SPF и DKIM, поскольку электронная почта исходит из авторизованного источника; Таким образом, это означает, что антиспамовые и антифишинговые программы с меньшей вероятностью пометят сообщение как вредоносное.

Независимо от фактического ущерба, факт остается фактом: такие взломы позволяют злоумышленникам выполнять очень эффективные фишинговые атаки. Итак, если система электронной почты была взломана, что организации могут сделать, чтобы защитить свои сети от таких атак?

Защита сети, когда фишинг невозможно остановить сразу

Специалисты по сетям и безопасности должны использовать множество ресурсов для защиты бизнеса от крупных атак. Хотя было бы слишком исчерпывающим перечислять их все, давайте рассмотрим хорошо продуманный, многоуровневый подход, чтобы попытаться помешать этим атакам получить контроль над сетью:

1. Расширенная защита электронной почты

Хотя безопасность электронной почты не является безошибочной, как обсуждалось выше, в системе безопасности электронной почты есть некоторые функции, которые следует включить, чтобы вероятность заражения из-за компрометации электронной почты была как можно ниже.

Один из наиболее эффективных способов остановить фишинговые атаки - включить защиту ссылок в настройках корпоративной электронной почты. Такая защита позволяет почтовой системе открывать любые ссылки и удалять те, которые ведут к загрузке вредоносных программ. Очевидно, что эта защита не может защитить от всех гнусных ссылок, но она, безусловно, может помочь уменьшить количество вредоносных ссылок, которые попадают в почтовые ящики.

Установка более высоких уровней спам-фильтра также может помочь заблокировать электронные письма со злым умыслом. В этих настройках используется расширенное эвристическое моделирование для поиска писем с плохой формулировкой или писем с формулировкой, аналогичной другим известным вредоносным письмам. Опять же, хотя это и не идеально, это, безусловно, важная первая линия защиты.

2. Системы обнаружения и предотвращения вторжений

Будем надеяться, что во всех организациях уже есть брандмауэры, которые блокируют попадание известных вредоносных программ в сеть; однако в некоторых из них нет систем, блокирующих распространение вредоносного ПО после его проникновения. Системы обнаружения и предотвращения вторжений позволяют организациям обнаруживать (обнаруживать) и устранять / изменять (предотвращать) атаку, прежде чем она сможет захватить другие системы. Эти системы часто используются как согласованные усилия с защитой конечных точек (антивирус), которая помогает устранять вирусы и распространенные вредоносные программы.

Здесь есть одно предостережение: эти системы, хотя и очень сложные, не так эффективны при обнаружении относительно новых вредоносных программ или вредоносных программ, которые эффективно скрываются в течение длительных периодов времени. Это связано с тем, что система просматривает пакеты, когда они проходят по сети, и поэтому часто пропускает вредоносную активность, которая перемещается по сети через спорадические промежутки времени в течение нескольких дней или месяцев. Таким образом, они, как и повышенная безопасность электронной почты, должны быть включены в более широкий подход, включающий другие средства защиты.

3. Обнаружение потоковой сети и ответ на нее (NDR)

Еще одним важным аспектом многоуровневого подхода является обнаружение сети и ответ на нее (NDR), который специалисты по безопасности могут использовать для обнаружения подозрительного трафика и анализа / блокировки вредоносных программ, которые проходят через другие системы безопасности.

Согласно Gartner, системы отчетов о недоставке работают, применяя «машинное обучение и другие аналитические методы к сетевому трафику», и «помогают предприятиям обнаруживать подозрительный трафик, который отсутствует у других инструментов безопасности». Поведенческие инструменты NDR на основе потоков дополняют решения для обнаружения на основе сигнатур,

поскольку они могут обнаруживать аномальное поведение на основе ранее известного сетевого трафика.

Сбалансированный подход

Эти три варианта, а также обучение пользователей, обнаружение конечных точек и другие передовые методы могут способствовать снижению эффективности сложных фишинговых атак. Развертывая многоуровневый подход к безопасности, даже при взломе сторонних систем группы безопасности более эффективны в предотвращении распространения вредоносных программ по своей сети». ***(Justin Jett. 3 Top Tools for Defending Against Phishing Attacks // Threatpost (https://threatpost.com/tools-defending-phishing-attacks/176463/). 18.11.2021).***

***

«Защиты через безопасный почтовый шлюз (SEG) не всегда достаточно, чтобы фишинговые письма не доставляли вымогателей сотрудникам, особенно если киберпреступники используют законные облачные сервисы для размещения вредоносных страниц.

Исследователи бьют тревогу в связи с фишинговым письмом, инициирующим хеллоуинское наступление программы-вымогателя MICROP, которое, по их наблюдениям, проникает в почтовый ящик жертвы несмотря на то, что он защищен SEG.

Порядок заражения

В исходном письме якобы требовалась поддержка «DWG, следующего за списком расходных материалов», который предположительно содержит гиперссылку на URL-адрес Google Диска. URL-адрес на самом деле является ссылкой для заражения, по которой был загружен файл.MHT.

«Расширения файлов.MHT обычно используются веб-браузерами в качестве архива веб-страниц», - пояснили исследователи Cofense. «После открытия файла цель представляется в размытой и явно проштампованной форме, но злоумышленник использует файл.MHT для доступа к вредоносной программе».

Эти полезные данные поступают в виде загруженного файла .RAR, который, в свою очередь, содержит файл.EXE.

«Исполняемый файл представляет собой DotNETLoader, который использует сценарии VBS для удаления и запуска вымогателя MIRCOP в памяти», - говорится в анализе.

Кампания не особенно сложна, но использование Google Диска позволило ей пройти через SEG.

«Его первая приманка — это бизнес-тематика, использующая сервис, такой как Google Drive, который предприятия используют для доставки файлов», - пояснили исследователи. «Быстрое развертывание от полезной нагрузки MHT до окончательного шифрования показывает, что эту группу не беспокоит подлость. Поскольку доставка этой программы-вымогателя настолько проста, особенно беспокоит то, что это электронное письмо попало в почтовый ящик среды, использующей SEG».

Получатель этого Halloween MICROP сообщил, что электронное письмо является подозрительным, что привело Cofense к обнаружению новой потенциальной угрозы.

Кровавая тема, необычное использование Skype

«Программа-вымогатель MIRCOP, также известная как программа-вымогатель Crypt888, шифрует файлы пользователей, чтобы удерживать их в заложниках», - сообщили аналитики Cofense. «После удовлетворения требования об оплате злоумышленник обещает предоставить метод дешифрования. Для этой атаки злоумышленник дает набор инструкций на обоях ".

Пользователь также не может открывать какие-либо приложения, кроме нескольких веб-браузеров, которые могут предоставить им доступ к их адресу электронной почты, который используется для связи со злоумышленником», - написали исследователи Cofense в недавнем сообщении. «Затем адрес электронной почты используется для настройки платежа, необходимого для получения доступа к инструменту дешифрования, который, как утверждает злоумышленник, разблокирует файлы и приложения».

Они добавили: «Использование Skype в качестве средства для переговоров - редкость, поскольку у большинства организованных банд вымогателей есть специальные сайты или мобильные приложения для чата».

Просмотр паролей, хранящихся локально

Другой интересный аспект этой кампании - обнаруженный командой Cofense вредоносный файл под названием «PI2.exe». Он крадет пароли из веб-браузеров, включая Explorer, Google Chrome, Firefox и Opera, предоставляя злоумышленникам как боковой доступ к сети, так и точку входа для будущих атак.

«Глядя на хэш SHA256 этого исполняемого файла на Virus Total, он может быть связан с десятками вредоносных исполняемых файлов, начиная с июня этого года», - говорят исследователи.

Этот «инструмент» указывает на то, что переход к работе вне офиса только еще больше подвергает бизнес такого рода атакам, по словам Миклена Кеффелера, консультанта по безопасности приложений из nVisium, поэтому локальное управление паролями, а также ограничение разрешений в облаке становятся все более популярными. «необходимо», - объяснил он Threatpost.

«Crypt888 стремится к горизонтальной эскалации привилегий путем кражи паролей, которые пользователи могли сохранить локально - неизбежно для использования другими способами, которые могут нанести ущерб бизнесу», - сказал Кеффелер. «По мере того, как облако продолжает расти, эти сохраненные пароли становятся ключевым вектором атаки, поскольку они часто могут предоставлять большие объемы доступа - практически без контроля безопасности». ***(Becky Bracken. Ransomware Phishing Emails Sneak Through SEGs // Threatpost (https://threatpost.com/ransomware-phishing-emails-segs/176470/). 18.11.2021).***

***

«Исследователи установили 320 приманок, чтобы увидеть, как быстро злоумышленники будут атаковать открытые облачные сервисы, и сообщили, что 80% из них были взломаны менее чем за 24 часа.

Злоумышленники постоянно сканируют Интернет в поисках незащищенных служб, которые могут быть использованы для доступа к внутренним сетям или выполнения других вредоносных действий.

Чтобы отследить, какое программное обеспечение и услуги являются целью злоумышленников, исследователи создают общедоступные приманки. Приманки — это серверы, настроенные так, чтобы они выглядели так, как будто на них запущено различное программное обеспечение, в качестве приманки для отслеживания тактики злоумышленников.

Соблазнительная приманка

В новом исследовании, проведенном подразделением 42 Palo Altos Networks, исследователи установили 320 приманок и обнаружили, что 80% приманок были взломаны в течение первых 24 часов.

Развернутые приманки включали в себя приманки с протоколом удаленного рабочего стола (RDP), протоколом защищенной оболочки (SSH), блоком сообщений сервера (SMB) и службами баз данных Postgres, и они поддерживались с июля по август 2021 года.

Эти приманки были развернуты по всему миру, в том числе в Северной Америке, Азиатско-Тихоокеанском регионе и Европе.

Как передвигаются злоумышленники

Время до первого компромисса аналогично тому, насколько нацелен тип службы.

Для SSH-приманок, которые были наиболее уязвимыми, среднее время первого взлома составило три часа, а среднее время между двумя последовательными атаками - около 2 часов.

Unit 42 также наблюдал примечательный случай, когда злоумышленник взломал 96% из 80 экспериментальных приманок Postgres всего за 30 секунд.

Это открытие очень тревожно, поскольку развертывание новых обновлений безопасности по мере их выпуска может занять несколько дней, а то и больше, в то время как злоумышленникам нужны часы, чтобы использовать уязвимые службы.

Наконец, что касается того, имеет ли место какое-либо значение, регион APAC привлек наибольшее внимание со стороны злоумышленников.

Подавляющее большинство (85%) IP-адресов злоумышленников наблюдались в течение одного дня, что означает, что субъекты редко (15%) повторно используют один и тот же IP-адрес для последующих атак.

Это постоянное изменение IP-адреса делает правила брандмауэра «уровня 3» неэффективными против большинства злоумышленников.

Что может иметь больше шансов смягчить атаки, так это блокировка IP-адресов путем извлечения данных из проектов сканирования сети, которые ежедневно выявляют сотни тысяч вредоносных IP-адресов.

Однако Unit 42 проверил эту гипотезу на подгруппе из 48 приманок и обнаружил, что блокировка более 700 000 IP-адресов не имеет существенной разницы в количестве атак между подгруппой и контрольной группой…». ***(Bill Toulas. Threat actors find and compromise exposed services in 24 hours // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/threat-actors-find-and-compromise-exposed-services-in-24-hours/). 23.11.2021).***

***

«Специалист компании Microsoft поделился интересной статистикой: большинство злоумышленников предпочитают брутфорсить только короткие пароли, и лишь малый процент атак нацелен на длинные пароли, содержащие специальные символы.

Статистику для этого анализа исследователь собрал с многочисленных honeypot-серверов, которыми он заведует по долгу службы, изучая актуальные среди злоумышленников тенденции:

«Я проанализировал учетные данные, использованные более чем в 25 000 000 брутфорс-атак на SSH, — рассказывает компании эксперт Microsoft Росс Бевингтон (Ross Bevington). — В 77% случаев брутфорс был направлен на пароли от 1 до 7 символов. Пароль длиной более 10 символов встречался только в 6% случаев».

Также эксперт пишет, что лишь в 7% случаев во время брутфорс-атак использовался хотя бы один специальный символ, тогда как в 39% случаев использовалась хотя бы одна цифра. При этом ни одна из попыток брутфорса не учитывала пароли, которые могут содержать пробелы.

Результаты этого исследования демонстрируют, что более длинные пароли, содержащие специальные символы, скорее всего, защищены от подавляющего большинства подобных атак (если учетные данные не «утекли» в открытый доступ иным образом и не входят в специальные словари и списки злоумышленников).

Бевингтон отмечает, что, основываясь на данных, полученных из 14 млрд брутфорс-атак на honeypot-серверы Mocrosoft, атаки на RDP утроились по сравнению с 2020 годом, продемонстрировав рост на 325%. Кроме того, на 178% участились атаки на сетевые службы печати (Network printing services), а также Docker и Kubernetes — на 110%...» ***(Мария Нефёдова. Хакеры редко брутфорсят пароли, длиннее 7 символов // Xakep (https://xakep.ru/2021/11/23/bruteforce-stats/). 23.11.2021).***

***

«Киберпреступник или киберпреступники, называющие себя AgainstTheWest (ATW), заявили о взломе китайской телестанции. Судя по скриншотам, опубликованным vx-underground, злоумышленники запланировали прямую трансляцию на 53 минуты и предоставили QR-код для просмотра.

Кто такие AgainstTheWest, и можно ли верить их заявлениям, не совсем понятно. Если это действительно новая хакерская группировка, то появилась она недавно, и сведений о ней почти нет. Судя по статье в англоязычной «Википедии», AgainstTheWest – это хактивистская группировка, «поддерживающая Тайвань». Если верить статье, она осуществила целый ряд кибератак на серьезные организации в Китае, причем все они имели место в октябре-ноябре 2021 года (сама статья в «Википедии» была создана в ноябре).

Среди заявленных жертв AgainstTheWest есть Народный Банк Китая (подконтрольный правительству центральный банк страны), Центр по контролю и профилактике заболеваний, Министерство общественной безопасности,

Министерство науки и технологий, Государственная администрация по регулированию рынка, производитель кабелей Zhongtian Technology Submarine Cable Co, Alibaba Cloud и компания Tencent.

В открытом интернете помимо статьи в «Википедии» AgainstTheWest можно найти только на форуме RaidForums. Пользователь с таким именем был зарегистрирован 12 октября, а ссылки на Twitter и Instagram ведут на страницы Интерпола». ***(Таинственные AgainstTheWest заявили о взломе китайской телестанции // SecurityLab.ru (https://www.securitylab.ru/news/526847.php). 25.11.2021).***

***

«Компания Tet (ранее Lattelecom) накануне всемирной распродажи сообщает о росте числа кибератак. В 2021 году специалистами Tet было выявлено 36 миллионов спам-писем, заблокировано 90 900 электронных писем с вирусами и предотвращено 2 506 DDoS-атак.

Согласно последним исследованиям Tet по кибербезопасности, которые приведены в пресс-релизе компании, ежедневно компания блокирует минимум девять DDoS-атак на бизнес и частные лица. Количество киберпреступлений продолжает расти, и тенденция сохраняется во всем мире, так как хакеры становятся все более активными. О повышении активности и изобретательности киберпреступников также свидетельствует рост количества уязвимостей нулевого дня (Zero day). Они подразумевают возможность кибератак на программное обеспечение до того, как производитель ПО ее обнаружил. В этом году уязвимостей нулевого дня выявлено в два раза больше, чем в 2020 году. По сравнению с 2018 годом их количество увеличилось в четыре раза.

Согласно данным клиентов и партнеров Tet, в настоящее время один час простоя системы электронной коммерции может обходиться в не менее пяти млн рублей упущенной выгоды. С приближением распродажи в Черную пятницу крупные предприятия э-коммерции на 2-3 недели усиливают свои ресурсы до 250%, что существенно увеличивает поверхность атаки. Специалисты Tet выделяют электронную коммерцию как наиболее уязвимую отрасль в период распродаж.

«Большое количество компаний все еще минимально вкладывается в кибербезопасность, и организации редко заблаговременно обеспечивают защиту данных. При этом бизнесу важно уделять особое внимание ИБ, чтобы уменьшить возможности мошенников развивать нелегальную деятельность за счет честного бизнеса. Со своей стороны для изменения ситуации в области кибербезопасности, мы разработали руководство по основам кибергигиены, ознакомиться с которым приглашаем всех жителей России», — комментирует Артур Филатов, руководитель бизнеса кибербезопасности Tet (ранее Lattelecom).

Руководство по основам кибергигиены включает в себя свод рекомендаций для частных лиц и компаний. Состоит из семи блоков, которые помогут обезопасить деятельность в интернете, настроить удаленный рабочий доступ и научат реагировать на фишинговые письма». ***(За 4 года количество уязвимостей нулевого дня выросло более чем в 4 раза // ООО "ИКС-МЕДИА"***

(https://www.iksmedia.ru/news/5863883-Tet-za-4-goda-kolichestvo-uyazvimos.html). 25.11.2021).

****

Діяльність хакерів та хакерські угруповування

«Lazarus, аффилированная с Северной Кореей группа, спонсируемая государством, снова пытается атаковать исследователей безопасности с помощью бэкдоров и троянов удаленного доступа, используя троянскую пиратскую версию популярного программного обеспечения обратного инжиниринга IDA Pro.

О результатах сообщил на прошлой неделе исследователь безопасности ESET Антон Черепанов в серии твитов.

IDA Pro - это интерактивный дизассемблер, предназначенный для перевода машинного языка (также известного как исполняемые файлы) на язык ассемблера, позволяющий исследователям безопасности анализировать внутреннюю работу программы (вредоносной или иной), а также выполнять функции отладчика для обнаружения ошибок.

«Злоумышленники объединили оригинальное программное обеспечение IDA Pro 7.5, разработанное [Hex-Rays], с двумя вредоносными компонентами», - сообщила словацкая фирма по кибербезопасности, один из которых является внутренним модулем под названием «win_fw.dll», который запускается во время установки приложения. Эта измененная версия затем настраивается для загрузки второго компонента с именем «idahelper.dll» из папки плагинов IDA в системе.

После успешного выполнения двоичный файл idahelper.dll подключается к удаленному серверу www [.] Devguardmap [.] Org» для получения последующих полезных данных. Домен также примечателен тем, что ранее он был связан с аналогичной кампанией при поддержке Северной Кореи, нацеленной на профессионалов в области безопасности и раскрытой Группой анализа угроз Google в начале марта.

В тайной операции злоумышленники создали поддельную охранную компанию, известную как SecuriElite, вместе с несколькими учетными записями в социальных сетях Twitter и LinkedIn, пытаясь обманом заставить ничего не подозревающих исследователей посетить веб-сайт компании, зараженный вредоносным ПО, чтобы запустить эксплойт, который использовал затем нулевой день в браузере Internet Explorer. В конечном итоге Microsoft решила эту проблему в своем обновлении Patch Tuesday за март 2021 года.

Также известен под прозвищами APT38, Hidden Cobra, алюминий и цинк, Lazarus Group, как известно, быть активным, как еще в 2009 году и связан с строкой из атак для получения финансовой выгоды и сбора конфиденциальной информации, полученной от скомпрометированных среды.

«Киберпрограмма Северной Кореи представляет собой растущую угрозу шпионажа, краж и атак», - говорится в Ежегодной оценке угрозы директора

национальной разведки США на период до 2021 года, опубликованной ранее в апреле этого года.

«Северная Корея провела кибер-кражу финансовых учреждений и криптовалютных бирж по всему миру, потенциально похитив сотни миллионов долларов, вероятно, для финансирования государственных приоритетов, таких как ядерные и ракетные программы». ***(Ravie Lakshmanan. North Korean Hackers Target Cybersecurity Researchers with Trojanized IDA Pro // The Hacker News (https://thehackernews.com/2021/11/north-korean-hackers-target.html). 15.11.2021).***

***

«Согласно отчету, опубликованному во вторник ведущей платформой для выявления ошибок, за последний год этические хакеры предотвратили киберпреступность на сумму более 27 миллиардов долларов США.

В своем ежегодном отчете «Внутри разума хакера» Bugcrowd утверждал, что этичные хакеры, работающие на его платформе, смогли предотвратить потери организаций от киберпреступности, выявив уязвимости, которые в противном случае остались бы незамеченными.

Отчет основан на опросе пользователей платформы и исследованиях в области безопасности, проведенных с мая 2020 года по август 2021 года, в дополнение к миллионам точек данных, собранных по уязвимостям из почти 3000 программ безопасности.

«Хакерство уже давно оклеветано стереотипными изображениями преступников в капюшонах, тогда как на самом деле этические хакеры пользуются большим доверием и являются трудолюбивыми экспертами, которые позволяют организациям быстрее выпускать безопасные продукты на рынок», - сказал в пресс-релизе президент и генеральный директор Bugcrowd Ашиш Гупта.

В отчете отмечается, что почти три из четырех этических хакеров (74 процента) согласны с тем, что с начала пандемии Covid-19 количество уязвимостей увеличилось.

«Из-за быстрых изменений, которые претерпел почти каждый из-за пандемии, появилось множество уязвимостей и слабых мест», - заметил Джон Бамбенек, главный специалист по поиску угроз в Netenrich, компании, работающей в сфере ИТ и цифровой безопасности в Сан-Хосе, Калифорния.

«Вы можете делать что-то быстро или делать что-то безопасно, и по необходимости мы делали это быстро», - сказал он TechNewsWorld.

Изменение ландшафта уязвимости

Нет сомнений в том, что ландшафт уязвимостей изменился с начала пандемии, добавил Джейк Уильямс, соучредитель и технический директор BreachQuest, компании по реагированию на инциденты в Далласе.

«По мере того как большинство работников умственного труда перешли от локальной к удаленной работе, сетевая архитектура кардинально изменилась, - пояснил он TechNewsWorld.

«Мы рассматриваем безопасность как пересечение конфиденциальности, целостности и доступности», - продолжил он. «Переход к удаленной работе

произошел так быстро, что большинство организаций работали только над доступностью, не беспокоясь о других аспектах безопасности».

«Уязвимости, вызванные быстрым переходом к удаленной работе, несомненно, будут обнаруживаться и дальше», - настаивал Уильямс.

Пандемия также увеличила спрос на новые таланты в компаниях, занимающихся кибербезопасностью. Из множества сертификатов, которые могут получить кибер-новички, Certified Ethical Hacker считает наиболее важным Абхиджит Гош, технический директор и соучредитель Confluera, производителя платформы отслеживания киберугроз в Пало-Альто, Калифорния.

«Помимо демонстрации своего понимания инструментов и методов взлома, опыт проведения хакерских атак и соревнований по ловле флага мало чем отличается от реального сценария, в котором профессионалы в области кибербезопасности должны реагировать в режиме реального времени на атаку. в процессе», - сказал он TechNewsWorld.

«Я также связываю эту сертификацию со страстью человека к этой отрасли, - добавил он, - что вам часто понадобится, когда кибератаки ударит в самое неподходящее время, например, в выходные и праздничные дни».

Необходим непрерывный мониторинг

В отчете Bugcrowd также отмечается, что более девяти из 10 опрошенных этических хакеров (91 процент) признали, что тестирование на определенный момент времени - что они и делают - не может защитить организацию круглый год.

«Это отражение того, что профессионалы по доставке программного обеспечения знали на протяжении многих лет - более короткие и гибкие циклы улучшают качество», - сказал Тим Уэйд, технический директор группы технического директора Vectra AI, поставщика автоматизированных систем из Сан-Хосе, Калифорния. решения для управления угрозами

«Быстрые, менее масштабные мероприятия с возможностью постепенно измерять возможности с течением времени почти наверняка сдвинут иглу для организаций», - сказал он TechNewsWorld.

Бонусы за ошибки имеют свои достоинства в области кибербезопасности, но по-прежнему относятся к категории сосредоточения усилий на пост-развертывании и реагирования, добавил Арчи Агарвал, основатель и генеральный директор ThreatModeler, поставщика автоматизированного моделирования угроз в Джерси-Сити, штат Нью-Джерси.

«Я бы предпочел, чтобы законные исследователи безопасности всегда находили уязвимости раньше, чем преступники, однако отраслевой фокус должен сместиться в сторону упреждающей, непрерывной безопасности на этапе проектирования и сборки», - сказал он TechNewsWorld.

«Только используя автоматическое моделирование угроз, которое органично пронизывает весь жизненный цикл разработки программного обеспечения, мы начнем по-настоящему бороться с масштабом обнаруживаемых уязвимостей», - сказал он.

Образ жизни хакера

В отчете также содержится информация об образе жизни, опыте и мотивах этических хакеров на платформе Bugcrowd, а также несколько «близких» статей о некоторых хакерах.

«Меня всегда вдохновляли изобретательность и предпринимательский склад ума тех, кто стремится к этическому хакерству», - заметил основатель и генеральный директор Bugcrowd Кейси Эллис.

«Наш последний отчет показывает, что 79 процентов этичных хакеров сами научились взламывать, используя онлайн-ресурсы», - сказал он TechNewsWorld.

«Отчет также показал, что это самое молодое и наиболее этнически разнообразное поколение этичных хакеров в истории», - добавил он. «Влияние этой группы на предотвращение кибератак и развитие отрасли колоссально, и это обязательно будет продолжаться».

Крейг Янг, главный исследователь безопасности в Tripwire, компании по обнаружению и предотвращению угроз кибербезопасности из Портленда, штат Орегон, объяснил, что организации используют программы вознаграждения за ошибки как форму краудсорсингового тестирования безопасности.

«Ни одна группа безопасности, какой бы зрелой она ни была, не способна выявлять 100% проблем в 100% случаев, - сказал он TechNewsWorld, - но программы вознаграждения за ошибки помогают снизить риск того, что пропущенная проблема будет использована для вторжения».

Преимущество "многих глаз"

«Наличие большого количества глаз, особенно при необходимом таланте и обучении, - одна из лучших вещей, которые вы можете сделать для поиска и устранения ошибок», - добавил Роджер Граймс, защитник из KnowBe4, поставщика услуг по обучению вопросам безопасности в Клируотере, штат Флорида.

«Независимо от того, насколько хороша ваша внутренняя команда по поиску ошибок, внешняя команда всегда найдет ошибки, которых не обнаружила внутренняя группа», - сказал он TechNewsWorld. «Программы Bug Bounty приглашают множество внешних людей и команд искать ошибки в вашем программном обеспечении - до того, как это сделают злоумышленники».

Несмотря на те преимущества, которые этические хакеры могут принести организации, остаются очаги недоверия.

«Большинству отраслей не нравятся программы вознаграждений за ошибки и этические хакеры, потому что они не понимают огромных преимуществ», - сказал Граймс. «Они думают, что приглашение хакеров взломать их программное обеспечение приведет к увеличению злоумышленников в целом, в то время как реальный результат будет прямо противоположным».

Тем не менее, он отметил, что с годами ситуация наладилась. «Десять лет назад большинство организаций никогда бы не разрешили программы по выявлению ошибок», - заметил он. «Теперь у вас есть множество конкурирующих консорциумов по борьбе с ошибками и людей, которые зарабатывают деньги на обнаружении ошибок до того, как это сделают злонамеренные хакеры». ***(John P. Mello Jr. Bugcrowd Reports Ethical Hackers Prevented $27B in Cybercrime // ECT News Network, Inc. (https://www.technewsworld.com/story/bugcrowd-reports-ethical-hackers-prevented-27b-in-cybercrime-87340.html). 17.11.2021).***

***

«Русскоязычная группа Void Balaur, также известная под названием Rockethack, была определена как плодовитая группа кибер-наемников, которую можно нанять для взлома электронной почты и аккаунтов в социальных сетях высокопоставленных целей по всему миру.

После более чем годичного мониторинга Void Balaur компания Trend Micro опубликовала отчет, в котором идентифицировано более 3500 целей группы. Amnesty International также выявила кибератаки на активистов и журналистов, работающих в Узбекистане, которые были осуществлены службой кибернаемничества.

«Наше исследование показало четкую картину: Void Balaur собирает самые частные и личные данные компаний и частных лиц, а затем продает эти данные тому, кто хочет за это заплатить», - говорится в отчете Trend Micro.

За дополнительную плату группа часто может предоставить полные копии почтовых ящиков, украденных без помощи целевого пользователя, сообщает Trend Micro.

Void Balaur получает рейвы на подпольных форумах

По словам аналитиков Trend Micro, предприимчивый и вечно собирающий массу данных, которые впоследствии можно будет продать, деятельность Void Balaur началась в 2015 году. К 2019 году группа интенсивно продавала личные данные, собранные о гражданах России, в том числе сведения о судимости, кредитную историю, отчеты о рейсах, остатки на счетах и распечатки текстовых SMS-сообщений, поясняется в отчете. Группа также продает данные сотовых телефонов, которые, скорее всего, были получены путем подкупа сотрудников телекоммуникационных компаний или инсайдеров, говорится в отчете.

По словам Trend Micro, популярными целями группы являются СМИ и сайты политических новостей, журналисты и правозащитники.

«Пустота Балаур тоже не прочь преследовать более громкие цели, поскольку группа также начала нападать на бывшего главу разведывательного агентства, действующих министров правительства, членов национального парламента в одной из восточноевропейских стран и даже кандидатов в президенты. - добавил он.

В настоящее время группа рекламирует свои услуги на российских подпольных форумах Darkmoney и Probiv, сообщает Trend Micro.

«Кажется, что Void Balaur пользуется большим уважением на этих подпольных форумах, поскольку отзывы об их услугах почти единодушно положительны, а их клиенты указывают на способность злоумышленника предоставить запрошенную информацию вовремя, а также на качество данных. при условии », - говорится в сообщении.

Группа использует вредоносные инструменты, такие как Z * Stealer credential stealer и DroidWatcher, которые крадут данные и добавляют возможности отслеживания и шпионажа, сообщает Trend Micro. Фирма предложила индикаторы компрометации Void Balaur как часть своего отчета.

Балаур Бездны атакует хранилища данных

Группа также начала атаки на криптовалютные биржи, такие как EMXO, которые, как говорится в отчете, неоднократно подвергались нападениям со стороны Void Balaur.

В сентябре группа нацелена на главу разведывательного агентства, министров правительства и двух членов парламента Восточной Европы, сообщает Trend Micro, но с 2020 года нападения на государственных чиновников и кандидатов в странах, включая Армению, Беларусь, Францию, Итлей, совершались., Казахстан, Норвегия, Россия и Украина, говорится в сообщении. Исследователи обнаружили, что Void Balaur также активен в США, Израиле и Японии.

В течение 2020 года Void Balaur более года атаковал один российский конгломерат, демонстрируя его терпение и настойчивость, сообщает Trend Micro. Он был нацелен на членов правления организации, руководителей и даже членов семьи владельца компании-миллиардера.

Группа, похоже, готова работать практически в любом секторе, который предлагает множество ценных данных, как обнаружила компания Trend Micro в своем анализе, включая телекоммуникации, радио- и спутниковую связь, банковское дело, авиацию и медицинское страхование; и даже клиники экстракорпорального оплодотворения (ЭКО) в России, биотехнологии и генетическое тестирование.

«Что отличает Void Balaur от большинства киберпреступных групп, так это огромное количество различных видов преступной деятельности, в которые они вовлечены», - сказал Threatpost в ответ на отчет Арчи Агарвал, генеральный директор ThreatModeler. «Казалось бы, они работают почти во всех отраслях промышленности, с разными типами данных и даже нацелены на высокопоставленных лиц. Они определенно не делают различий ».

Восстание кибер-наемников

Компания Trend Micro пришла к выводу, что экосистема кибернаемников поддерживается интересом правительств стран мира к использованию этих злоумышленников в рамках своих национальных стратегий кибербезопасности.

«Во-первых, услуги и инструменты кибернаемников могут быть использованы в наступательных атаках против терроризма и организованной преступности, а также для нацеливания на иностранные активы», - предупреждают исследователи. «Во-вторых, их также можно продавать в другие страны и использовать в качестве экономического или политического инструмента во внешней политике. Хотя это может принести пользу некоторым странам, это также создает огромный риск возможной негативной реакции, когда злонамеренные элементы используют эти инструменты. Хуже того, инструменты, которые были проданы за границу, могут в конечном итоге использоваться против граждан страны, которая изначально экспортировала эти инструменты». ***(Becky Bracken. Cyber-Mercenary Group Void Balaur Attacks High-Profile Targets for Cash // Threatpost (https://threatpost.com/cyber-mercenary-void-balaur/176230/). 11.11.2021).***

***

«На русскоязычных форумах по борьбе с киберпреступностью назревает некоторая необычная активность, где хакеры, похоже, обращаются к китайским коллегам для сотрудничества.

Эти попытки привлечь китайских злоумышленников в основном видны на хакерском форуме RAMP, который побуждает говорящих на китайском языке актеров участвовать в обсуждениях, делиться советами и сотрудничать в борьбе с атаками.

Китайские пользователи на русскоязычных форумах

Согласно новому отчету Flashpoint, высокопоставленные пользователи и администраторы RAMP сейчас активно пытаются общаться с новыми участниками форума на китайском с машинным переводом.

Сообщается, что на форуме было зарегистрировано не менее тридцати новых пользователей из Китая, так что это может стать началом чего-то примечательного.

Исследователи предполагают, что наиболее вероятная причина заключается в том, что российские банды программ-вымогателей стремятся создать альянсы с китайскими игроками для проведения кибератак против целей в США, обмена уязвимостями или даже привлечения новых специалистов для своих операций по программе-вымогателю как услуге (RaaS).

Аналитик угроз сообщил BleepingComputer ранее в этом месяце, что эта инициатива была инициирована администратором RAMP, известным как Kajit, который утверждает, что недавно провел некоторое время в Китае и может говорить на этом языке.

В предыдущей версии RAMP он намекнул, что будет приглашать китайских злоумышленников на форум, который, похоже, сейчас и происходит.

Однако российские хакеры, пытающиеся сотрудничать с китайскими злоумышленниками, не ограничиваются хакерским форумом RAMP, поскольку Flashpoint также видел подобное сотрудничество на хакерском форуме XSS.

«На скриншоте ниже пользователь XSS« hoffman »приветствует двух участников форума, которые оказались китайцами», - объясняет новое исследование Flashpoint.

«Злоумышленник спрашивает их, могут ли они предоставить информацию о программах-вымогателях и покупке различных уязвимостей системы. Судя по всему, это китайский язык с машинным переводом».

Основываясь на предыдущей истории, связанной с администраторами RAMP, Flashpoint подчеркивает, что всегда есть вероятность того, что это просто дымовая завеса, поскольку настоящие китайские пользователи не присоединились к RAMP.

В прошлом месяце администратор RAMP, известный как 'Orange' или 'boriselcin' и управляющий сайтом Groove, опубликовал сообщение, в котором призвал злоумышленников атаковать США.

После того, как СМИ осветили этот пост, в том числе BleepingComputer, актер Groove заявил, что операция была фальшивкой с самого начала и была создана для троллинга и манипулирования исследователями СМИ и безопасности.

Исследователи в области безопасности из McAfee и Intel 471 полагают, что это, скорее всего, просто злоумышленник, пытающийся скрыть тот факт, что попытка злоумышленника с использованием программы-вымогателя как услуги не сработала, как планировалось.

В связи с этим предварительные действия администратора RAMP требуют, чтобы мы относились ко всему, что они говорят, с некоторым скептицизмом.

Тем не менее, операция вымогателя Conti недавно разместила сообщение на форуме RAMP, чтобы привлечь аффилированных лиц и купить первоначальный доступ к сетям. На скриншоте, предоставленном BleepingComputer, банда говорит, что обычно они работают только с русскоязычными хакерами, но делают исключение для китайскоязычных злоумышленников из уважения к администратору RAMP…

Таким образом, похоже, что форум RAMP активно приглашает говорящих по-китайски лиц, создающих угрозы, для участия в обсуждениях и атаках.

RAMP продолжает расти

Теперь, когда RAMP снова в сети, он, похоже, неуклонно растет, несмотря на волны DDOS, которые он выдержал вскоре после его запуска.

RAMP была создана прошлым летом одним из основных членов первоначальной банды вымогателей Babuk с целью служить новым местом для утечки ценных данных, украденных в результате кибератак, и вербовки партнеров, связанных с программами-вымогателями.

Заметный случай такой утечки произошел в сентябре, когда администратор RAMP опубликовал 498 908 учетных данных Fortinet VPN для доступа к 12 856 устройствам в различных корпоративных сетях.

Хотя многие из этих учетных данных были старыми, исследователи безопасности заявили, что многие из учетных данных все еще действительны и позволили форуму RAMP заработать репутацию в этой области.

Flashpoint сообщает, что RAMP достигла своей третьей итерации с использованием нового домена.onion и требует от всех бывших пользователей перерегистрации». ***(Bill Toulas. Russian ransomware gangs start collaborating with Chinese hackers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/russian-ransomware-gangs-start-collaborating-with-chinese-hackers/). 17.11.2021).***

***

«Группа высококвалифицированных хакеров, специализирующихся на корпоративном шпионаже, возобновила свою деятельность, и одной из их жертв в этом году стала крупная оптовая компания в России.

Отмеченная как RedCurl, группа дважды в этом году атаковала российский бизнес, каждый раз используя тщательно сконструированные целевые фишинговые электронные письма с вредоносным ПО на начальной стадии.

Увеличение количества жертв

RedCurl, действующий с 2018 года, несет ответственность за не менее 30 атак на предприятия в России (18 из них), Украине, Канаде, Норвегии, Великобритании и Германии, последние четыре из которых произошли в этом году.

Хакеры умеют оставаться незамеченными в течение длительного времени, от двух до шести месяцев, прежде чем украсть корпоративные данные (записи о персонале, документы о юридических лицах, судебные записи, внутренние файлы, историю электронной почты).

Дважды ударил по одной и той же компании

Исследователи из компании по кибербезопасности Group-IB заметили семимесячный перерыв в активности RedCurl, который хакеры использовали для внесения значительных улучшений в свой набор настраиваемых инструментов и методов атаки.

Среди последних жертв хакера - одна из крупнейших в России оптовых компаний, которая поставляет сетевым магазинам и другим оптовикам товары для дома, офиса и отдыха.

По неизвестным причинам RedCurl дважды атаковал эту компанию, получая первоначальный доступ через электронные письма, выдававшие себя за отдел кадров компании с объявлением бонусов и портал государственных услуг.

В обоих случаях целью было развернуть на компьютере сотрудника загрузчик вредоносного ПО (RedCurl.InitialDropper), скрытый во вложенном документе, который мог запустить следующий этап атаки.

В ходе расследования Group-IB обнаружила, что RedCurl увеличил цепочку атаки до пяти этапов с трех или четырех этапов, которые наблюдались ранее.

Хакеры старались не вызывать подозрений, когда получатель открывал вредоносный документ, который запускал начальный дроппер, поэтому они включили хорошо созданный файл-приманку с содержимым, связанным с организацией.

Дроппер получал инструмент RedCurl.Downloader, который собирал информацию о зараженной машине и доставлял ее на управляющий сервер (C2), а также инициировал следующий этап атаки.

Обновленный набор инструментов

Group-IB обнаружила, что хакеры теперь использовали RedCurl.Extractor, модифицированную версию RedCurl.Dropper, которую они обнаружили в предыдущих атаках этого злоумышленника.

Целью этого инструмента была только подготовка к заключительному этапу атаки, который заключался в достижении устойчивости системы.

Исследователи отмечают, что RedCurl перешел от типичного использования пакетных сценариев и сценариев PowerShell к исполняемым файлам и что антивирусное программное обеспечение не смогло обнаружить первоначальное заражение или злоумышленника, перемещающегося по сети жертвы.

Однако улучшения в наборе инструментов RedCurl, похоже, были поспешными, поскольку Group-IB обнаружила логическую ошибку в одной из команд. Одно из объяснений состоит в том, что у группы было мало времени, чтобы начать атаку, и она не могла должным образом протестировать свои инструменты.

Group-IB опубликовала сегодня отчет с индикаторами взлома и технической информацией об обновленном наборе инструментов RedCurl и их функциональности:

RedCurl.InitialDropper: файл LNK, используемый на начальном этапе заражения, загружает пакетные сценарии или сценарии PowerShell с C2, которые получают вредоносное ПО для следующего этапа.

RedCurl.Downloader (новый инструмент): загрузчик промежуточного этапа, который собирает данные о зараженной системе, загружает и развертывает вредоносное ПО для следующего этапа

RedCurl.Extractor: DLL-файл, эквивалентный RedCurl.Dropper, извлекает законную утилиту 7-Zip, загружает и устанавливает вредоносное ПО следующего уровня.

RedCurl.FSABIN: двоичный эквивалент старого RedCurl.FirstStageAgent, получает команды от HTTP-серверов, контролируемых хакерами.

RedCurl.CHABIN1: форк FSABIN

RedCurl.CHABIN2: аналогично CHABIN1, определяет настройки прокси-сервера для подключения зараженной системы к серверам, контролируемым хакерами.

Несмотря на то, что он не так активен, как в другие годы, RedCurl сохраняет свою изощренность и остается продвинутым субъектом угроз, способным оставаться незамеченным в течение нескольких месяцев.

Group-IB сообщает, что из четырех атак, выявленных в этом году, две были направлены против одной и той же цели. Однако они ожидают, что появится больше жертв, поскольку обновленные инструменты RedCurl обнаруживаются в дикой природе все чаще». ***(Ionut Ilascu. RedCurl corporate espionage hackers resume attacks with updated tools // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/redcurl-corporate-espionage-hackers-resume-attacks-with-updated-tools/). 18.11.2021).***

***

«Новая хакерская группа под названием Moses Staff недавно взяла на себя ответственность за многочисленные атаки на израильские организации, которые выглядят политически мотивированными, поскольку они не требуют выплаты выкупа.

Злоумышленники неоднократно наносили ущерб израильским системам за последние пару месяцев, проникая в сети и шифруя файлы, а затем передавая украденные копии общественности.

Таким образом, очевидный мотив группы состоит в том, чтобы вызвать максимальные сбои в работе и нанести ущерб своим целям путем раскрытия корпоративных секретов и другой конфиденциальной информации через специальные сайты утечки данных, учетные записи Twitter и каналы Telegram.

Общедоступная информация

Исследователи Check Point опубликовали сегодня подробный отчет о Moses Staff, в котором изучаются методы, цепочка заражения и набор инструментов, используемых актером.

Moses Staff, похоже, использует общедоступные эксплойты для известных уязвимостей, которые не исправлены в общедоступной инфраструктуре.

Например, хакерская группа нацелена на уязвимые серверы Microsoft Exchange, которые эксплуатируются уже несколько месяцев, но многие развертывания остаются без исправлений.

После успешного проникновения в систему злоумышленники будут перемещаться по сети в боковом направлении с помощью PsExec, WMIC и Powershell, поэтому специальные бэкдоры не используются.

В конечном итоге участники используют специальную вредоносную программу PyDCrypt, которая использует DiskCryptor, инструмент шифрования дисков с открытым исходным кодом, доступный на GitHub, для шифрования устройств.

Слабая схема шифрования

CheckPoint объясняет, что зашифрованные файлы можно восстановить при определенных обстоятельствах, поскольку схема шифрования использует генерацию симметричного ключа при шифровании устройств.

PyDCrypt генерирует уникальные ключи для каждого имени хоста на основе хэша MD5 и созданной соли. Если копия PyDCrypt, используемая в атаке, извлекается и отменяется, функция хеширования может быть получена.

Это возможно во многих случаях, когда самоудаление вымогателя не сработало или было отключено в конфигурации.

В общем, Moses Staff не прилагает особых усилий к этому аспекту своей работы, поскольку главное, к чему они стремятся, - это вызвать хаос в целевой израильской операции, а не гарантировать, что зашифрованные диски невозможно восстановить.

Политическая мотивация

Несмотря на то, что актер является новым по имени, у него могут быть ссылки на Pay2Key или BlackShadow, у которых такая же политическая мотивация и сфера охвата таргетинга.

«В сентябре 2021 года хакерская группа Moses Staff начала атаковать израильские организации, присоединившись к волне атак, начатых около года назад группами атак Pay2Key и BlackShadow », - поясняют исследователи в своем отчете.

«Эти субъекты действовали в основном по политическим мотивам, пытаясь создать шум в СМИ и нанести ущерб имиджу страны, требуя денег и проводя длительные и публичные переговоры с жертвами».

Группа активно присутствует в социальных сетях, на сайте утечки данных Tor и в канале Telegram, и все они используются для публикации украденных данных по как можно большему количеству каналов, чтобы максимизировать ущерб.

До сих пор аналитикам не удалось связать Moses Staff с каким-либо конкретным географическим положением или принадлежностью ли они к группе, спонсируемой государством.

Однако один из образцов вредоносного ПО, использованных в атаках Moses Staff, был загружен на VirusTotal из Палестины за несколько месяцев до начала атак.

«Хотя это не является убедительным признаком, это может выдать происхождение злоумышленников; иногда они тестируют инструменты в государственных службах, таких как VT, чтобы убедиться, что они достаточно скрытны», - объясняет Check Point.

Поскольку в атаках Moses Staff используются старые уязвимости, для которых есть доступные исправления, Check Point рекомендует всем израильским организациям исправлять свое программное обеспечение, чтобы предотвратить атаки». ***(Bill Toulas. Moses Staff hackers wreak havoc on Israeli orgs with ransomless encryptions // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/moses-staff-hackers-wreak-havoc-on-israeli-orgs-with-ransomless-encryptions/). 15.11.2021).

***

«Компания Facebook сообщила, что помешала работе одной пакистанской и трех сирийских хакерских групп. Пакистанская хак-группа использовала аккаунты Facebook для атак на членов бывшего афганского правительства, вооруженных сил и правоохранительных органов.

Исследователи рассказывают, что пакистанская хак-группа SideCopy создала поддельный магазин приложений для Android, чтобы атаковать лиц, связанных с бывшим правительством Афганистана (еще до его падения и прихода к власти запрещенной в РФ организации «Талибан»). Эти атаки длились с апреля по август текущего года.

Операторы SideCopy создавали в Facebook поддельные профили, обычно выдавая себя за молодых женщин, знакомились с целями и обманом вынуждали их переходить по вредоносным ссылкам. Такие ссылки вели на фишинговые сайты, которые собирали учетные данные, или, в некоторых случаях, в фиктивные магазины приложений, где размещались зараженные малварью приложения для Android. Обычно хакеры использовали приложения, замаскированные под мессенджеры и имитировали известные бренды, такие как Viber и Signal.

«Среди них были приложения HappyChat, HangOn, ChatOut, TrendBanter, SmartSnap и TeleChat. Некоторые из них на самом деле являются действующими мессенджерами», — рассказывают эксперты.

На самом деле такие фейки были заражены троянами удаленного доступа. Так, некоторые приложения содержали малварь PJobRAT, тогда как другие были заражены ранее неизвестной угрозой под названием Mayhem. Оба вредоноса позволяли хакерам полностью контролировать зараженные устройства.

Кроме того, аналитики Facebook сообщили, что еще в октябре 2021 года они помешали работе трех сирийских хак-групп. Эти злоумышленники атаковали лиц и активистов, противостоящих режиму Башара Асада.

Syrian Electronic Army (Сирийская электронная армия): преследовала правозащитников, журналистов и других лиц противостоящие правящему режиму.

APT-C-37: была нацелена на людей, связанных со Свободной сирийской армией, и бывших военнослужащих, которые присоединились к силам оппозиции.

Неназванная группировка: атаковала группы меньшинств, активистов, оппозицию, курдских журналистов, членов отрядов народной защиты, а также членов Гражданской обороны Сирии или «Белых касок» (добровольческой гуманитарной организации).

Facebook заявляет, что деятельность первых двух групп связана с двумя подразделениями Воздушных разведывательных сил Сирии, одной из самых влиятельных спецслужб страны». ***(Мария Нефёдова. Пакистанские хакеры создали фейковый магазин приложений для своих атак // xakep (https://xakep.ru/2021/11/17/facebook-sidecopy/). 17.11.2021).***

***

«Компанія Microsoft опублікувала звіт про атаки хакерів протягом 2020-2021 років. Деякі цифри дивують: майже 20% усіх кібератак у світі спрямовані проти України. Найчастіше нападам піддавалися лише США…

Аналіз кіберситуації, проведений Microsoft, засвідчив, що найбільшою загрозою є Росія. За даними звіту, 58% усіх атак хакерів, виявлених компанією, вчинені російськими угрупованнями.

На другому місці за такою активністю – КНДР (23%). Далі йдуть Іран (11%) та Китай (8%). Південна Корея, Туреччина і В'єтнам також виявляли активність, але їхні атаки «крапля в морі» – 1%.

Хакери з Росії, Ірану, Китаю та Північної Кореї найчастіше атакували американські організації – 46% кібернападів за звітний період.

19% кібератак було скоєно проти України. Для порівняння, частка Бельгії, Німеччини та Японії не перевищує 3%.

У звіті Microsoft згадує три російські хакерські угруповання – Bromine, Nobelium та Strontium. Хакери з Nobelium найчастіше здійснювали зломи у сфері державного управління, дипломатії та оборони. Ще одне активне хакерське угруповання – Thallium, яке базується в КНДР.

Росія, на думку Microsoft, за рік наростила кількість кібернападів, а також збільшила їхню ефективність – з 21% до 32%. При цьому російські хакери почали частіше зламувати урядові організації: кількість таких злочинів збільшилася з 3% до 53%.

Державний сектор взагалі зараз стає найбажанішою метою хакерів – 48% атак. На другому місці неурядові організації та аналітичні центри – 31%. Освіта – 3% атак, IT, медіа, енергетика та охорона здоров'я – по 1%...» ***(Хакерські атаки: які країни найчастіше зазнають нападів і чим це небезпечно // «Слово і Діло» (https://www.slovoidilo.ua/2021/11/08/video/suspilstvo/xakerski-ataky-yaki-krayiny-najchastishe-zaznayut-napadiv-chym-ce-nebezpechno). 08.11.2021).***

***

«По словам исследователей, связанная с Северной Кореей группа повышенной постоянной угрозы TA406, известная как Kimsuky или Thallium, в 2021 году активизировала свои операции по кибершпионажу, нацеленные на дипломатов и экспертов по политике в Азии, Великобритании и США.

В начале года группа угроз начала еженедельные кампании, посвященные темам, которые включали безопасность ядерного оружия, президента США Джо Байдена и корейскую внешнюю политику, говорят исследователи из охранной фирмы Proofpoint.

Группа также «пыталась собрать учетные данные, такие как логины Microsoft или другие корпоративные учетные данные, от целевых лиц. В некоторых случаях электронные письма были безобидными по своему характеру, [но] эти сообщения могли быть попытками злоумышленников взаимодействовать с жертвами. перед отправкой им вредоносной ссылки или вложения», - отмечают исследователи.

По словам исследователей, группа TA406 также участвовала в частых кампаниях по краже учетных данных, направленных против исследований, образования, СМИ, финансов и некоммерческих организаций. Они добавляют, что

последнее дополнение к этому списку - это «отдельные лица и организации, связанные с криптовалютой с целью получения финансовой выгоды».

История и черты характера

Исследователи Proofpoint говорят, что они считают «TA406 одним из нескольких участников деятельности, публично отслеживаемой как Kimsuky, Thallium и Konni Group». Хотя APT-группа TA406 действует по крайней мере с 2012 года, хакеры Kimsuky стали предметом совместного предупреждения, выпущенного ФБР и Агентством кибербезопасности и безопасности инфраструктуры США в октябре 2020 года из-за постепенного роста активности (см.: Оценка деятельности северокорейской Kimsuky APT Group).

Предупреждение вызвало предположения о том, что субъект угрозы связан с Корейской Народно-Демократической Республикой и является спонсируемой государством организацией. Но в отчете Proofpoint говорится, что у него есть «большая уверенность в том, что TA406 действует от имени правительства Северной Кореи». Он также связал Kimsuky с двумя другими APT - TA408 и TA427, которые, похоже, работают в тандеме, а также имеют много векторов атак и инфраструктуры, согласно Proofpoint.

Исследователи говорят, что TA406 использовал целевые фишинговые кампании в 2021 году для доставки как ссылок для сбора учетных данных, так и вредоносных программ, таких как Konni, Sanny, Carrotbat / Carrotball, Babyshark, Amadey и Android Moez.

TA406 использует различные платформы обмена сообщениями для проведения целевых фишинговых кампаний, в том числе собственную инфраструктуру на основе серверов PHP, таких как PHPMailer и Star, и использует крупных поставщиков услуг, таких как GMail или Яндекс, а также украденные или синтетические идентичности, чтобы обмануть целевых людей, говорят исследователи.

Исследователи говорят, что в то время как многие группы APT запускают целевые фишинговые атаки с использованием вредоносных вложений или поддельных страниц входа, TA406 идет на шаг впереди и создает поддельные учетные записи LinkedIn.

Одна из таких учетных записей LinkedIn, раскрытая исследователями, предназначена для «Томаса Джими», который, как указано в учетной записи, является исследователем из Стэнфордского университета. Исследователи Proofpoint не обнаружили физического существования человека с таким именем и титулом.

Другие вредоносные инструменты

В ноябре 2020 года исследователи из компании Cybereason, занимающейся кибербезопасностью, обнаружили новый набор вредоносных инструментов, связанных с группой Kimsuky…

Инструменты, связанные с Kimsuky, включали модульный пакет шпионского ПО под названием «KGH_SPY», загрузчик вредоносных программ, получивший название «CSPY Downloader», а также дополнительную инфраструктуру, которая частично совпадала с предыдущей кампанией, нацеленной на аналитический центр США в 2018 году, согласно отчету Cybereason.

В июне исследователи из Malwarebytes раскрыли еще один набор тактик, приемов и процедур, используемых Kimsuky, который в то время использовал бэкдор AppleSeed для выполнения своих шпионских операций…» ***(Mihir Bagwe. North Korean APT Group Steps Up Espionage Ops in 2021 // Information Security Media Group, Corp. (https://www.govinfosecurity.com/north-korean-apt-group-steps-up-espionage-ops-in-2021-a-17957). 19.11.2021).***

***

«…Российская киберкриминальная группировка FIN7 создала фальшивую фирму по информационной безопасности в надежде нанять профессионалов, чтобы использовать их втемную для проведения кибератак.

Эксперты группы Gemini Advisory обнаружили некую подозрительную компанию под названием Bastion Secure, чей сайт целиком состоял из украденного и перекомпонованного контента других веб-ресурсов. В информационном разделе утверждалось, что компания базируется в Англии, однако сервер, на котором располагается сайт, выдавал сообщения об ошибках 404 (несуществующие разделы) на русском языке.

Кроме того, в информационном разделе содержалось утверждение, что Bastion является дочерним предприятием реально существующей фирмы по кибербезопасности Convergent Network Solutions. Пока неизвестно, в курсе ли Convergent о появлении у них такого «дочернего предприятия».

В разделе вакансий Bastion (или FIN7) предлагались позиции программистов на C/C++, PHP и Python, системных администраторов Windows и специалистов по обратной разработке. Обещанная зарплата составляла от $800 до $1200 в месяц.

Неназванный эксперт, проинформировавший Gemini об этих вакансиях, сообщил, что отправил в Bastion свое резюме и был принят на работу. Ему даже открыли доступ к внутреннему инструментарию Bastion. На поверку оказалось, что это широко известные специалистам по ИБ средства пост-эксплуатации (развития атаки после изначальной компрометации системы) Carbanak и Lizar/Tirion. Различные группы исследователей уже неоднократно ассоциировали Carbanak и Lizar/Tirion с деятельностью группировки FIN7.

Нанятым работникам их представляли как «менеджер команд». Судя по скриншоту, который приводится в блоге Gemini Advisory, интерфейс этой панели управления весь на русском языке.

Реальные атаки под видом пентеста

Работнику предоставлялся доступ к внутренним ресурсам сторонней компании (якобы клиента, заказавшего услуги пентестеров), после чего предлагалось собрать информацию об аккаунтах с административными полномочиями, резервных копиях и пр., то есть, обо всем, что интересует операторов будущей атаки с помощью шифровальщиков.

Источник Gemini запросил юридическую документацию на пентест, но ничего не получил, из чего сделал окончательный вывод о криминальной природе своего нанимателя.

Как указывается в публикации Gemini, помимо собственного сайта, Bastion/FIN7 опубликовали вакансии на множестве легитимных сайтов по поиску

работы в России и на Украине (например, Superjob.ru и Rabota.ua). На сайте Zoon.ru даже было размещено целое досье с указанием физического адреса: Пресненская набережная, 12. Это башня «Федерация». Между тем, на сайте Bastion Secure говорится, что московский офис компании якобы располагается в башне «Империя» (Пресненская набережная, 6, стр. 2), хотя адрес указан тот же.

В сервисе «Яндекс.карты» фирма Bastion Secure по указанным адресам не значится.

«Хотя нет ничего нового в попытках киберпреступных групп нанимать людей на легитимных сайтах по поиску работы, размах и наглость, с которыми действует FIN7, явственно превосходит поведение других киберкриминальных группировок... Решение нанимать работников для использования втемную вместо поиска подельников в даркнете, по-видимому, связано с банальной жадностью. С теми, кто сотрудничает сознательно, FIN7 пришлось бы делиться процентом от сумм выкупа, которые могут составлять миллионы долларов, в то время как ничего не подозревающие наемные работники готовы были бы трудиться за ежемесячную зарплату в районе тысячи долларов. Это примерный размер зарплат на рынках постсоветских стран», — говорится в публикации Gemini.

К настоящему моменту Google Chrome маркирует сайт Bastion Secure как вредоносный.

«Характерно, что группировка пытается нанимать в первую очередь именно программистов и системных администраторов, а не экспертов по информационной безопасности, — говорит Данила Каревский, эксперт по информационной безопасности компании SEQ. — Специалист мог бы опознать, и в описываемом случае действительно опознал, инструментарий FIN7, даже и слегка замаскированный. Кроме того, услуги тестирования на проникновение всегда оказываются с большим количеством юридически заверенных условий, с которыми должны знакомиться и непосредственные исполнители. Если работодатель не предоставляет документы, это признак криминала». ***(Роман Георгиев. Хакеры втемную используют российских программистов для атак на бизнес // CNews (https://www.cnews.ru/news/top/2021-10-26_hakery_vtemnuyu_ispolzuyut). 16.11.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Emotet, который когда-то описывался как «самое опасное вредоносное ПО в мире» до того, как был устранен крупной международной полицейской операцией, по-видимому, вернулся - и устанавливается на системы Windows, зараженные вредоносным ПО TrickBot.

Вредоносная программа Emotet снабжала свои контроллеры лазейкой в скомпрометированные машины, которую можно было сдавать в аренду другим группам, включая банды вымогателей, для использования в своих собственных кампаниях. Emotet также использовал зараженные системы для рассылки

автоматических фишинговых писем, чтобы увеличить размер ботнета - до того, как он был удален в январе этого года.

Демонтаж ботнета стал одним из самых серьезных сбоев в киберпреступных операциях за последние годы, поскольку правоохранительные органы всего мира, включая Европол и ФБР, работали вместе, чтобы получить контроль над сотнями серверов Emotet, которые контролировали миллионы компьютеров, зараженных вирусом. вредоносное ПО. Специально созданное обновление Killswitch, созданное следователями, в апреле эффективно удалило ботнет с зараженных компьютеров.

Но теперь исследователи из ряда компаний, занимающихся кибербезопасностью, предупредили, что Emotet вернулся. Другой вредоносный ботнет, TrickBot, который стал излюбленным местом многих киберпреступников после январской атаки, используется для установки Emotet на зараженные системы Windows.

«На нескольких наших трекерах Trickbot мы наблюдали, что бот пытался загрузить DLL в систему. Согласно внутренней обработке, эти DLL были идентифицированы как Emotet. Однако, поскольку ботнет был отключен в начале этого года, мы с подозрением относились к», - написал в своем блоге Лука Эбах, исследователь безопасности немецкой компании по кибербезопасности G Data.

«В настоящее время мы уверены, что образцы действительно кажутся реинкарнацией печально известного Emotet», - добавил он.

Исследователи кибербезопасности из AdvIntel, Crypolaemus и других также подтвердили, что это действительно похоже на возвращение Emotet, который, похоже, использует другую технику шифрования, чем та, которая была замечена ранее.

В настоящее время Emotet не пытается распространяться, вместо этого полагаясь на TrickBot для распространения новых инфекций, но это указывает на то, что те, кто стоит за Emotet, пытаются снова запустить ботнет.

«Взаимоотношения между этим новым вариантом и старым Emotet демонстрируют совпадение кода и пересечения технологий», - сказал Джеймс Шэнк, главный архитектор общественных служб и старший евангелист по безопасности в Team Cymru, компании по кибербезопасности, которая была среди тех, кто помог разрушить Emotet в январе. ZDNet по электронной почте.

«Потребуется некоторое время, чтобы увидеть, как Emotet перестраивается и сможет ли он снова стать «самым опасным вредоносным ПО в мире». Вы можете быть уверены, что те, кто помог устранить его с первого раза, внимательно следят за ним. Этого не происходит. как сюрприз, что снова появился Emotet. На самом деле, многие могут задаться вопросом, почему это заняло так много времени», - добавил он.

Исследователи кибербезопасности предоставили список серверов управления и контроля, которые сетевые администраторы могут блокировать, чтобы предотвратить заражение Emotet.

Чтобы защитить системы от попадания в жертву Emotet, Trickbot и других загрузчиков вредоносных программ, рекомендуется применять исправления безопасности при их выпуске, чтобы предотвратить использование киберпреступниками известных уязвимостей, и чтобы пользователи были

осведомлены об опасностях фишинговых писем. ***(Danny Palmer. Emotet, once the world's most dangerous malware, is back // ZDNet (https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/). 16.11.2021).***

***

«Согласно отчету Sophos об угрозах за 2022 год, в будущем заражение вредоносными программами и программами-вымогателями будет состоять из «дробовых атак с точным нацеливанием».

Как будто этого было недостаточно, британский информационный бизнес считает, что известные атаки массового вредоносного ПО в конечном итоге приведут к появлению еще большего количества программ-вымогателей, в то время как тактика вымогательства, используемая бандами вымогателей, станет более разнообразной и интенсивной - с целью запугивания жертв для передачи денег.

«Программы-вымогатели процветают благодаря своей способности адаптироваться и вводить новшества», - сказал Честер Вишневски, главный научный сотрудник Sophos, в стандартном заявлении. «Например, хотя предложения RaaS не новы, в предыдущие годы их основной вклад заключался в том, чтобы сделать программы-вымогатели доступными для злоумышленников с низкой квалификацией или с меньшим финансированием».

В последнее время почти повсеместная киберугроза широко освещалась в новостях после того, как США получили миллионы долларов за информацию, которая привела к арестам и осуждению некоторых известных банд программ-вымогателей. Вдобавок ко всему, полиция многих стран, в первую очередь Украины, арестовывала людей, предположительно являющихся членами банд.

Помимо программ-вымогателей, Sophos заявила, что в 2022 году будут повторены атаки ProxyLogon и ProxyShell, при которых на уязвимости в широко используемых ИТ-сервисах и продуктах мгновенно нападут преступники и государства. Фирма ожидает увидеть «рост [криминального] интереса к системам на базе Linux в течение 2022 года, как в облаке, так и на веб-серверах и виртуальных серверах».

Прицельные атаки из дробовика, как их описал Sophos, также могут увеличиваться. Компания использовала атаки Gootloader в качестве примера, подчеркнув, как злоумышленники повышали рейтинг вредоносных веб-сайтов в результатах поиска Google. Фильтрация отметок, которые переходили по этим вредоносным ссылкам, исключала тех, кто не использовал определенные комбинации операционных систем и браузеров.

«SophosLabs считает, что это может представлять собой новый способ для распространителей вредоносных программ помешать исследователям вредоносных программ, в то же время давая себе большую степень уверенности в том, что их вредоносное ПО попадет к подмножеству жертв, которое может быть более желанным, чем население в целом», - заключили в компании.

Сами по себе методы антианализа не являются чем-то новым: в сентябре Касперский подчеркнул, что шпионское ПО FinFisher включало в себя несколько методов, призванных помешать исследователям, исследующим работу вредоносного

ПО. Sophos, однако, указала, что в некоторых кампаниях по рассылке спама, которые она наблюдала, единственной приманкой был номер телефона; Затем телефонные операторы-люди «проводят своего рода психологическое профилирование звонящего, чтобы определить, могут ли они стать настоящей жертвой».

По мнению Sophos, Linux и виртуализированные системы также могут столкнуться с большей угрозой в 2022 году с твердым предупреждением: «Одна программа-вымогатель, с которой мы столкнулись в 2021 году, была нацелена на платформу VMware ESXi и представляла собой сценарий Python, который при запуске на гипервизор, выключает все работающие виртуальные машины, а затем шифрует хранилище данных, в котором виртуальные жесткие диски и другие файлы конфигурации хранятся на гипервизоре ".

Неприятные вещи - и вышеупомянутый инцидент произошел с компанией «логистики и судоходства» в этом году. RansomEXX троян, который нацелен на VMware ESXi гипервизор, был замечен Sophos в июне 2021 года после атаки против другого ESXi гипервизора «управляет крупной коммерческой пекарней».

Угрозы развиваются. Старое убеждение в том, что ваша организация слишком мала, неясна или с низким доходом, чтобы ее можно было атаковать, в наши дни опасно - так что держите оборону на высоком уровне». ***(Gareth Corfield. Shotgun targeting of malware attacks will be the defining infosec theme of 2022, reckons Sophos // The Register (https://www.theregister.com/2021/11/09/sophos_infosec_predictions_2022_linux_targeting/). 09.11.2021).***

***

«Исследователи кибербезопасности поделились информацией о новом вредоносном ПО, которое использует более тридцати эксплойтов и потенциально может связать миллионы маршрутизаторов, модемов, сетевых хранилищ (NAS) и устройств Интернета вещей (IoT) в ботнет.

Обнаруженное лабораторией Alien Labs компании AT&T, новое вредоносное ПО, получившее название BotenaGo, написано на языке программирования Go с открытым исходным кодом, который в последнее время стал популярным среди авторов вредоносных программ благодаря его способности кодировать полезные нагрузки, которые труднее обнаружить и проанализировать. в BleepingComputer.

Это также очевидно в отношении BotenaGo, который отмечен только шестью из 62 антивирусных движков на VirusTotal, причем некоторые ошибочно идентифицируют его как ботнет Mirai.

«Авторы вредоносных программ продолжают создавать новые методы написания вредоносных программ и расширения их возможностей. В этом случае [BotenaGo] может работать как ботнет на разных платформах ОС с небольшими изменениями», - пишет Офер Каспи, исследователь безопасности из Alien Labs.

Необычный ботнет

По словам исследователей, вредоносная программа создает бэкдор и ждет либо получения цели для атаки от удаленного оператора, либо от другого связанного модуля, работающего на той же машине.

Удивительно, но BotenaGo, похоже, не имеет активной связи со своим сервером управления и контроля (C2), что сбивает исследователей с толку относительно его работы.

У исследователей есть несколько теорий, одна из которых заключается в том, что вредоносное ПО все еще находится в стадии разработки и было выпущено в свет случайно. Другая теория заключается в том, что вредоносная программа может быть частью «набора вредоносных программ», и в этом случае будет другой модуль, который будет взаимодействовать с сервером C2.

В любом случае исследователи предлагают администраторам всегда следить за исходящим сетевым трафиком, чтобы следить за необоснованным использованием полосы пропускания». ***(Mayank Sharma. A new botnet is launching attacks on millions of routers and IoT devices // Future US, Inc. (https://www.techradar.com/news/a-new-botnet-is-launching-attacks-on-millions-of-routers-and-iot-devices). 13.11.2021).***

***

«Исследователи Google подробно описали широко распространенную атаку, в ходе которой на устройствах Apple был установлен бэкдор, который посещал гонконгские СМИ и продемократические сайты.

По крайней мере, с конца августа злоумышленники использовали уязвимости в macOS и iOS, в том числе в «дикой природе» то, что тогда считалось недостатком нулевого дня, для установки бэкдора на устройства Apple пользователей, посетивших СМИ в Гонконге. и продемократические сайты.

Это кампания не с точным таргетингом, но очень сложная. Согласно отчету, опубликованному в четверг Группой анализа угроз Google (TAG), в результате этой атаки вредоносное ПО было без разбора внедрено на любое устройство iOS или macOS, которое, к сожалению, наткнулось на зараженные сайты.

Другими словами, по данным TAG, злоумышленники внедрили вредоносное ПО на легитимные веб-сайты «СМИ и известной продемократической профсоюзной и политической группы» в Гонконге.

Согласно отчету TAG, на устройства жертв было нанесено то, что тогда было нулевым днем, плюс еще один эксплойт, который использовал ранее исправленную уязвимость для macOS, которая использовалась для установки бэкдора на их компьютеры.

Скорее всего, работа поддерживаемых государством злоумышленников

TAG обычно не спекулирует на атрибуции, и, во всяком случае, заявляет, что в данном случае у нее нет достаточных доказательств, чтобы окончательно установить личность злоумышленника.

Но, судя по тому, что команда могла видеть, они полагают, что нападавшие, вероятно, поддерживаются государством.

«Основываясь на наших выводах, мы полагаем, что этим злоумышленником является группа с хорошо обеспеченными ресурсами, вероятно, поддерживаемая государством, с доступом к собственной команде разработчиков программного обеспечения в зависимости от качества кода полезной нагрузки», - написал Эри

Эрнандес, исследователь Google, обнаруживший кампания. «Полезная нагрузка, похоже, является продуктом обширной разработки программного обеспечения».

Эрнандес также был одним из исследователей TAG, которым приписывают первоначальное обнаружение использовавшегося нулевого дня: CVE-2021-30869, проблему путаницы типов, которую Apple исправила в сентябре с помощью «улучшенной обработки состояния», согласно ее рекомендациям в то время. В сентябрьском сообщении также отмечалось, что Apple знала о дикой природе уязвимостей.

Уязвимость была серьезной: она позволяет вредоносному приложению выполнять произвольный код с привилегиями ядра в macOS Catalina. Полезная нагрузка, по-видимому, была настроена также для атаки на macOS Mojave (10.14), сначала выполняя проверку, чтобы увидеть, какая версия ОС использовалась, прежде чем запускать эксплойты. Однако TAG сказал, что когда они посетили сфальсифицированный сайт с использованием Mojave, они увидели только остатки эксплойта. Они получили полный Монти - всю незашифрованную цепочку эксплойтов - при просмотре сайта с помощью Catalina.

В случае кампании, ориентированной на Гонконг, эксплойт привел к установке бэкдора, который имеет впечатляющий список возможностей наблюдения, включая сбор отпечатков пальцев с устройств жертв, снимки экрана, загрузку / выгрузку файлов, выполнение команд терминала., аудиозаписи и кейлоггеров.

Ссылки на Китай

Известно, что сторонники угроз, поддерживаемые Китаем, используют нулевые дни для создания тщательно продуманных, обширных, нецелевых атак с целью уничтожения широких слоев населения, включая кампании, направленные против мусульманского меньшинства страны - уйгуров в Синьцзяне.

Google Project Zero выявил одну такую кампанию в 2019 году после обнаружения небольшой коллекции взломанных веб-сайтов. Кампания, продолжавшаяся более двух лет, аналогичным образом использовала уязвимости - две из них - нулевые дни, включая нулевой день iPhone, - в цепочке атак, которая опиралась в общей сложности на 14 недостатков, - в неизбирательных атаках на водопой на посетители сайта.

Кроме того, в мае MIT Technology Review сообщило, что актеры, работающие на китайскую разведку, использовали уязвимость, представленную в 2017 году на хакерском соревновании Tianfu Cup, для нацеливания на уйгуров.

Другая ссылка на Китай исходит из кода, который содержит строки, написанные на китайском языке, согласно тому, что исследователь продуктов Apple Патрик Уордл сказал Материнской плате после проверки кода эксплойта. Кроме того, сервер управления и контроля, к которому он подключался, находился в Гонконге.

Полезные данные эксплойта macOS

Однако веб-сайты были скомпрометированы, и в результате они обслужили два фрейма для цепочек эксплойтов iOS и macOS, которые обслуживали эксплойты с сервера, контролируемого злоумышленником. Исследователи TAG смогли получить только MacOS.

Цепочка эксплойтов для macOS объединила слабость удаленного выполнения кода (RCE) в WebKit и нулевой день, CVE-2021-30869.

Эрнандес объяснил, что эксплойт напоминает другую уязвимость в естественных условиях, ранее проанализированную Иэном Биром из Project Zero. И оказалось, что точно такой же эксплойт был представлен исследовательской группой в области кибербезопасности Pangu Lab в ходе публичного выступления на конференции zer0con21 в Китае в апреле, сообщил Motherboard глава TAG Шейн Хантли. Эрнандес написал, что он также был представлен на конференции Mobile Security Conference (MOSEC) в июле, другими словами, всего за несколько месяцев до того, как он был использован против жителей Гонконга.

В полезной нагрузке macOS было несколько компонентов, которые, по-видимому, были настроены как модули, объяснил Эрнандес, включая модуль ядра для захвата нажатий клавиш, а также другие функции, к которым двоичные файлы не имели прямого доступа, но которые могли быть загружены на машины жертв на более поздних этапах. цепочки атак.

Пегасоподобное использование нулевых дней для наблюдения

Предположение TAG о том, что эта кампания, похоже, исходит от поддерживаемого государством злоумышленника, имеет исторический приоритет, учитывая изощренное использование нулевого дня в кампаниях слежки, проводимых национальными государствами. На ум приходят кампании с использованием инструмента наблюдения военного уровня NSO Group - Pegasus. И атаки на водные ресурсы в Гонконге, и инструменты NSO Group полагаются на использование нулевых дней до того, как продавцы или общественность что-либо узнают о них.

Например, в августе служба по надзору за кибербезопасностью Citizen Lab увидела, что новый эксплойт нулевого дня FORCEDENTRY был успешно развернут против iPhone бахрейнских активистов, в том числе одного, жившего в то время в Лондоне». ***(Lisa Vaas. Mac Zero Day Targets Apple Devices in Hong Kong // Threatpost (https://threatpost.com/mac-zero-day-apple-hong-kong/176300/). 12.11.2021).***

****

«За последние несколько лет, по мере развития экосистемы Android, широко распространенные вредоносные программы с возможностями рутирования стали редкостью. Но его редкость не означает, что он все еще не представляет угрозы.

По определению, рутирование вредоносного ПО чрезвычайно опасно, поскольку оно может получить привилегированный доступ к операционной системе Android. Это позволяет вредоносному ПО предоставлять себе дополнительные разрешения, изменять системные настройки и устанавливать дополнительные вредоносные программы - шаги, которые обычно требуют взаимодействия с пользователем. Вооружившись этими инвазивными средствами контроля, злоумышленники могут затем проводить целевые фишинговые атаки, красть конфиденциальные данные, необходимые для взлома учетных записей пользователей или вести наблюдение.

Недавно Lookout Threat Lab обнаружила первую за пять лет широкомасштабную кампанию по рутированию вредоносных программ. Вредоносное ПО, получившее название AbstractEmu, из-за использования извлечения кода и проверок на защиту от эмуляции во избежание обнаружения было обнаружено в Google Play и других известных сторонних магазинах приложений, таких как Amazon Appstore и Samsung Galaxy Store. Lookout уведомил Google, и приложения были немедленно удалены.

На примере AbstractEmu. Вот вещи, на которые вы должны обратить внимание, чтобы не стать жертвой вредоносного ПО.

Есть множество уязвимостей, которые можно обойти

AbstractEmu - отличный пример того, как злоумышленники могут использовать уязвимости с root-доступом для неизбирательного нацеливания на население в целом. Большинство уязвимостей после обнаружения исправляются с помощью обновлений. Но пользователи защищены только в том случае, если они не торопятся обновлять свои устройства.

В экосистеме Android есть множество уязвимостей, которые можно использовать. Эта кампания нацелена на самые современные уязвимости с 2019 по 2020 годы, включая CVE-2020-0041, уязвимость, ранее не использовавшуюся в реальных условиях. AbstractEmu также нацелился на CVE-2020-0069, уязвимость, обнаруженную в чипах MediaTek, используемых десятками производителей смартфонов. В совокупности этой уязвимости подвержены миллионы устройств.

Вещи не всегда такие, какими кажутся: троянские приложения

Троянизирование приложений связано не только с рутингом вредоносных программ, но и с помощью распространения кампании AbstractEmu. Маскируя свой злой умысел за, казалось бы, безобидными приложениями, злоумышленник может заманить ничего не подозревающих пользователей в загрузку вредоносного ПО.

Исследователи Lookout обнаружили в общей сложности 19 приложений, связанных с вредоносным ПО, семь из которых содержат функции рутирования. Было подтверждено, что одно приложение, обнаруженное в Google Play, было загружено более 10 000 раз. AbstractEmu замаскировался под несколько различных приложений, включая служебные приложения, такие как менеджеры паролей, и системные инструменты, такие как средства запуска приложений или средства сохранения данных.

AbstractEmu не имеет сложной функциональности удаленного эксплойта с нулевым щелчком, используемой в сложных угрозах типа APT, таких как Pegasus. Но эта возможность не нужна, поскольку вредоносная программа будет активирована, когда пользователь откроет троянизированное приложение вскоре после его загрузки.

Редко или нет, всегда используйте передовые методы кибербезопасности

Защита от AbstractEmu выделяет несколько лучших практик кибербезопасности, о которых мы должны помнить, независимо от того, являетесь ли вы ИТ-специалистом или отдельным лицом. С помощью планшетов и смартфонов большинство из нас остается на связи с работой и управляет личными обязанностями, а это означает, что они хранят огромный объем данных. Эти

устройства также очень сложны и обладают бесчисленным множеством функций, которые могут использовать злоумышленники.

Чтобы защитить себя и свою организацию, вы всегда должны обновлять операционную систему своего устройства. Я также рекомендую использовать только официальные магазины приложений, и даже в этом случае проявлять осторожность при загрузке чего-то неизвестного вам». ***(Hank Schless. Rooting Malware Is Back for Mobile. Here's What to Look Out For // Threatpost (https://threatpost.com/rooting-malware-mobile/176376/). 16.11.2021).***

***

«Антивирусная борьба длится почти столько же лет, сколько существуют персональные компьютеры. Никто не хочет вирус на свой компьютер, но знаете ли вы почему? В этой статье разберёмся какие опасности в себе таят компьютерные вирусы, и даже те, о которых вы могли не знать.

Использование вычислительной мощности компьютера

Вирусы не всегда дают сразу о себе знать, явно демонстрируя бурную деятельность. Есть вирусы, которые не делают ничего «плохого», кроме того, что используют аппаратные мощности компьютера в своих целях. Вирус может загружать центральный процессор, видеокарту, оперативную память, жёсткий диск, канал связи Интернет.

Для чего? Сферы применения ограничены лишь фантазией разработчиков такого зловреда. Например, вирус может использовать компьютер для подбора паролей или обсчитывать звёздное пространство во Вселенной.

Правда, в последние годы практически все подобные вирусы – это майнеры, т.е. вирусы, которые используют мощности процессора и видеокарты для добычи криптовалюты. Это направление стало наиболее выгодным, поэтому и стало таким популярным.

Майнер может долго жить в вашем компьютере, и вы не будете даже догадываться о его существовании. Он будет работать, когда вас нет за экраном монитора, или же работать по чуть-чуть, когда вы на месте. Конечно, есть и такие майнеры, которые стараются выжать по максимуму из вашего железа, пока есть такая возможность.

Последствия работы майнера такие:

Компьютер тормозит.

Процессор и видеокарта сильно греются.

Шумят вентиляторы, даже когда компьютер простаивает.

Счётчик накручивает дополнительные киловатты, растёт счёт на оплату коммунальных услуг.

Для защиты от майнеров нужно придерживаться основ компьютерной безопасности: не скачивать программы на сомнительных сайтах, не запускать почтовые вложения, устанавливать последние обновления операционной системы. Но самый большой плюс к защите даст установка антивирусной программы. Даже бесплатный антивирус поднимает уровень защиты компьютера в десятки раз, более подробная информация о бесплатном антивирусе. Главное правило – антивирус должен быть резидентным, т.е. не просто сканер файлов.

Другая разновидность вирусов, использующих ресурсы, это ботнеты. Злоумышленники заражают множество компьютеров по всему миру для выполнения одной общей задачи. Например, проводят массированную DDoS-атаку на сервер жертвы.

Выгода подобного подхода очевидна. Хакерам не требуется арендовать ресурсы, они их получают бесплатно. Каждый заражённый компьютер имеет свой IP-адрес, т.ч. атакуемый сервер не может просто отфильтровать атаку по IP-адресу.

А вот пользователи, чей компьютер заражён ботнетом, могут столкнуться с блокировками интернет-сервисов. Крупные DDoS-атаки фиксируются, и атакующие IP-адреса заносятся в чёрные списки. Возможно, вы уже сталкивались с тем, когда поисковые системы часто просят ввести капчу, чтобы продолжить работу, и вообще, на каждом шагу стали появляться капчи.

Или ваши письма с вашего IP попадают в спам. Ботнет мог заниматься рассылкой спама. Обидно то, что страдают даже те пользователи, которые никогда небыли заражены ботнетом. Просто провайдеры интернета работают так, что сотни пользователей сидят под одним IP-адресом. И если один компьютер был заражён и его IP-попал в чёрный список, то и все остальные пользователи под этим IP будут в этом чёрном списке.

У провайдеров интернета существует отдельная услуга – белый IP-адрес. Можно арендовать постоянный, «личный» IP-адрес. Если же проблема случилась внезапно, то достаточно просто перезагрузить роутер, IP-адрес обычно меняется на другой после каждой перезагрузки роутера.

Вымогание денег

Возможно, вы уже слышали слёзные истории о вирусах-вымогателях. Вирусы вымогатели блокируют работу компьютера и требуют деньги за возможность разблокировки Windows. Эти вирусы также умеют шифровать содержимое жёсткого диска.

Шифровальщик находит документы, таблицы, электронную почту, фотоархив, видео на компьютере жертвы и нещадно шифрует содержимое файлов. А чтобы пользователь ничего не заметил, вирус работает тихо, не мешая работать за компьютером. Когда шифрование закончено, вирус блокирует работу операционной системы Windows и вешает заглушку на весь экран с требованием выкупа ключа расшифровки данных.

Шифрование может происходить по-разному. Одни вирусы старательно шифруют всё содержимое файлов. Другие просто стирают первые байты в начале файлов, т.ч. программы больше не могут распознать тип файла и его становится невозможно открыть. Третьи могут просто заполнить содержимое файлов нулями.

В первом случае, восстановление исходного содержимого возможно только в тех случаях, когда точно известно название вируса-шифровщика или алгоритм шифрования. В сети можно найти утилиты для расшифровки данных после известных шифровщиков.

Во втором случае нужно каждый файл восстанавливать вручную, используя программы для восстановления каждого типа файла в отдельности, например, для документов «.docx», таблиц «.xlsx», фотографий «.jpg» и т. д.

Затёртые нулями файлы никак невозможно восстановить. На такой случай очень полезно иметь бекап данных на внешнем хранилище или в облачном пространстве.

Самое интересное во всей этой истории то, что если вы отправите деньги на указанный кошелёк (обычно требуют в Биткоинах), то никакого ключа взамен не получите, пустая трата времени и средств. Найти злоумышленника также сложно или вообще невозможно, т.к. они пользуются криптовалютами, движение которых практически не отслеживается.

Слежка и личные данные

Любимая работа вирусов – это кража конфиденциальных данных, таких как логины, пароли, данные банковских карт, личные документы и другие файлы.

Вирус сканирует содержимое подключённых дисков и с лёгкостью находит потенциально важные файлы. Очень плохо, если пользователь хранит пароли в обычном текстовом файле или в электронной таблице. Такие пароли мгновенно уходят в руки злоумышленников.

Но на этом вирус не останавливается, активируется режим слежки за клавиатурой, такая разновидность вирусов называется «Кейлоггеры». Вирус записывает все ваши нажатия на клавиатуру, а специальный алгоритм с лёгкостью выделит логины и пароли из всего потока символов.

Поэтому, следуя из всего написанного, нельзя хранить пароли в блокнотах на рабочем столе. Для этого есть специальное ПО – менеджеры паролей. Они хранят логины и пароли в зашифрованном виде и автоматически подставляют их на сайтах так, что их не нужно вводить с клавиатуры или копировать в буфер обмена, за которым вирусы также следят.

Другие вирусы пытаются ворваться в личную жизнь пользователя. Они активируют микрофон и веб-камеру, снимая всё происходящее в комнате. Затем полученные данные могут использоваться для шантажа пользователя или в других личных целях. Для сжатия видеопотока используются высокоэффективные кодеки, такие как AVC, HEVC, а с недавнего времени лучшим кодеком стал LCEVC.

Подстановка кошельков

Очень интересная угроза, о которой вы могли не знать. Вирус поселяется в ОС Windows и никак себя не проявляет. Затем, когда вы будете отправлять кому-то деньги на электронный или криптовалютный кошелёк, то вирус заменит номер кошелька в буфере обмена.

Т.е., это сработает, если вы скопировали в буфер номер кошелька и вставляете его в поле ввода, вирус подменит кошелёк на свой. У меня уже давно выработалась привычка, чтобы проверять первые и последние символы скопированного номера кошелька». ***(Афанасий Веретенников. Опасности компьютерных вирусов, о которых вы, возможно, даже не знаете // Mediasat (https://mediasat.info/2021/11/17/opasnosti-kompyuternyx-virusov/). 17.11.2021).***

***

«Если у вас есть телефон Huawei, скорее всего, вы используете его галерею приложений. Учитывая все вышесказанное, важно отметить, что люди, которые используют эту функцию, почти наверняка заразили свои устройства

новой формой вредоносного ПО. Это новое вредоносное ПО для Android — это троянец, который может быть уже на вашем телефоне, и вы не могли бы об этом знать, потому что это одна из тех вещей, которые потенциально могут выдавать себя за одно из 190 различных приложений.

Dr. Web недавно обнаружил это вредоносное ПО и обнаружил, что это измененная форма хорошо известного вредоносного ПО Cynos. Основная цель этого вредоносного ПО - получить конфиденциальную информацию от пользователей и тому подобное, поэтому для вас чрезвычайно важно избавиться от вредоносного ПО, если оно у вас есть на вашем устройстве.

Одна вещь, которая может заставить многих людей вздохнуть с облегчением, — это тот факт, что доктор Веб сообщил Huawei об этой проблеме, и они быстро отреагировали, чтобы немедленно от нее избавиться. По сути, это означает, что теперь вы можете спокойно пользоваться Галереей приложений, потому что она больше не содержит вредоносных программ, которые могли бы заразить ваше устройство и привести к краже значительной части вашей личной информации.

Однако люди, которым удалось получить вредоносное ПО, по-прежнему оставались на своих телефонах. Вы должны просмотреть свой телефон, чтобы увидеть, есть ли какие-либо приложения, которые вы не знаете, и если это так, вы должны немедленно удалить их. Вредоносной программой было заражено более 9,3 миллиона устройств, поэтому велика вероятность того, что вы тоже заражены, и принятие мер предосторожности поможет минимизировать ущерб, который она может причинить». ***(Zia Muhammad. New Android Malware Infects Over 9 Million Devices, Through 190 Different Apps // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/new-android-malware-infects-over-9.html). 25.11.2021).***

***

«Ботнеты являются одним из ключевых факторов кибератак, используемых для распространения вредоносных программ, программ-вымогателей и других вредоносных программ, а форумы в темной сети теперь предлагают уроки о том, как зарабатывать на них деньги, что со временем может усилить угрозу.

Зараженные компьютеры и устройства в ботнете, контролируемом киберпреступниками, могут использоваться для отправки фишинговых писем или вредоносных программ на еще большее количество устройств. Операторы ботнетов часто сдают в аренду свою коллекцию непреднамеренно контролируемых машин, которых могут быть тысячи, другим киберпреступникам.

Например, вредоносная программа TrickBot связывает машины с ботнетом, обеспечивая злоумышленнику лазейку в них. Этот доступ часто продается киберпреступникам, которые затем могут использовать их для развертывания программ-вымогателей, используя этот доступ для шифрования файлов и требуя значительного выкупа. Многие ботнеты используются для кражи имен пользователей и паролей, в то время как другие берут вычислительную мощность компьютеров, которыми они управляют, и сдают их в аренду для запуска DDoS-атак, чтобы переполнить веб-сайты трафиком и отключить их.

Таким образом, операторы ботнетов могут зарабатывать значительные суммы денег, и теперь есть операторы дарквеба, которые предлагают онлайн-курсы для обучения других использованию ботнетов - и они действуют во многом так же, как их законные коллеги, обучающие кибербезопасности и другим навыкам на онлайн-курсах.

Исследователи кибербезопасности из Recorded Future проанализировали рекламу и активность в ботнет-школах на известном подпольном форуме и обнаружили, что эти курсы пользуются спросом - что может стать потенциальной проблемой для организаций, которые могут стать мишенью для киберпреступников, обучающихся этим навыкам.

«По сути, это похоже на то, как будто ты учишься в колледже», - сказал ZDNet Дэнни Пантон, аналитик по киберпреступности из Recorded Future. "У вас будет директор, и они будут виртуально обучать вас - я не верю, что камеры будут на человеке, - но у них есть доступ к платформе, и их учат понимать, что вам нужно делать, чтобы использовать ботнеты. против потенциальных жертв».

Курсы преподают люди, которые сами управляют крупными ботнетами. Курсы недешевы - они стоят более 1400 долларов - но обещают дать даже начинающим киберпреступникам знания о том, как создавать, поддерживать и монетизировать ботнеты.

«Это действительно диапазон опыта и уровней киберпреступности. У вас могут быть люди, которые являются закаленными мошенниками в киберпреступности, но на самом деле не знакомы с использованием ботнетов», - пояснил Пантон. «Кроме того, есть люди, которые совершенно не знакомы с киберпреступностью в целом, им просто любопытно, и они хотят стать лучше закаленными и повысить свои навыки», - добавил он.

Учитывая природу мира киберпреступности, некоторые могут подозревать, что, если они передадут деньги, чтобы принять участие в курсе, их обманут и ничего не получат взамен. Но это похоже на законную услугу, и курс подлежит проверке, которая предполагает, что школа ботнетов действительно предлагает то, что, по ее словам, делает. Если бы это была афера, это не длилось бы так долго.

У исследователей нет данных, чтобы детализировать, сколько всего подражателей киберпреступников прошли курс, но за время, потраченное на анализ этой деятельности, количество людей, посещающих занятия одновременно, может варьироваться; иногда всего пять человек, иногда целых 100.

Курс охватывает такие темы, как управление ботнетом таким образом, чтобы избежать внимания со стороны правоохранительных органов, потому что, как продемонстрировало удаление Emotet, власти будут жестко пресекать ботнеты, когда смогут.

И исследователи предупреждают, что существование этих курсов, вероятно, приведет к увеличению угрозы ботнетов - хотя насколько сложно определить количественно, не имея возможности отслеживать активность отдельных пользователей.

«Весьма вероятно, что в результате этих курсов больше злоумышленников научатся атакам, ориентированным на бот-сети», - сказал Пантон…». ***(Danny Palmer. Dark web crooks are now teaching courses on how to build botnets // ZDNet***

(https://www.zdnet.com/article/college-for-cyber-criminals-dark-web-crooks-are-teaching-courses-on-how-to-build-botnets/). 18.11.2021).

***

«Эксперты предупреждают, что на рынке появился новый загрузчик JavaScript, который не только распространяет восемь различных троянов удаленного доступа (RAT), клавиатурных шпионов и программ для кражи информации, но также может обойти обнаружение большинством инструментов безопасности.

Исследователи кибербезопасности из HP Wolf Security назвали вредоносную программу RATDispenser, отметив, что, хотя у загрузчиков JavaScript обычно более низкий уровень обнаружения, чем у других загрузчиков, эта конкретная вредоносная программа более опасна, поскольку использует несколько методов, позволяющих избежать обнаружения.

«Особенно беспокоит то, что RATDispenser обнаруживается только около 11% антивирусных систем, что приводит к тому, что это скрытое вредоносное ПО в большинстве случаев успешно развертывается на конечных точках жертв», - отметил Патрик Шлапфер, аналитик вредоносного ПО HP.

Шлапфер добавляет, что RAT и кейлоггеры помогают злоумышленникам получить черный доступ к зараженным компьютерам. Затем субъекты обычно используют доступ для перекачивания учетных данных для учетных записей пользователей и все чаще криптовалютных кошельков, а в некоторых случаях могут даже предлагать доступ операторам программ- вымогателей.

Исследователи отмечают, что цепочка заражения начинается с того, что пользователь получает электронное письмо, содержащее вредоносный запутанный код JavaScript. Когда он запускается, JavaScript записывает файл VBScript, который, в свою очередь, загружает полезную нагрузку вредоносной программы, прежде чем удалить себя.

Дальнейшие исследования показали, что за последние три месяца было выпущено как минимум три различных варианта RATDispenser, всего 155 образцов. Хотя большинство этих образцов были дропперами, десять были загрузчиками, которые обменивались данными по сети для получения вторичного уровня вредоносного ПО.

«Разнообразие семейств вредоносных программ, многие из которых можно бесплатно купить или загрузить с подпольных торговых площадок, и предпочтение операторов вредоносных программ отказаться от своих полезных нагрузок, позволяют предположить, что авторы RATDispenser могут работать в режиме «вредоносное ПО как услуга». бизнес-модель», - считают исследователи». ***(Mayank Sharma. New malware is capable of evading almost all antivirus products // Future US, Inc. (https://www.techradar.com/news/new-malware-is-capable-of-evading-almost-all-antivirus-products). 23.11.2021).***

***

«Компания Avast (дочерняя структура NortonLifeLock) представила отчет об угрозах за III квартал. По данным исследователей, риск столкнуться с атаками

программ-вымогателей и троянов удаленного доступа (RAT) вырос как для бизнеса, так и для обычных пользователей. RAT могут использоваться для отраслевого шпионажа, кражи учетных данных, преследования и даже распределенных атак типа «отказ в обслуживании» (DDoS). Исследователи угроз отмечают постоянное внедрение инноваций в кибепреступности, появление новых механизмов в области наборов эксплойтов и мобильного банковского трояна Flubot.

В начале третьего квартала произошла масштабная атака на компанию Kaseya. Провайдер ИТ-услуг и его клиенты стали жертвами программы-вымогателя Sodinokibi (также известна как Revil). Команда исследователей Avast обнаружила и предотвратила более 2,4 тыс. попыток атак. Вследствие вмешательства правоохранительных органов, операторы ПО-вымогателя выпустили ключ дешифрования, что привело к выходу из строя системы Sodinokibi. Однако 9 сентября специалисты Avast обнаружили и заблокировали новую попытку атаки. В третьей четверти команда Avast отметила, что коэффициент риска атак программ-вымогателей увеличился на 5% по сравнению со вторым кварталом и на 22% по сравнению с началом 2021 г.

Трояны удаленного доступа (RAT) также представляли собой опасную угрозу для бизнеса и обычных пользователей, которая в III квартале имела большее распространение, чем в предыдущие. Исследователи Avast обнаружили три новых версии троянов удаленного доступа: FatalRAT с возможностями защиты от виртуальных машин, VBA RAT, который использует уязвимость Internet Explorer CVE-2021-26411, и новую версию Reverse RAT 2.0, в которую добавлены фотосъемка с веб-камеры, кража файлов и защиту от обнаружения антивирусами.

Специалисты лаборатории угроз Avast также зафиксировали значительное увеличение активности руткитов в конце третьего квартала. Руткит – вредоносное ПО, предназначенное для предоставления злоумышленникам несанкционированного доступа с определенными системными привилегиями. Руткиты обычно предоставляют услуги другим вредоносным программам в пользовательском режиме.

Снова стали использоваться усовершенствованные наборы эксплойтов, которые теперь ориентируются на уязвимости Google Chrome. Самым активным набором стал PurpleFox. От него Avast в день защищал в среднем более 6000 пользователей. Rig и Magnitude активно использовались с июля по сентябрь. Набор эксплойтов Underminer появился после длительного периода бездействия и начал время от времени обслуживать HiddenBee и Amadey. В стадии интенсивной разработки находятся комплекты эксплойтов PurpleFox и Magnitude, которые регулярно получают новые функции и возможности эксплуатации.

Также эксперты Avast отслеживали новые способы атак на мобильные устройства с помощью FluBot, банковского трояна для Android, операторы которого изменили свой подход к социальной инженерии.

Flubot сначала распространялся, выдавая себя за службы доставки, чтобы побудить жертв загрузить якобы приложение для отслеживания посылки, которую они пропустили или скоро должны получить. В третьем квартале исследователи Avast обнаружили новые сценарии распространения этого вредоносного ПО. Один из примеров – это приложение для записи голосовой почты. Другой – фальшивые

сообщения об утечке личных фотографий. В самом опасном варианте атаки жертву заманивали на поддельную страницу, на которой было написано, что устройство пользователя уже заражено трояном FluBot. В этот момент заражение, скорее всего, не произошло. Затем жертву обманом заставляли установить программу, чтобы избавиться от Flubot. Тем самым, жертва не избавлялась от заражения, а наоборот устанавливала вредоносное ПО.

Flubot продолжил распространяться в тех странах, откуда во второй четверти атаковал пользователей из Европы, а именно в Испании, Италии, Германии, Австралии и Новой Зеландии». ***(Заметно растет активность троянов удаленного доступа // Компьютерное Обозрение (https://ko.com.ua/rastushhaya_aktivnost_troyanov_udalennogo_dostupa_ugrozhaet_bezopasnosti_biznesa_i_ryadovyh_polzovatelej_139495). 25.11.2021).***

***

«…Исследователи компании JFrog обнаружили в официальном репозитории Python Package Index (PyPI) 11 вредоносных пакетов, которые могут быть использованы для кражи токенов доступа к Discord и паролей или для осуществления атак с «подменой зависимостей» (Dependency Confusion).

Как вредоносные обозначены следующие пакеты: importantpackage/important-package, pptest, ipboards, owlmoon, DiscordSafety, trrfab, 10Cent10/10Cent11, yandex-yt и yiffparty. Пакеты importantpackage, 10Cent10 и 10Cent11 способны устанавливать обратный шелл на скомпрометированных системах.

Кроме того, выяснилось, что importantpackage использует сеть доставки контента FastlyCDN для маскировки коммуникаций с контрольным сервером — все выглядит как невинный обмен трафиком с доменом репозитория pypi.org. HTTPS-запросы направляются на pypi.python.org, а потом CDN перенаправляет их уже в виде HTTP-запроса к контрольному серверу psec.forward.io.global.prod.fastly.net. Обратное соединение осуществляется по тому же принципу.

Подмена зависимостей

В свою очередь, ipboards и trrfab способны выводить важную информацию с помощью метода под «подмены зависимостей».

Суть этой методики заключается в том, чтобы загружать в публичный репозиторий скомпрометированные компоненты под теми же именами, которые носят легитимные внутренние приватные пакеты, но с присвоением более высокого индекса версии. В результате менеджер пакетов целевого ПО автоматически скачивает скомпрометированную версию и устанавливает вредоносный модуль.

Это уже не первый случай использования Dependency Confusion в контексте PyPI: в начале этого года CNews уже писал об использовании этого механизма в кибератаках.

Атаки подобного рода позволяют злоумышленникам встраивать свой собственный вредоносный код во внутренние приложения атакуемых компаний, просто подменив внешние компоненты, используемые при сборке приложения.

Описавший эту атаку эксперт Алекс Бёрсан (Alex Birsan) получил вознаграждения сразу от 35 компаний-разработчиков. Но, как видим, ею до сих пор пытаются пользоваться.

Пакеты ipboards и pptest, как выяснилось, также способны использовать туннелирование DNS для вывода данных; подобное наблюдается впервые.

В исследовании JFrog указывается, что, хотя выявленные вредоносные пакеты не выглядят слишком уж опасными, обращает на себя внимание уровень их продвинутости в исполнении. «Они не тянутся к вашему кошельку среди бела дня, но на более скрытом уровне эти пакеты способны на многое; некоторые из них могут быть использованы для разведки и подготовки почвы для последующей атаки...», — говорится в исследовании.

На данный момент все вредоносные пакеты удалены.

«Компрометация популярных программных репозиториев — всегда большая удача для киберзлоумышленников, открывающая широкие возможности для дальнейших кибератак, — говорит Анастасия Мельникова, директор по кибербезопасности компании SEQ. — Отрадно, что эти вредоносные компоненты в репозитории не задержались, но остается вопрос, как избежать подобного в будущем…» ***(Роман Георгиев. Официальный репозиторий языка Python наводнили программы для кражи данных и паролей // CNews (https://www.cnews.ru/news/top/2021-11-23_ofitsialnyj_repozitorij). 24.11.2021).***

***

«Киберпреступная группировка APT-C-23 (также известная как GnatSpy, FrozenCell и VAMP) обновила функционал своего шпионского ПО для Android-устройств для проведения атак на пользователей на Ближнем Востоке. Новые возможности вредоноса позволяют ему быть более устойчивым к удалению с устройства и маскироваться под безобидные обновления приложений.

Группировка APT-C-23 активна по крайней мере с 2017 года. За годы существования группировка неоднократно обновляла свой инструмент для шпионажа, добавляя новые функции. Теперь вредонос получил возможность слежки за изображениями, контактами и журналами вызовов, чтение уведомления из приложений для обмена сообщениями, запись звонков (в том числе WhatsApp) и отклонение уведомлений из встроенных приложений безопасности Android.

В прошлом шпионское ПО группировки APT-C-23 распространялось через поддельные магазины Android-приложений под видом AndroidUpdate, Threema и Telegram. В ходе последней вредоносной кампании шпионское ПО принимает форму приложений, которые предназначены для установки обновлений на телефон, например, «Обновление приложений», «Обновление системных приложений» и «Аналитика обновлений Android». Предположительно, злоумышленники доставляют шпионское приложение, отправляя ссылку для скачивания потенциальным целям через смишинг-сообщения (вид фишинга через SMS).

После установки приложение начинает запрашивать разрешения для выполнения ряда вредоносных действий, предназначенных для обхода любых попыток вручную удалить вредоносное ПО. Приложение меняет свою иконку, маскируясь под такие популярные приложения, такими как Chrome, Google, Google Play и YouTube. Кроме того, если пользователь щелкнет на мошенническую иконку, запускается легитимная версия приложения, пока в фоновом режиме будет происходить слежка». ***(Шпионское ПО группировки APT-C-23 обзавелось новыми***

функциями // SecurityLab.ru (https://www.securitylab.ru/news/526845.php). 25.11.2021).

***

Програми-вимагачі

«Банда киберпреступников Conti, известная своими атаками с использованием программ-вымогателей, по сообщениям, раскрыла подробности о мировых лидерах, актерах и бизнес-магнатах после забастовки лондонского ювелирного дома Graff.

Нарушение было подтверждено Information Security Media Group официальным представителем Дома Граффа, который сказал, что организация работает с соответствующими правоохранительными органами, и проинформировал Офис Комиссара по информации Великобритании об инциденте.

«К сожалению, мы, как и ряд других предприятий, в последнее время стали объектом изощренных, хотя и ограниченных, кибератак со стороны профессиональных и решительных преступников. Наши системы безопасности предупредили нас об их вторжении, что позволило нам быстро отреагировать и выключить нашу сеть», - сказал ISMG представитель The House of Graff.

Сэм Карри, директор по безопасности Cybereason, поставщика решений для кибербезопасности, говорит, что может пройти много недель, прежде чем общественность станет известна о реальных последствиях атаки.

«Одна вещь, которая не является тривиальной для знаменитостей и знаменитостей, у которых, как сообщается, была украдена личная информация, заключается в том, что люди или организации с большими карманами с большей вероятностью заплатят выкуп, чем другие. Злоумышленники знают об этом и когда они нацеливаются организации за воровство, они будут настойчивы, терпеливы и основательны в своих атаках», - отмечает Карри.

Утечка высокого профиля

В сообщении британской газеты The Daily Mirror утверждается, что злоумышленники слили 69 000 конфиденциальных документов на сайт даркнета, включая файлы, связанные с Дональдом Трампом, Опрой Уинфри и Дэвидом Бекхэмом.

В сообщении газеты также утверждается, что утечка данных примерно 11000 человек касается состоятельных клиентов Граффа, а участники программы-вымогателя требуют выкуп на несколько десятков миллионов фунтов, чтобы остановить раскрытие дополнительной конфиденциальной информации.

«Мы проинформировали тех лиц, чьи личные данные были затронуты, и посоветовали им необходимые шаги. Благодаря нашим надежным средствам резервного копирования мы смогли восстановить и перезапустить наши системы в течение нескольких дней - что очень важно, без безвозвратной потери данных,» - говорит представитель Graff.

Согласно отчету, просочившиеся документы включают списки клиентов, счета-фактуры, квитанции и кредитовые авизо. В список вошли международные суперзвезды, такие как Том Хэнкс, Сэмюэл Л. Джексон и Алек Болдуин.

«К сожалению, похоже, что известные бренды, корпорации и даже правительственные ведомства преднамеренно становятся мишенью недобросовестных операторов, пытаясь вымогать деньги [и] вызвать сбои или просто смущение», - отмечает представитель House of Graff.

Тревор Морган, менеджер по продукту Comforte AG, говорит, что детали первоначального вектора атаки на данный момент являются спекулятивными, однако тактика могла быть простой социальной инженерией, при которой человека обманом заставляют запустить вредоносный код, который выглядит как безобидный на первый взгляд. вложение.

Морган также говорит, что злоумышленники, скорее всего, потребовали выкуп в биткойнах или какой-либо другой форме платежа, которую трудно отследить.

«Некоторые организации в подобных ситуациях были склонны не платить выкуп и просто восстанавливать все ИТ-системы в случае зашифрованных файлов, которые останавливают операции. Но в этой ситуации, очевидно, мы говорим о украденной конфиденциальной информации, которую Графф не хотел бы извлекать под открытым небом», - отмечает он.

По словам Моргана, чтобы избежать таких ситуаций, любая организация, обладающая конфиденциальной информацией, должна защищать ее с помощью системы безопасности, ориентированной на данные, как только она входит в корпоративную экосистему.

Он рекомендует хранить конфиденциальную информацию в токенизированном или зашифрованном виде с сохранением исходного формата данных.

«Киберпреступность продолжает расти и становиться все более сложной. Это угроза для любого бизнеса. Поддержание наивысшего уровня защиты от этих угроз всегда было для нас главным приоритетом. Мы постоянно укрепляем наши системы, чтобы противостоять этим угрозам по мере их развития», - отмечает представитель House of Graff.

Конти Атаки

Conti - одна из нескольких русскоязычных программ-вымогателей - предположительно действующих из стран, которые ранее были частью Советского Союза - которые продолжают поражать цели в США и Европе, вызывая массовые сбои.

Правительство США, которое отслеживает рост числа атак, связанных с программой-вымогателем Conti, недавно выпустило совместные рекомендации по кибербезопасности от Агентства по кибербезопасности и безопасности инфраструктуры США, ФБР и Агентства национальной безопасности, предупреждая, что Conti на данный момент успешно ударил больше более 400 организаций, базирующихся в США и за рубежом.

«В типичных атаках программ-вымогателей Conti злоумышленники крадут файлы, шифруют серверы и рабочие станции и требуют выкуп», - говорится в сообщении.

Чтобы лучше обезопасить себя от атак Conti, в предупреждении рекомендуется ряд мер защиты, в том числе «реализация мер по смягчению последствий, описанных в этом сообщении, которые включают требование многофакторной аутентификации, реализацию сегментации сети и поддержание операционных систем и программного обеспечения в актуальном состоянии».

Компания Coveware, занимающаяся реагированием на инциденты с программами- вымогателями, сообщает, что, судя по тысячам инцидентов, которые она помогала расследовать с апреля по июнь, Conti была вторым по распространенности программ-вымогателем, с которым она столкнулась, после Sodinokibi, также известного как REvil. Coveware сообщила, что в то время как на долю Sodinokibi приходилось более 16% всех инцидентов, с которыми она оказывала помощь, на Conti приходилось более 14%.

Как и другие операции с программой-вымогателем как услуга, Conti полагается на аффилированные лица для заражения жертв. Поскольку в последние месяцы некоторые крупные операции с программами-вымогателями исчезли, были переименованы или были приостановлены, эксперты говорят, что Conti, похоже, привлекает многих из своих аффилированных лиц, помогая им проводить больше атак». ***(Prajeet Nair. Celebrities' Data Dumped on Darknet Site After Hack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/celebrities-data-dumped-on-darknet-site-after-hack-a-17830). 01.11.2021).***

***

«Программы-вымогатели продолжают оставаться излюбленным оружием многих преступников для надежного уничтожения жертв малых, средних и крупных в погоне за безопасным, легким и надежным заработком.

Но сама среда вымогателей продолжает развиваться по-разному. Например, появление новых игроков остается постоянным, в то время как крупные имена иногда отключаются. Некоторые банды проводят сложные операции с использованием программы-вымогателя как услуги, обращаясь к специалистам по проникновению в сеть, переговорам, разработке вредоносных программ и многому другому. Однако многим другим не хватает бюджета и персонала, необходимого для надежной борьбы с крупными целями, поэтому они действуют на периферии. И хотя многие предприятия имеют собственные сайты утечки данных, даже они сопряжены с проблемами эксплуатации.

По мере того, как атаки программ-вымогателей продолжаются, экосистема продолжает развиваться по семи направлениям:

1. Группы взлета и падения

Фирмы, занимающиеся безопасностью, продолжают отслеживать постоянный отток хакеров-вымогателей, включая приток новых лиц или, по крайней мере, имен.

Темнеет в 3 -м квартале были Avaddon, Noname, относительный новичок Прометея и Revil, иначе Sodinokibi. Но REvil вернулся в сентябре, а затем снова исчез в прошлом месяце, возможно, из-за того, что его нарушили правоохранительные органы.

Также в третьем квартале появились новые игроки - или, по крайней мере, их имена - в том числе CryptBD, Grief, Hive, Karma, Thanos и Vice Society, пишут в блоге исследователи безопасности Cisco Talos Дэвид Либенберг и Кейтлин Хьюи.

2. Ребрендинг - обычное дело

Однако некоторые из этих якобы новых операций могут быть просто ребрендингом существующих групп. В третьем квартале, например, «группа программ-вымогателей SynAck, которая размещала сайт утечки данных под названием File Leaks, переименовала себя в El_Cometa», - говорит Иван Риги, аналитик по киберугрозам из Digital Shadows в анализе тенденций третьего квартала.

«Было обнаружено, что программа-вымогатель DoppelPaymer, вероятно, была переименована в группу вымогателей Grief, и считается, что группа вымогателей Karma является ребрендингом банды вымогателей Nemty», - добавляет он.

3. Атаки распространяются на множество групп.

Независимо от имен, большее количество игроков в третьем квартале, по-видимому, участвовало в большем объеме наблюдаемых атак, говорят исследователи Cisco Talos. В частности, из взаимодействий по реагированию на инциденты, с которыми работал Cisco Talos, только Vice Society и REvil были замечены в более чем одном взаимодействии, говорят они, «подчеркивая большую демократизацию появляющихся вариантов программ-вымогателей».

Cisco Talos не видел во время какого-либо взаимодействия, несмотря на то, что ранее был плодотворным: Рюк. «Многие исследователи безопасности считают, что семейство программ-вымогателей Conti является преемником Ryuk, что потенциально объясняет снижение количества наблюдений за деятельностью Ryuk», - говорят Либенберг и Хьюи из Cisco Talos.

Эти результаты во многом совпадают с данными других фирм. Например, компания Coveware, занимающаяся реагированием на инциденты с программами-вымогателями, зафиксировала резкий рост атак Conti и снижение атак Ryuk, основываясь на тысячах случаев, в которых она оказывала помощь в течение третьего квартала. Поскольку фирма помогает жертвам с инцидентами, которые не всегда становятся достоянием общественности, это, вероятно, одна из наиболее точных оценок того, что на самом деле происходит в дикой природе.

4. Не все операторы программ-вымогателей хорошо зарабатывают

Похоже, что большое количество групп программ-вымогателей остаются активными. Например, только с 25 октября израильская разведывательная компания Kela сообщает, что 11 групп перечислили жертв на своих порталах утечки данных: Avos Locker, BlackByte, BlackMatter, Clop, Conti, Grief, LockBit, Marketo, Midas, Pysa и Xing.

Некоторые накапливают большие деньги. По данным Coveware, в течение третьего квартала, когда бизнес, государственное учреждение или любая другая организация решали заплатить выкуп, в среднем они платили 140 000 долларов США, исходя из тысяч случаев, в расследовании которых они участвовали. Хотя этот средний показатель оставался неизменным со второго квартала, в нем отмечается, что за тот же период средний платеж увеличился более чем на 50%, что свидетельствует о том, что злоумышленники начали уделять больше внимания

жертвам меньшего и среднего размера после того, как администрация Байдена этим летом объявила о том, что борьба с программами-вымогателями.

Но исследователь McAfee Тибо Серет в своем блоге отмечает, что не при каждой операции вымогателя как услуги выплата выкупа исчисляется шестизначными и более цифрами.

«Судя по последним заголовкам, можно простить мысль, что все операторы программ-вымогателей ежегодно загребают миллионы долларов нечестным путем в результате своей гнусной деятельности», - говорит он. "Однако, скрываясь в тени каждой крупномасштабной атаки организованных банд киберпреступников, можно найти множество более мелких субъектов, у которых нет доступа к последним образцам программ-вымогателей, а также возможности присоединиться к пост-DarkSide RaaS мир или финансовое влияние, чтобы быстро нарастить».

5. Утечки вредоносных программ подпитывают более мелких игроков

Но небольшие предприятия могут быть новаторскими и в других отношениях. Например, Серет подробно описывает, как некоторые из них воспользовались июньской утечкой сборщика программ-вымогателей Babuk как строительным блоком для развертывания собственного, более совершенного вредоносного ПО для криптоблокировки.

Но в другом случае, по его словам, злоумышленники, ранее привязанные к программе-вымогателю.NET под названием Delta Plus, просто изменили записку о выкупе Бабука, вставив адреса биткойн-кошельков, которые они, а не Бабук, контролировали, чтобы жертвы заплатили выкуп, а затем использовали их для нацеливания жертвы. Он отмечает, что с помощью этого нового, хотя и слегка измененного вредоносного ПО, группа атаки начала требовать выкуп не в сотни долларов, а в тысячи.

6. Утечка украденных данных создает проблемы

Хотя кража данных у жертвы и угроза утечки - это стратегия, широко применяемая бандами вымогателей, она не является надежной. Проблема заключается в том, что жертва, конечно, все же может отказаться от оплаты - а если злоумышленник не украл конфиденциальные данные, возможно, даже в большей степени. Кроме того, размещение данных также сопряжено с проблемами, - говорит Риги из Digital Shadows в своем блоге.

«Многие группы программ-вымогателей испытывали трудности с управлением сайтами утечки данных и размещением данных в темной сети для загрузки», - говорит он. «Это привело к тому, что некоторые группы программ-вымогателей раскрыли данные с помощью общедоступных веб-сайтов для обмена файлами, таких как Mega [.] Nz или PrivatLab [.] Com. Поскольку эти службы размещены в открытом Интернете, их часто можно отключить, и большинство ссылки для скачивания удаляются в течение дня или двух».

Еще одна проблема, отмечает он, заключается в том, что темные веб-сайты - то есть сайты, доступные только через анонимизирующий браузер Tor - предназначены для приоритета конфиденциальности над производительностью. Следовательно, навигация в темной паутине может быть медленной, а попытка загрузить просочившиеся данные может вызвать разочарование.

По крайней мере, об этом сообщили многие пользователи русскоязычного форума по киберпреступности XSS, когда они попытались загрузить данные, просочившиеся в марте операцией вымогателя Clop, которая украла их у охранной фирмы Qualys.

«Скорость загрузки была настолько низкой, что некоторые пользователи утверждали, что им потребовалась почти неделя, чтобы загрузить первый набор данных, в то время как другие пользователи отказались», - говорит Риги.

Размещение сайтов утечки данных и платежных порталов также делает их мишенью для правоохранительных органов. Похоже, именно это и произошло с REvil, когда администратор перезагрузил сайты, основанные на Tor, только для того, чтобы обнаружить, что кто-то другой - возможно, бывший администратор, возможно, сотрудник правоохранительных органов, возможно, оба - также имели копию установочных файлов, позволяя им взламывать сайты Tor REvil.

7. Разоблачение рисков операторами

Некоторые операции с программами-вымогателями приносят особенно большой доход, отчасти благодаря тому, что некоторые жертвы платят выкуп в криптовалюте на сумму в миллионы долларов.

На прошлой неделе еженедельная немецкая газета Die Zeit сообщила, что, по мнению полиции Германии, они установили личность подозреваемого лидера REvil, самопровозглашенного биткойн-предпринимателя по имени Николай К. - не его настоящее имя - отчасти благодаря отслеживанию криптовалюты, связанной с атакой GandCrab, бывшего воплощением REvil. По сообщениям, полиция установила его личность после того, как выяснила, что одна из жертв, Государственный театр в Штутгарте, в 2019 году заплатила GandCrab криптовалюту на сумму 17000 долларов, и обнаружила, что она была привязана к учетной записи электронной почты, которую использовал Николай К.

Если он является администратором REvil, сообщает Die Zeit, это поможет объяснить роскошный образ жизни, задокументированный в социальных сетях его женой, который включает каникулы на яхте, роскошные часы Vanguard Encrypto на его запястье и высококачественный BMW на подъездной дорожке.

Но образ жизни, основанный на использовании программ-вымогателей, и попытки сохранить анонимность также могут сказаться на практикующих.

Например, 22 октября администратор программы-вымогателя Groove, известный под именем Orange, а также TetyaSluha и boriselcin для первого избранного президента России Бориса Ельцина, разместил сообщение на сайте утечки данных Groove, в котором утверждалось, что все усилия были предприняты. эксперимент, призванный «троллить» западные СМИ. Сообщение было опубликовано Boriselcin на форуме XSS Cybercrime.

В его сообщениях «утверждалось, что не существует такой вещи, как банда Groove, и что за всем этим стоит один человек, который работал со многими партнерскими программами вымогателей, включая BlackMatter, LockBit и другие», - Виктория Кивилевич, директор по исследованию угроз компании Kela, сообщает Information Security Media Group. «Автор утверждает, что его попросили написать статью о манипуляциях со СМИ, и сайт Groove был создан именно для этого».

Джон Фоккер, главный инженер и руководитель отдела кибер-расследований Advanced Threat Research в McAfee Enterprise, рекомендует относиться ко всем уголовным искам с большой долей скептицизма. «Независимо от того, является ли Groove мистификацией или нет, они или он - Orange - могут быть связаны с множеством взломов. Так что это определенно не розыгрыш для жертв», - говорит он.

Склонность некоторых главарей программ-вымогателей высказывать свои мысли на русскоязычных форумах о киберпреступности вместо того, чтобы просто забирать свои заработки и тихо уйти, также предполагает, что они находятся в повышенном стрессе, чтобы поддерживать темп операций, а то и оставаться анонимными. «Я думаю, что эмоции действительно накаляются, и если правоохранительные органы начнут принимать жесткие меры, мы можем ожидать гораздо больше подобных вспышек», - говорит Фоккер». ***(Mathew J. Schwartz. 7 Trends: How Ransomware Operations Continue to Evolve // Information Security Media Group, Corp. (https://www.govinfosecurity.com/7-trends-how-ransomware-operations-continue-to-evolve-a-17841). 02.11.2021).***

***

«Программы-вымогатели превратились в многомиллиардную индустрию. Вместо похищения человека киберпреступники размещают вредоносное ПО в компьютерных системах, блокируя их использование до тех пор, пока не будет выплачен денежный выкуп. По данным Statista, в этом году от атак программ-вымогателей пострадали 68,5% компаний.

Организации теряют 17 700 долларов каждую минуту из-за фишинга. Разработанный для того, чтобы обманом заставить людей раскрывать конфиденциальные данные по электронной почте, Google по состоянию на январь 2021 года выявил более 2 миллионов фишинговых сайтов.

Киберпреступность растет повсюду, потому что преступники зарабатывают деньги, заражая устройства вирусами, создавая угрозы, получая доступ к правительственным или корпоративным данным и многое другое.

Вот почему потребность в людях, обладающих знаниями в области кибербезопасности, для борьбы с этими киберпреступниками настолько велика. Бюро статистики труда США прогнозирует рост карьеры в сфере информационной безопасности на 32% к 2028 году.

«Некоторое время кибербезопасность является областью роста, - говорит Крис Юэлл, главный специалист по безопасности и конфиденциальности в NRC Health и младший преподаватель Городского университета Сиэтла. «В последние 5-10 лет компании стали больше интересоваться защитой своего бизнеса от киберпреступлений, и им нужны люди для выполнения этой работы».

По его словам, страховые компании, заинтересованные стороны и акционеры также оказывают давление на компании, чтобы те защищали свои данные.

Множество доступных профессий

Возможности специализированной работы в области кибербезопасности разнообразны. «Вы можете начать с работы аналитиком по безопасности,

архитектором или инженером, а затем перейти на уровень управления», - говорит Юэлл. После этого возможно повышение до начальника службы безопасности.

«Есть также общий контроль безопасности, судебно-медицинский анализ, эксперты по расследованию инцидентов, аналитики кода и множество других возможностей», - говорит Юэлл. «Получите базовые знания о кибербезопасности, а затем определите, в чем заключается ваша страсть».

Все отрасли нуждаются в квалифицированных специалистах по кибербезопасности. Правительство, правоохранительные органы, транспорт, здравоохранение, финансы, высшее образование, энергетика, малый и средний бизнес - у всех есть спрос на сотрудников, которые могут бороться с киберпреступниками. Чтобы помочь в борьбе, преподавание кибербезопасности в средней школе и даже в средней школе стало необходимым.

«Нам нужны старшеклассники, разбирающиеся в кибербезопасности, - говорит Морган Зантуа, доцент и программный директор Школы технологий и вычислений CityU. «Обучая необходимых нам учителей, мы можем направить студентов на карьеру в области кибербезопасности и увеличить количество рабочих мест».

CityU недавно получил грант в размере 700 000 долларов от Агентства национальной безопасности на обучение учителей региональных средних школ вопросам кибербезопасности. Через два года консорциум наймет 70 учителей старших классов для изучения содержания и принципов кибербезопасности в Интернете. Местные, региональные и национальные организации, правительственные учреждения и военные организации будут призваны поддержать эту сеть, чтобы увеличить количество выпускников средних школ, которые выберут карьерный путь в области кибербезопасности.

Подготовка к роли кибербезопасности

Зантуа предлагает потенциальным работникам в этой области сначала оценить свой карьерный интерес, а затем начать изучать технические аспекты, необходимые для работы, которую они хотят.

«Как минимум, вы должны знать язык программирования общего назначения, такой как Python, и понимать как сети, так и операционные системы», - говорит Зантуа. «Добавление сертификатов в ваше резюме также поможет вам получить работу».

Юэлл говорит, что есть много возможностей для этого карьерного роста - вот что так интересно и увлекательно в этой области - нет предела. Тем не менее, вам нужно войти в эту профессию с определенными талантами.

«У вас должны быть отличные коммуникативные навыки и навыки работы с людьми, вы должны отлично решать проблемы и обладать хорошими аналитическими способностями», - говорит он. «Остальное я могу научить».

Юэлл говорит, что лучше всего начать с получения сертификата Security +. Это учетные данные кибербезопасности начального уровня, предлагаемые некоммерческой ассоциацией CompTIA. Часто это первая сертификация, полученная ИТ-специалистом.

По словам Юэлла, для большинства вакансий в этой области требуется степень бакалавра, но, возможно, вам удастся встать на ноги, работая стажером без ученой

степени. Но когда вы станете менеджером или директором, вам потребуется ученая степень. По его словам, для работы на более высоком уровне может потребоваться докторская степень.

Зантуа говорит, что в области кибербезопасности может быть роль для любого, от подростка до взрослого, который уже второй год делает карьеру. В настоящее время эта карьера может похвастаться нулевой безработицей». ***(Demand for qualified cybersecurity workers is soaring // The Seattle Times (https://www.seattletimes.com/sponsored/demand-for-qualified-cybersecurity-workers-is-soaring/). 15.11.2021).***

***

«Недавняя волна атак программ-вымогателей вызвала повышенное беспокойство у всех, от частного сектора до федерального правительства. Чтобы лучше бороться с атаками программ-вымогателей, организации осознают, что им необходимо улучшить ключевые аспекты своей киберзащиты. В отчете, опубликованном в понедельник поставщиком управления идентификацией Hitachi ID, рассматриваются изменения, которые предпринимают предприятия, чтобы не стать жертвой программ-вымогателей.

В ходе опроса, проведенного Pulse и Hitachi ID в сентябре, 100 руководителей ИТ-отдела и службы безопасности опрашивали, какие изменения они вносят в свою инфраструктуру кибербезопасности, как эти изменения могут лучше справляться с кибератаками и какую роль политика играет в их стратегии.

Программное обеспечение как услуга (SaaS) - один из ключевых методов кибербезопасности. Полные 99% респондентов заявили, что по крайней мере часть их инициатив по обеспечению безопасности включает переход на SaaS, в котором внешний поставщик размещает и доставляет облачные приложения своим клиентам. Около 36% заявили, что более половины их усилий связаны с этим типом переездов.

Среди других целей безопасности, которые были инициированы, многофакторная аутентификация была запущена 82% опрошенных, единый вход - 80%, управление доступом к удостоверениям - 74% и управление привилегированным доступом - 60%. Но Zero Trust, который все чаще пропагандируется как более эффективная стратегия, находится ниже в списке.

Только 47% респондентов заявили, что они соблюдают принципы и политику нулевого доверия. Однако почти три четверти признали, что видят преимущество в передаче компонентов архитектуры Zero Trust на аутсорсинг у меньшего числа поставщиков как способ упростить стратегию.

Одна из проблем при переносе приложений в облако связана с устаревшими системами, которые нелегко перенести. Полные 86% опрошенных признали, что у них есть устаревшие системы, которые необходимо защитить.

Киберпреступники, внедряющие программы-вымогатели, все смелее разрабатывают свои атаки. Одна из стратегий - попытаться привлечь инсайдеров, желающих использовать свою собственную компанию. Почти половина (48%) респондентов заявили, что к ним или другим сотрудникам обращались напрямую, чтобы помочь в проведении атаки с использованием программ-вымогателей. Более половины (55%) директоров заявили, что к ним обращались так же. Среди тех, кто

сказал, что с ними связались, 83% заявили, что этот метод расширился, поскольку все больше людей работают из дома.

Обучение сотрудников вопросам кибербезопасности - еще один ключевой метод предотвращения атак программ-вымогателей. 69% опрошенных заявили, что их организация улучшила киберобразование для сотрудников за последние 12 месяцев. Около 20% заявили, что еще не сделали этого, но планируют увеличить тренировку в следующие 12 месяцев.

Знание того, как разработать обучение сотрудников безопасности, имеет первостепенное значение. Около 89% респондентов заявили, что они обучили сотрудников тому, как предотвращать фишинговые атаки, 95% сосредоточились на том, как обеспечить безопасность паролей, а 86% - на том, как создавать безопасные пароли.

Наконец, более трех четвертей (76%) респондентов заявили, что они обеспокоены атаками со стороны других правительств или национальных государств, влияющими на их организацию. В ответ 47% заявили, что они не считают, что их собственное правительство принимает достаточные меры для защиты бизнеса от кибератак, а 81% считают, что правительство должно играть более важную роль в определении национального протокола и инфраструктуры кибербезопасности.

«ИТ-среды стали более подвижными, открытыми и, в конечном итоге, уязвимыми, - сказал Брайан Крист, инженер по продажам Hitachi ID Systems. «В результате все больше компаний меньше полагаются на традиционные методы, такие как VPN, для обеспечения безопасности своих сетей. Определенные учетные данные, такие как пароли к привилегированным учетным записям, являются ключом к королевству. Если злоумышленник получит эти учетные данные в свои руки, почти наверняка последует атака программы-вымогателя».

Рекомендации

Чтобы помочь вашей организации лучше защитить себя от атак программ-вымогателей, Христос рекомендует упреждающую стратегию для блокировки данных и управления доступом изнутри.

Во-первых, пароли, которые являются статическими или хранятся локально, могут быть использованы для взлома данных. Поэтому организациям необходимо настроить защиту управления доступом, чтобы снизить этот риск.

Во-вторых, использование многофакторной аутентификации (MFA) и единого входа (SSO) может уменьшить угрозу, не дав злоумышленникам возможности получить доступ к вашей сети.

В-третьих, предоставление пользователям минимального доступа, необходимого им для выполнения своей работы, может дополнительно защитить вашу организацию. Два метода достижения этого уровня безопасности - это оперативный доступ (JIT) и случайные пароли привилегированных учетных записей.

В-четвертых, умное управление паролями и привилегированная защита должны привести к конечной цели Zero Trust.

«Zero Trust - это подход к безопасности, который обращается к этим новым сетевым реалиям, не доверяя никому - и многие тяготеют к Zero Trust, чтобы снизить риск кибератак из нескольких точек входа (включая внутренние)», - сказал Крист.

«При этом важно помнить, что Zero Trust - это путешествие, а не пункт назначения, и это может занять время».

Но организации могут достичь нулевого доверия, выполнив ряд шагов: 1) ничему не доверять; 2) Закрепите все; 3) аутентифицировать запросы и оценивать запросы доступа на основе контекста; 4) Оценить все запросы; и 5) предоставлять доступ по принципу наименьших привилегий (PoLP)». ***(Lance Whitney. How organizations are beefing up their cybersecurity to combat ransomware // TechnologyAdvice (https://www.techrepublic.com/article/how-organizations-are-beefing-up-their-cybersecurity-to-combat-ransomware/). 15.11.2021).***

***

«Программы-вымогатели. Пять лет назад сообщество кибербезопасности хорошо знало этот термин, хотя, среди прочего, он был далек от разговоров за обеденным столом. Времена изменились. С начала 2020 года о программах-вымогателях много заголовков. Об этом говорят как внутри, так и вне индустрии безопасности, и многие из них на собственном опыте испытали на себе боль от программ-вымогателей.

В отчете IBM Security 2021 Cost of a Data Breach отмечается, что атаки программ-вымогателей обходятся в среднем в 4,62 миллиона долларов без учета стоимости выкупа. Убыток может нанести вред компании вплоть до ее закрытия. И компании - не единственные жертвы. Только в 2021 году рост атак программ-вымогателей нарушил основные потребности потребителей - от нефтепроводов до цепочки поставок продуктов питания.

Федеральное правительство Соединенных Штатов обратило на это внимание. Палата представителей приняла пять законодательных актов, касающихся кибербезопасности критически важных систем. Администрация транспортной безопасности (TSA) недавно выпустила новую директиву по безопасности для операторов трубопроводов. Дополнительный ответ был объявлен в мае 2021 года президентом США Джо Байденом. «Исполнительный указ о повышении кибербезопасности нации» (также известный как EO 14028) требует от федеральных агентств разработать новые требования, направленные на усиление их программ безопасности. Эти требования все еще определяются, но они варьируются от реализации архитектуры нулевого доверия до модернизации программ кибербезопасности и разработки стратегии облачной безопасности.

Четвертый раздел вызвал наибольший интерес у нашей команды X-Force, главным образом потому, что он сосредоточен на цепочке поставок для критически важной инфраструктуры, которая, как мы видели во многих наиболее заметных утечках данных, может быть главной целью злоумышленников. Раздел «Повышение безопасности цепочки поставок программного обеспечения» включает четыре темы, которые связаны с обеспечением безопасности в жизненном цикле разработки программного обеспечения:

Базовые стандарты безопасности: Национальный институт стандартов и технологий (NIST) установит базовые стандарты для разработки программного обеспечения, продаваемого правительству США, включая минимальные уровни для проверки кода, моделирования угроз и автоматического тестирования.

Маркировка «Безопасное программное обеспечение»: будет внедрена система маркировки, которая будет отражать всесторонние уровни тестирования и оценки, которым, возможно, подвергался продукт.

Спецификация программного обеспечения (SBOM): SBOM поможет организациям управлять рисками, позволяя им быстро определять, какие уязвимые программные компоненты присутствуют в их продуктах.

Определение «критического программного обеспечения»: NIST разработает четкое определение программного обеспечения, подпадающего под действие ЕО. NIST рекомендовал, чтобы начальная фаза внедрения ЕО была сосредоточена на автономном локальном программном обеспечении, которое имеет критически важные для безопасности функции или представляет собой аналогичный значительный потенциал вреда в случае компрометации.

Хотя эти темы предназначены специально для поставщиков программного обеспечения, этот пул больше, чем вы можете ожидать. Федеральное правительство затрагивает практически все сферы здравоохранения, розничной торговли, промышленности и финансов.

Какие первые шаги компании должны предпринять сегодня? Во-первых, осознав, что большинство требований в рамках ЕО еще не определены, просмотрите ЕО и оцените свою среду. Мы рекомендуем обратить внимание на четыре конкретные области:

Есть ли у многофакторной аутентификации, шифрования данных и обнаружения и реагирования на процессы, встроенные в среду разработки программного обеспечения?

Есть ли у вас инструменты для поддержки надежного исходного кода и проводите ли вы анализ кода, чтобы найти и исправить уязвимые места в этом коде?

Есть ли у вас инструменты, которые могут помочь вам определить и устранить известные и потенциальные уязвимости, которые могут сделать ваше программное обеспечение, устройства и подключенную среду уязвимыми для злоумышленников?

Обновлены ли данные о вашем программном коде или компонентах, средствах контроля внутренних и сторонних программных компонентов, а также об инструментах и услугах в процессе разработки программного обеспечения? Важно регулярно оценивать эти процессы и средства контроля, чтобы быть уверенным, что у вас есть точная информация, и вы можете найти и исправить любые недостатки.

ОР особо подчеркивает важность тестирования программного обеспечения. NIST предложил минимальный набор стандартов для тестирования, который включает моделирование угроз, тестирование на проникновение, анализ кода (SAST) и динамический анализ (DAST) в отношении программного кода и любых связанных библиотек, пакетов и служб. Также подчеркивается устранение критических уязвимостей.

Наконец, в этом разделе подчеркивается важность определения процессов реагирования на инциденты и средств контроля, которые должны включать круглосуточный мониторинг и возможности реагирования.

Хотя этот процесс может показаться утомительным и трудоемким, решение этих проблем может значительно улучшить ваши программы обеспечения безопасности и соответствия нормативным требованиям. Оценка и переоценка

ваших инвестиций в безопасность может помочь вам максимизировать их эффективность и снизить риск серьезной компрометации. Вы также можете получить институциональную поддержку от вашей исполнительной команды и правления, поскольку за этим ОР стоит федеральное правительство. А с увеличением заинтересованности происходит сдвиг в корпоративной культуре. Безопасность может иметь приоритет сверху вниз, что может означать больше ресурсов и бюджета.

Обращение к ОР также может помочь навести порядок в вашем доме. Вы всегда будете понимать своих людей, процессы и технологии. У вас будет возможность понять, какие данные у вас есть, куда они передаются, что они контролируют и какие облачные сервисы используются.

Федеральное правительство уделяет внимание безопасности, и мы ожидаем, что это внимание будет только возрастать.

Если вы хотите сотрудничать с командой экспертов по ЕО, IBM Security может вам в этом помочь. X-Force рада обсудить вашу среду и возможные варианты применения ЕО». ***(Abby Ross. A New Cybersecurity Executive Order Puts the Heat on Critical Infrastructure Suppliers // IBM (https://securityintelligence.com/posts/new-cybersecurity-executive-order-critical-infrastructure-suppliers/). 09.11.2021).***

***

«Федеральное бюро расследований (ФБР) выпустило уведомление частной отрасли (PIN), в котором говорится, что банды программ-вымогателей нацелены на компании, участвующие в «финансовых событиях, зависящих от времени», таких как слияния и поглощения.

По данным бюро, банды ищут непубличную финансовую информацию и угрожают опубликовать ее, если жертвы не выполнят требования о выкупе.

Агентство отмечает, что группы программ-вымогателей используют надвигающиеся события, которые могут повлиять на цены акций компаний, такие как объявления, слияния и поглощения, чтобы заставить жертв заплатить.

Банды программ-вымогателей используют информацию о фондовых рынках для вымогательства у жертв

Федеральные правоохранительные органы перечислили несколько попыток вымогательства, связанных с информацией о фондовых рынках.

В 2020 году злоумышленники, ведущие переговоры о выплате выкупа, пригрозили утечь данные жертвы на биржу NASDAQ и «посмотреть, что произойдет» с акциями.

Эти попытки вымогательства произошли после того, как злоумышленник под псевдонимом «Неизвестный» призвал других на российском хакерском форуме «Эксплойт» использовать информацию из NASDAQ для принуждения своих жертв к уплате выкупа.

Точно так же три публично торгуемые американские компании, участвовавшие в слияниях и поглощениях, стали жертвами банд вымогателей в период с марта по июль 2020 года.

Анализ трояна удаленного доступа Pyxie (RAT) показал, что этот вариант вредоносного ПО искал информацию об акциях, используя такие ключевые слова,

как 10-q1, 10-sb2, n-csr3, Marketwired, NASDAQ и Newswire. Злоумышленники используют бэкдор в атаках программ-вымогателей Defray777 и RansomEXX.

Кроме того, банда вымогателей Darkside разместила на своем сайте утечки данных сообщение о том, что ее «команда и партнеры шифруют многие компании, торгующиеся на NASDAQ и других фондовых биржах».

Группа попросила заинтересованные стороны навести справки о таких компаниях, пообещав, что «если компания откажется платить, мы готовы предоставить информацию до публикации».

Точно так же банда вымогателей REvil / Sodinokibi сообщила, что планирует добавить авто-рассылку для связи с платформами фондовой биржи и информировать их о том, что жертва подверглась атаке с помощью программы-вымогателя.

Инсайдерская информация имеет большое значение на подпольных рынках. В 2015 году девять человек были обвинены во взломе Newswire с целью кражи неопубликованной корпоративной информации. Точно так же гражданин Калифорнии столкнулся с обвинениями после якобы продажи инсайдерской информации в даркнете в 2016 и 2017 годах.

«Неудивительно, что хакеры могут получить доступ ко всем видам конфиденциальной информации после того, как они взломали системы организации или учетную запись пользователя», - отметил Ариэль Зоммер, старший менеджер по продукту OneLogin. «Финансовые данные и данные о слияниях и поглощениях - это одна из самых конфиденциальных сведений, которые может иметь организация. А с учетом того, что в 2021 году глобальные слияния и поглощения станут рекордными, банды вымогателей - еще раз - демонстрируют свою способность быстро адаптировать свою тактику в зависимости от рыночных условий ».

Жертвы с большей вероятностью заплатят при слияниях и поглощениях

Согласно предупреждению ФБР, банды программ-вымогателей получили рычаги воздействия на компании во время слияний и поглощений, поскольку жертвы пытаются избежать негативной реакции инвесторов.

Банды вымогателей тщательно выбирают своих жертв и корректируют сроки вымогательства, чтобы они совпадали со значительными финансовыми событиями.

«ФБР оценивает, что участники программ-вымогателей, скорее всего, используют важные финансовые события, такие как слияния и поглощения, для нацеливания и использования компаний-жертв для заражения программ-вымогателей».

Эрих Крон, специалист по безопасности в KnowBe4, отметил, что время атаки гарантирует, что банды вымогателей нанесут наибольший ущерб.

«Выбор времени для атак программ-вымогателей, чтобы вызвать сбои в определенное время для повышения шансов на выплату, не является новой тактикой; однако для организаций, участвующих в слияниях и поглощениях, это важно знать», - продолжил Крон. «В отличие от ранних разновидностей программ-вымогателей, которые автоматически и неизбирательно шифруют любые файлы, которые они могут найти, новые версии программ-вымогателей требуют значительных человеческих действий перед началом фазы шифрования».

По данным ФБР, «если жертвы не заплатят выкуп быстро, участники программ-вымогателей будут угрожать публично раскрыть эту информацию, что вызовет негативную реакцию потенциальных инвесторов».

Джек Чапман, вице-президент по анализу угроз компании Egress, согласен с тем, что банды вымогателей всегда ищут способы «мотивировать» своих жертв платить, зная, что чем больше боли и давления они применяют, тем больше шансов на успех.

Ориентируясь на организации, находящиеся в процессе важных финансовых событий, таких как слияния и поглощения, банды программ-вымогателей ожидают, что их атаки окажут более сильное воздействие, поскольку они могут отрицательно повлиять на стоимость акций жертвы.

«Банды программ-вымогателей не остановятся ни перед чем, чтобы обеспечить успех своих атак - и для организаций, подверженных риску нападения, это должно стать серьезной проблемой», - заявляет ФБР.

Однако ФБР не поощряло компании уступать этим требованиям и сообщало о любых попытках вымогательства, чтобы привлечь виновных к ответственности. Кроме того, выплата выкупа побуждает банды вымогателей атаковать большее количество компаний, участвующих в слияниях и поглощениях, используя аналогичную тактику.

Подчинение требованиям группировок программ-вымогателей не гарантирует восстановление данных и не препятствует продаже злоумышленниками инсайдерской информации третьим лицам. ФБР также призвало защитников сетей укрепить свои сети, чтобы не допустить доступа банд вымогателей.

Однако ФБР признало, что руководители сталкиваются с трудным выбором, когда их бизнес не может функционировать после атаки, посоветовав руководителям бизнеса рассмотреть все варианты защиты своих акционеров, клиентов и сотрудников…» ***(ALICIA HOPE. FBI Warns That Ransomware Gangs Target Companies During Mergers and Acquisitions, Threatening To Disclose Non-Public Information // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/fbi-warns-that-ransomware-gangs-target-companies-during-mergers-and-acquisitions-threatening-to-disclose-non-public-information/). 12.11.2021).***

***

«В то время как программы-вымогатели остаются чумой для организаций по всему миру, в новом отчете коммерческой страховой компании Corvus указывается, что расходы на программы-вымогатели значительно сокращаются из-за большей готовности. И хотя в начале 2021 года количество обращений по страхованию от киберпространства резко возросло из-за уязвимости Microsoft Exchange, с тех пор они имеют тенденцию к резкому снижению.

Количество претензий по киберстрахованию резко возросло после серьезной уязвимости, но в целом по сравнению с прошлым годом снизилось

Индекс Corvus Risk Insights Index - новое исследование, но его планируется выпускать ежеквартально. Эта первая редакция за 4 квартал 2021 года основана на базе данных требований компании, запатентованной технологии сканирования безопасности и избранных сторонних источниках.

Хотя это может показаться очевидным, отчет указывает на то, что улучшение основных принципов безопасности приводит к значительным немедленным улучшениям. Повышение осведомленности как о безопасности электронной почты, так и о надлежащем резервном копировании, по-видимому, снижает расходы на программы-вымогатели, несмотря на глобальный рост преступной индустрии и рост требований к выкупу.

В первом квартале 2021 года произошел значительный всплеск требований киберстрахования от технических фирм из-за последствий уязвимости Microsoft Exchange Server. Однако количество заявлений резко упало, как только эта уязвимость была исправлена. Они продолжали резко падать в течение 2021 года, в конечном итоге опустившись ниже уровней 2020 года в третьем квартале.

В то время как количество инцидентов снижается, затраты на программы-вымогатели, как правило, растут в зависимости от каждого инцидента из-за растущего распространения методов «двойного вымогательства» (при котором секретные документы вывозятся, а злоумышленники угрожают публично их опубликовать) за последний год. Но это только в том случае, если компанию поймают врасплох, без надлежащих резервных копий и без шифрования или отделения конфиденциальной информации от общедоступных систем. Компании, которые не успевают за безопасностью, платят больше за каждый инцидент, но в целом затраты на программы-вымогатели фактически снижаются из-за тенденции к большей осведомленности и подготовке к атакам.

Разбивка индивидуальных затрат на программы-вымогатели и влияние средств безопасности

В отчете Corvus представлены отдельные расходы на программы-вымогатели, которые обычно связаны с претензиями по страхованию от киберпространства. Одна из затрат, которую иногда упускают из виду, - это возможность судебного разбирательства после кражи конфиденциальных данных или в случае отказа в жизненно важной услуге из-за неработоспособности системы.

Цифры показывают, что чем больше организация, тем больше вероятность, что она понесет судебные издержки. Для самых маленьких предприятий с не более чем 10 сотрудниками вероятность быть привлеченным в суд после атаки составляет всего около 24%. Это число постоянно увеличивается до 76% для компаний с минимум 250 сотрудниками.

Некоторые отрасли также подвержены повышенному риску затрат на программы-вымогатели из-за судебных разбирательств и с большей вероятностью подадут в суд на поставщика из-за нарушения. На сегодняшний день наиболее спорными группами являются медиа-компании и, что несколько удивительно, производители металлов. Другие поставщики, подверженные существенно повышенному риску, включают поставщиков, работающих в сфере финансов, страхования и розничной торговли. Однако, хотя теперь атака программы-вымогателя может привести к смерти из-за нефункционирующего оборудования, отрасль здравоохранения с наименьшей вероятностью привлечет поставщика к суду.

Полная разбивка затрат по претензиям по киберстрахованию не будет доступна до 2022 года, но данные за 2020 год показывают, что меры реагирования на нарушения были, безусловно, самым дорогостоящим аспектом претензий.

Непредвиденное прерывание бизнеса или упущенная выгода из-за сбоев, вызванных атакой на стороннего поставщика, также были непропорционально большим фактором.

В отчете также отмечаются две основные тенденции в области безопасности среди организаций, которые напрямую способствовали общему снижению затрат на программы-вымогатели. Одним из них является постепенная замена очень уязвимых систем протокола удаленного рабочего стола (RDP). В прошлом году около 50% существующих систем RPD были заменены на более безопасные варианты, что в значительной степени обусловлено условиями пандемии и переходом на модели удаленной работы. До начала пандемии до 10% организаций все еще использовали системы RDP; сейчас это число упало до не более 4%.

Еще одно снижение затрат на программы-вымогатели произошло за счет увеличения на 158% использования средств защиты электронной почты с начала пандемии. Некоторые отрасли увеличили использование этих инструментов до 400%. Однако в отчете отмечается, что общее количество организаций, использующих эти инструменты, составляет чуть более 16% даже при таком значительном увеличении. Исследование показало, что качественные инструменты электронной почты, как правило, сокращают количество случаев фишинга в заявках на киберстрахование на 45% и вдвое в целом.

Увеличена сумма платежа за программу-вымогатель; компании производят выплаты

Средняя сумма выкупа выросла, но количество компаний, производящих эти выплаты, уменьшилось. Платежи неуклонно снижались с 44% инцидентов в третьем квартале 2020 года до 12% в третьем квартале 2021 года. Банды программ-вымогателей получают все больше от организаций, которые они все еще могут принуждать к выплате, однако, увеличивая средний платеж до 290 000 долларов в третьем квартале этого года (рост от 114000 долларов во втором квартале).

Подготовка компаний как центральный фактор в этих изменениях требований киберстрахования поддерживается тем, что количество инцидентов с программами-вымогателями остается относительно стабильным с 2019 года. Были и пики, и спады, но в третьем квартале 2021 года количество атак было примерно таким же, как и в третьем квартале. как 2020, так и 2019 годов». ***(SCOTT IKEDA. Cyber Insurance Claims Spike With Major Attacks, but Ransomware Costs Down Sharply From 2020 // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cyber-insurance-claims-spike-with-major-attacks-but-ransomware-costs-down-sharply-from-2020/). 15.11.2021).***

***

«После первых трех ходов в шахматной партии появляется 121 миллион возможностей. В то время как новичок играет в игру, пока не получит мат, гроссмейстер заранее понимает несколько ходов. Подобно способности великого мастера к визуализации, руководитель службы безопасности организации должен думать наперед, особенно когда киберпреступники используют чрезвычайно изощренные тактики, методы и процедуры.

Например, программа-вымогатель LockBit существует с 2019 года, но версия 2.0, как утверждают авторы LockBit, является одним из самых быстрых вариантов вымогателя с шифрованием файлов на рынке глубокой и темной сети на сегодняшний день. Программа-вымогатель 2.0 не просто шифрует; он разрушает. Еще одна особенность - боковое распространение на офлайн-устройства. Резервные копии данных становятся бесполезными, а доступ к критически важным данным обеспечивается с помощью законных учетных данных «нанятых» инсайдеров.

Для предприятий становится важным действовать по-другому и переходить к прогнозируемому подходу к борьбе с атаками программ-вымогателей.

Проблема: почему организациям не удается предотвратить атаки программ-вымогателей?

Атака программы-вымогателя может быть результатом нескольких векторов атаки, но наиболее распространенными из них являются фишинг, протокол удаленного рабочего стола (RDP) и уязвимости программного обеспечения. Для защиты от атак программ-вымогателей организации следуют глобальным стандартам, таким как NIST и CISA.руководящие указания. Организации вкладывают средства в симуляции фишинга, обучение сотрудников, менеджеров паролей и т.д. По вопросам кибербезопасности, чтобы контролировать потерю учетных данных. Чтобы предотвратить атаки на основе RDP, организации приобретают межсетевые экраны, службы ведения журналов и мониторинга, резервные копии данных и проводят периодическое сканирование уязвимостей и угроз. Наконец, организации также вкладывают средства в услуги управления уязвимостями для обнаружения уязвимостей программного обеспечения. Это самые основы того, что уже делают все организации, и составляют лишь небольшой процент от всех действий, которые организация выполняет для защиты от кибератак, включая программы-вымогатели.

В среднем предприятия развертывают в своей среде 45 сервисов и продуктов кибербезопасности. Каждый продукт предоставляет информацию на отдельной информационной панели, но не существует метода, с помощью которого группа безопасности могла бы сопоставить данные от всех услуг / продуктов кибербезопасности в своей среде, чтобы получить полную видимость в реальном времени. Несмотря на все вложения, службы безопасности не имеют возможности объективно предсказать вероятность взлома в масштабах всего предприятия. Разрозненные сервисы кибербезопасности без единой и динамичной метрики делают оценку кибербезопасности непрозрачным, сложным, сложным, своевременным и реактивным процессом.

Решение: прогнозируемый подход в реальном времени

Поскольку атаки программ-вымогателей превратились из тактики «спрей и молись» в тщательно спланированное мероприятие, предприятиям необходимо лучше подготовиться. Что является недостающим звеном, которое может подтолкнуть начинающий бизнес к тому, чтобы стать великим мастером кибербезопасности с дальновидностью и адекватной видимостью уязвимостей безопасности?

Руководители отдела безопасности и управления рисками могут улучшить прозрачность, приняв упреждающий и прогнозирующий подход к кибербезопасности, который:

Сопоставляет уязвимости, выявленные множеством продуктов кибербезопасности, для защиты людей, процессов, технологий и третьих лиц.

Принимает API-потоки сигналов от услуг / продуктов. Используя количественную оценку рисков с помощью машинного обучения в реальном времени, репозиторий может моделировать оценку вероятности взлома программ-вымогателей для каждого сотрудника, конечной точки, облачного актива, бизнес-подразделения и т.д.

Использует матрицу ATT & CK MITER для детального и упорядоченного списка уязвимостей, видимых лицам, принимающим решения. Например, вероятность взлома программ-вымогателей по начальному вектору, выполнение, постоянство, эскалация привилегий и уклонение от защиты доступны через данные, собранные со всех продуктов и услуг.

Несмотря на то, что проводятся значительные исследования первоначального использования и использования защиты периметра, существует пробел в центральных знаниях о противодействии после того, как был получен первоначальный доступ. ATT & CK for Enterprise фокусируется на TTP (террористическая, тактика, приемы и процедуры), которые злоумышленники используют для принятия решений, расширения доступа и выполнения своих задач. Он направлен на описание действий злоумышленника на достаточно высоком уровне, чтобы их можно было широко применять на разных платформах, при этом сохраняя достаточно деталей, чтобы быть технически полезными. Упрощенное представление вероятности программ-вымогателей превращает их угрозу из нематериального «возможно» в бизнес-проблему, которую нельзя оставлять без внимания.

Применяя прогнозный подход с количественными методами управления рисками, организации могут унифицировать свою стратегию кибербезопасности и получать прозрачность в реальном времени в своей среде, создавая платформу, которая улучшает их понимание финансовых рисков и способов передачи информации о них между внутренними и внешними заинтересованными сторонами.

Готовность к программам-вымогателям - это не только технические и кибернетические меры. Такой упреждающий подход к управлению рисками может помочь организациям лучше понять потенциальные финансовые последствия взлома, чтобы оценить необходимые шаги для уменьшения и уменьшения ущерба сейчас и в будущем». ***(SAKET MODI. Can You Predict the Likelihood of a Ransomware Attack? Yes, You Can // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/can-you-predict-the-likelihood-of-a-ransomware-attack-yes-you-can/). 16.11.2021).***

***

«Если ваша компания становится жертвой атаки программы-вымогателя, вы можете предположить, что эта атака является наихудшей из ваших организационных и финансовых проблем. Но рассматривали ли вы

возможность того, что ваше предприятие может дополнительно столкнуться с коллективным иском после атаки программы-вымогателя?

В наши дни этот риск увеличивается - и он определенно находится в поле зрения профессиональных юристов. Но предприятия, которые заранее готовятся к такому наихудшему сценарию, могут защитить себя от этого дополнительного слоя финансовых трудностей. Дело в том, что истцу в коллективном иске будет сложно выиграть мировое соглашение, если компания, на которую была направлена атака, была осторожна, внимательна и добросовестна, принимая все разумные меры предосторожности, которые она могла бы разумно предпринять для предотвращения атаки и восстановления после нее. Однако риск организации возрастает, если рассматриваемое предприятие небрежно использовало личные данные, которые были скомпрометированы, и это может быть доказано в суде.

Защитные меры

Агентство по кибербезопасности и безопасности инфраструктуры (входит в состав Министерства внутренней безопасности США) сообщило, что около 85 процентов атак с использованием программ-вымогателей можно полностью предотвратить, если компании соблюдают основные меры кибербезопасности. В нынешней благоприятной для взлома среде, когда атаки программ-вымогателей являются частью ежедневной ленты новостей, эти шаги не должны быть сложными, но многие предприятия оставляют эти уязвимости широко открытыми, не выполняя их:

Регулярное обновление операционных систем

Устранение известных уязвимостей программного обеспечения, ОС и приложений

Регулярное резервное копирование данных

Обучение сотрудников правилам, которые нужно искать в электронных письмах и ссылках

Ограничение административных прав для ОС и приложений

Блокирование запуска неавторизованных программ (так называемый «белый список» приложений)

Регулярное применение этих мер - лучший способ для предприятия, пострадавшего от программы-вымогателя, защитить себя от возможности подачи коллективного иска. Помимо обеспечения того, чтобы ваша компания инвестировала в превентивные меры, такие как решения для сетевой безопасности и восстановления, ИТ-отдел также должен регулярно документировать и проверять стратегию защиты данных компании. Также, возможно, стоит инвестировать в полис киберстрахования.

Исследования дают некоторое представление о количестве компаний, пренебрегающих передовыми практиками в области кибербезопасности. Например, когда дело доходит до обучения сотрудников распознаванию подозрительных электронных писем и ссылок, одно исследование показало, что только около трети компаний предлагают внутреннее обучение по угрозам, исходящим от программ-вымогателей. Исследование, проведенное Институтом Понемон, также выявило некоторые другие тревожные результаты:

Менее одной трети (29 процентов) опрошенных компаний были уверены, что их сотрудники заметят угрозы программ-вымогателей.

Менее половины опрошенных работодателей (46 процентов) заявили, что предотвращение программ-вымогателей является приоритетом компании, хотя более половины фактически уже стали жертвами атак программ-вымогателей.

Защищать PII клиента

Помните о том, что люди, которые, скорее всего, объединятся и подадут групповой иск, - это ваши клиенты, у которых есть основания полагать (или свидетельства этого факта), что ваша организация не смогла защитить их личную информацию, позволяющую установить личность (PII). Например, если хакер украл номера социального страхования и данные водительских прав, и достаточно людей было скомпрометировано, то нередко будет подан коллективный иск, если соответствующее предприятие не примет меры, перечисленные выше. Как и в случае коллективного иска публичной компании, если команда менеджеров не создает акционерной стоимости, компания станет главной целью для коллективных исков.

Какова вероятность того, что судебный процесс, связанный с программами-вымогателями, будет успешным? Очевидно, что если истец сможет доказать грубую халатность со стороны компании, возрастет вероятность того, что компании потребуется компенсация за компрометацию PII клиента. Но если ваша компания приняла надлежащие меры предосторожности в отношении кибербезопасности, задокументировала и проверила вашу стратегию, а также инвестировала в страхование от кибербезопасности, вы окажетесь в гораздо более привлекательном юридическом положении.

Также имейте в виду, что на карту поставлено больше, чем непосредственные финансовые последствия проигрыша коллективного иска; у такого костюма также есть потенциальные долгосрочные последствия.

В частности, вы можете столкнуться с проблемой восприятия клиентов, которая может повлиять на доходы компании, репутацию и лояльность клиентов на долгие годы.

Навигация и разработка надежной стратегии кибербезопасности является ключом к защите вашего предприятия от ряда негативных последствий, которые могут остаться после коллективного иска, связанного с программами-вымогателями. Найдите время, чтобы понять различные продукты и решения, которые могут помочь вам защитить, поддерживать и восстанавливать ваши данные и личную информацию ваших клиентов в случае утечки данных. Таким образом, у вас будет гораздо больше шансов доказать, что ваша компания приложила все усилия для защиты PII в меру своих возможностей». ***(MIHIR SHAH. Protecting Your Enterprise Against a Ransomware-Related Class Action Lawsuit // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/protecting-your-enterprise-against-a-ransomware-related-class-action-lawsuit/). 12.11.2021).***

***

«Недавние атаки программ-вымогателей доминировали в заголовках новостей в этом году. Согласно прогнозам, финансовый ущерб от программ-вымогателей может достигнуть 265 миллиардов долларов в мире к 2031 году. Это

означает, что кибератаки, нацеленные на предприятия и отдельных лиц, происходят со скоростью примерно одна атака каждые несколько секунд.

Средняя выплата выкупа производится бизнесом, чтобы восстановить данные после кибератаки составила $ 220 000 в первом квартале на 43% по сравнению с последним кварталом 2020 г. Cyberinsurance предназначен для защиты организаций против финансовых последствий кибератак. Это может сыграть роль как в действиях компании при атаке, так и в предотвращении атак в первую очередь. Угроза увеличения премий киберстрахования и более строгого контроля безопасности также играет важную роль в мотивации компаний укреплять свои системы безопасности.

Киберстрахование так же важно, как и медицинское страхование

Киберстрахование для бизнеса становится таким же необходимым, как и медицинское страхование для физических лиц. Некоторые предприятия, особенно мелкие, не хотят брать на себя расходы по страхованию в дополнение к расходам на улучшение своих протоколов безопасности. Однако безудержный рост кибератак продемонстрировал, что вопрос больше не в том, подвергнется ли компания атаке, а в том, когда - а это означает, что компании в конечном итоге не могут позволить себе отсутствие киберстрахования.

Когда атака неизбежно произойдет, компания столкнется с решением заплатить выкуп за расшифровку своих файлов или не платить. Если компания не застрахована, она часто обнаруживает, что не может заплатить выкуп, и, если может, сумма будет астрономически высокой.

Для компаний уже небезопасно отказываться от страховки, даже если у компании есть надежный план аварийного восстановления и она может восстановить большинство своих систем, не уплачивая выкуп. Преимущества киберстрахования выходят за рамки простого возмещения затрат на уплату выкупа, но также могут повысить вероятность восстановления данных и, например, защитить репутацию компании.

Пейзаж киберстрахования

Киберстраховщики анализируют данные, чтобы оценить, насколько рискованно страховать организацию. Однако эта оценка и моделирование рисков кибербезопасности стали более сложными после пандемии, включая переход к удаленной работе и сопутствующий рост удаленных систем. Кроме того, миграция в облако и внедрение новых технологий предоставили хакерам множество новых возможностей, изменив модели прогнозирования страховых рисков.

Страховщики осознают, что организации, которые не используют меры безопасности, такие как многофакторная аутентификация (MFA) и биометрия с привязкой к личности (IBB), подвергаются значительно большему риску атак. Стремясь снизить риск кибербезопасности, страховщики требуют от клиентов внедрения определенных мер безопасности, таких как MFA, и, в некоторых случаях, увеличивают премии для тех, кто не внедряет эти меры. MFA требует от конечных пользователей предоставления двух или более факторов проверки и является дополнительным уровнем безопасности поверх одного фактора, такого как пароль. Он часто включает в себя личный идентификационный номер или пароль, созданный

пользователем, а также внешнюю проверку, такую как телефонный или аппаратный токен.

Страховщики вводят более строгие квалификационные требования, поскольку динамика кибербезопасности изменилась. Это похоже на то, как поставщик медицинского страхования меняет свой список требований, таких как списки ранее существовавших заболеваний, и насколько он строг в том, что он покрывает, потому что динамика здоровья его застрахованного населения изменилась.

Что нужно иметь в виду

Для компаний, у которых уже есть страховка, проверьте свой полис и будьте готовы к продлению и изменениям:

Организации должны проверить свои политики и обратить особое внимание на то, что происходит в случае атаки программы-вымогателя. Им также следует посмотреть, какие условия и какие изменения в полисе страховщик может попытаться внести при продлении полиса.

Компании, которые имели страховку до пандемии или обеспечили страховое покрытие во время пандемии, должны спланировать свое продление и убедиться, что они соблюдают предлагаемые протоколы безопасности. Компании могут получить предупреждение об обновлении протоколов безопасности к следующему году.

К сожалению, обновления систем безопасности - это не те изменения, которые компании могут внести в одночасье. Организации должны иметь план проекта, чтобы установить эти меры безопасности. Страховщики не будут давать компаниям план внедрения этих протоколов безопасности, поэтому организации должны быть готовы сделать это самостоятельно.

Для организаций, впервые приобретающих страховку:

Компаниям следует внимательно изучить детали потенциальной политики и убедиться, что условия и требования соответствуют их потребностям. Обратите особое внимание на требования к ответу на восстановление и требования к резервному копированию данных, а также на требования к получению оплаты по претензиям в случае нарушения.

Сбор данных после взлома может быть сложной задачей, и организациям часто приходится доказывать влияние взлома или доказывать, что оно соответствует требованиям в отношении ожидаемых мер безопасности. Это похоже на медицинское страхование, когда пациенты доказывают, что они соответствуют требованиям для лечения, а если они не могут предоставить доказательства, они должны платить из своего кармана. Когда страховщики ужесточают требования безопасности, они часто также ужесточают требования к выплате. Страховщики требуют доказательств того, что инцидент действительно подпадает под их политику киберстрахования и что это действительно покрывается страховкой.

Оценка рисков жизненно важна

Оценка рисков - это стандартная основа, которую должна иметь любая организация, прежде чем внедрять меры безопасности и покупать страховку. Оценка риска покажет, где организация наиболее уязвима и, следовательно, имеет наибольший риск. Организации должны провести полную инвентаризацию данных и активов, чтобы оценить свой уровень готовности и определить, где находится наибольший риск.

Оценка сторонних рисков - еще одна важная область, на которую следует обратить внимание, поскольку сторонние нарушения растут. Рассмотрим историю SolarWinds, которая продемонстрировала, как атака на системы одной компании повлияла на другие.

Киберпреступники смогли проникнуть в компании, расположенные ниже по цепочке, взломав программный код до его распространения среди клиентов и партнеров SolarWinds. CISA пояснила, что, хотя фактическое количество клиентов, которые были взломаны с помощью Sunburst, было менее 100, компании должны понимать, что они наследуют риск кибербезопасности от поставщиков, с которыми они работают.

Организациям также следует не забывать проводить полную стороннюю оценку рисков своих потенциальных страховщиков, внимательно изучая их уровень риска. Киберстраховщики также сами могут быть объектами атак, и, если страховщик будет взломан и хакеры узнают подробности страхового плана компании, они могут не только пометить их как цель, но и указать хакеру, сколько выкупа требуется.

Киберстрахование - это только одна часть головоломки

Как только организации поймут, в чем заключаются их риски, они могут внедрить эффективные меры безопасности, такие как MFA, для снижения риска возникновения атак. Компании не должны ждать, пока страховщики потребуют от них внедрить эти протоколы, и должны активно внедрять их, чтобы снизить свои шансы подвергнуться атаке.

Атаки неизбежны, и если организации не оценят свой риск, не купят киберстрахование и не примут более строгие меры безопасности, они столкнутся с серьезными проблемами при атаке. Компаниям следует проявлять инициативу в устранении рисков кибербезопасности, проявлять должную осмотрительность при проверке политик и требований киберстрахования и обновлять свои протоколы безопасности до того, как это потребуется. Хорошо подготовленные организации принимают меры как для предотвращения атак, так и для уменьшения ущерба, когда атаки неизбежно происходят». ***(Kimberly Johnson. Are Cyber Insurers Cybersecurity's New Enforcers? // Techstrong Group Inc. (https://securityboulevard.com/2021/11/are-cyber-insurers-cybersecuritys-new-enforcers/). 12.11.2021).***

***

«Более половины опрошенных ИТ-специалистов заявили, что их организация пострадала от атаки программ-вымогателей в сфере здравоохранения. Но 61 процент опрошенных потенциальных пациентов заявили, что они не слышали о каких-либо кибератаках в сфере здравоохранения за последние 24 месяца, как показало новое исследование, проведенное Censuswide от имени Armis.

Опрос, в который вошли ответы 2000 потенциальных пациентов и 400 ИТ-специалистов в области здравоохранения, выявил резкое несоответствие между представлениями пациентов о рисках программ-вымогателей и серьезной угрозой, которую программы-вымогатели фактически представляют для сектора здравоохранения.

Атаки программ-вымогателей увеличились в объеме и серьезности в секторе здравоохранения за последние несколько лет и могут привести к простоям EHR, переадресации скорой помощи и отмене приема на прием. В некоторых редких случаях смерть пациентов напрямую связана с атаками программ-вымогателей.

Более 80% опрошенных ИТ-специалистов согласились с тем, что за последние 12 месяцев они заметили повышенный киберриск. Банды программ-вымогателей становятся все более изощренными, а поразительные пробелы в безопасности медицинских устройств выявили дополнительные уязвимости и расширили поверхность и масштабы атак.

Треть потенциальных пациентов-респондентов заявили, что они стали жертвой кибератаки в сфере здравоохранения, а половина пациентов заявили, что они поменяли бы больницу, если бы их медицинская организация пострадала от атаки вымогателя.

Представления пациентов о безопасности данных сильно различались. В то время как более 65 процентов потенциальных пациентов сообщили, что верят, что их поставщик медицинских услуг делает достаточно для защиты их личной информации, треть респондентов заявили, что они доверяют своим лучшим друзьям больше, чем своим поставщикам медицинских услуг, в отношении конфиденциальной медицинской информации.

Но, учитывая текущую картину угроз, более вероятно, что медицинская организация столкнулась с программами-вымогателями или другими угрозами безопасности. Разрыв между восприятием пациента и пониманием ИТ-специалистов показывает, что большинство пациентов могут не осознавать масштабы киберугроз в сфере здравоохранения.

Исследование Армиса показало, что ИТ-специалистов больше всего беспокоят утечки данных, приводящие к потере конфиденциальной информации о пациентах. Половина респондентов заявили, что риски безопасности в инфраструктуре больницы возглавляют их список проблем, за которыми следует риск размещения информации о пациенте на онлайн-портале и пребывания в больничной палате с несколькими подключенными медицинскими устройствами.

ИТ-специалисты выразили серьезную озабоченность по поводу безопасности систем отопления, вентиляции и кондиционирования воздуха и электрических систем, машин для визуализации, оборудования для выдачи лекарств, киосков регистрации и оборудования для контроля жизненно важных функций. Несмотря на эти опасения, 95 процентов опрошенных ИТ-специалистов заявили, что полагают, что подключенные устройства их организации имеют последнее программное обеспечение.

Три четверти ИТ-специалистов заявили, что недавние кибератаки оказали сильное влияние на принятие решений в отношении кибербезопасности в их организациях, и чуть более половины респондентов считают, что их организация выделяет более чем достаточно средств для защиты своих ИТ-систем.

Несмотря на эти улучшения, более 60 процентов респондентов заявили, что организация еще не подавала иски о страховании от киберпространства, несмотря на рост атак в отрасли. По мере того, как поверхность и область атаки продолжают расширяться, медицинские организации должны убедиться, что они внедрили

надлежащие меры безопасности для снижения риска». ***(Jill McKeon. Most Patients Unaware of the Magnitude Healthcare Ransomware Attacks // TechTarget, Inc. (https://healthitsecurity.com/news/most-patients-unaware-of-the-magnitude-healthcare-ransomware-attacks). 10.11.2021).***

***

«Преступники используют программы-вымогатели в качестве оружия, чтобы нанести ущерб кибербезопасности предприятий или стран и получить важную информацию. Поскольку США - одна из самых могущественных стран, они являются идеальной целью для кибератак.

Согласно недавним выводам команды Atlas VPN, более 60% глобальных атак программ-вымогателей направлены на США и Великобританию. Кроме того, большинство атак нацелены на правительственные администрации, намеревающиеся украсть конфиденциальную информацию, принадлежащую государству.

Данные основаны на отчете «Состояние программ-вымогателей в 2021 году», опубликованном Black Fog. Он охватывает атаки программ-вымогателей с начала года до конца октября.

По состоянию на октябрь 2021 года 52% всех атак программ-вымогателей в мире нацелены на США. В этом году хакеры предприняли самые масштабные кибератаки именно на предприятия США. Colonial Pipeline, JBS Foods, Kaseya - это лишь некоторые из самых крупных примеров. Атаки программ-вымогателей обходятся компаниям в миллионы долларов и нехватку поставок на несколько недель.

Около 11% хакерских атак программ-вымогателей направлены на британские предприятия. В октябре прошлого года произошел масштабный взлом британского ювелира Graff. Преступная группировка Конти слила 69000 конфиденциальных документов, касающихся таких знаменитостей, как Дональд Трамп, Опра Уинфри, Дэвид Бекхэм и других. Группа потребовала выкуп, чтобы прекратить дальнейшее распространение информации.

Канадские компании пострадали от 4,51% всех атак с использованием программ-вымогателей в мире. Еще в феврале банда вымогателей DarkSide поразила одно из крупнейших канадских агентств по аренде автомобилей Discount Car and Truck Rental. Киберпреступники разместили на сайте утечки уведомление о том, что они украли у компании 120 ГБ корпоративных, банковских данных и данных о франшизе.

С другой стороны, Франция и Япония стали объектами примерно 3% атак программ-вымогателей. На бразильские, индийские и австралийские компании приходилось по 2% атак программ-вымогателей во всем мире. Почти 21% атак программ-вымогателей были направлены на остальной мир.

Правительство под давлением программ-вымогателей

Атака программы-вымогателя может стать худшим кошмаром для организации. Хакеры специально выбирают отрасли и компании, в которых потеря данных может нанести ущерб его успешной деятельности.

На сегодняшний день наибольшее количество атак с использованием программ-вымогателей в 2021 году пострадало от правительственных администраций - 47. Устаревшие технологии и нехватка специалистов по кибербезопасности делают правительства уязвимыми для атак. Киберпреступники знают, что правительства владеют конфиденциальной информацией, которая имеет важное значение для государственной службы.

В этом году в сфере образования во всем мире произошло 35 атак с использованием программ-вымогателей. Взаимосвязанные сети в образовательных учреждениях обычно помогают быстрее распространять программы-вымогатели, нанося больший ущерб. Хотя учащиеся участвуют во многих онлайн-действиях, их легче использовать в качестве входа в сеть для программ-вымогателей.

Киберпреступники осуществили 33 атаки программ-вымогателей на медицинские учреждения. Больницы являются прибыльной целью для хакеров, поскольку они хранят конфиденциальные данные пациентов, такие как номера социального страхования и другую личную информацию. Взяв под контроль больничные системы, хакеры подвергают опасности жизни многих людей.

В этом году сфера услуг пострадала от 28 атак программ-вымогателей. Обычно компании, работающие в сфере услуг, хранят много личной информации о своих клиентах. В результате сервисные компании становятся привлекательными целями для хакеров, которые получат прибыль либо от выкупа, либо от продажи украденных данных.

Программы-вымогатели продолжают оставаться одной из самых опасных киберугроз для предприятий и правительств. В то время как компании и власти пытаются догнать технологии киберзащиты, киберпреступные атаки становятся все более изощренными и разрушительными». ***(William S. Over 60% of global ransomware attacks are directed at the US and UK // AtlasVPN (https://atlasvpn.com/blog/over-60-of-global-ransomware-attacks-are-directed-at-the-us-and-uk). 10.11.2021).***

***

«Кибербезопасность была в центре внимания на протяжении 2021 года после серии атак программ-вымогателей на крупные промышленные, коммунальные и потребительские объекты, и новые данные показывают, насколько распространена проблема.

В исследовании, опубликованном NordLocker в конце октября, были собраны доступные глобальные данные об инцидентах с программами-вымогателями с начала 2021 года и разбиты по отраслям.

В отчете NordLocker указано 35 отраслей, которые подверглись наибольшему количеству атак, и строительство возглавило их с 93. Обрабатывающая промышленность заняла второе место с 86, за ним следуют финансы (69), здравоохранение (65) и образование (63) в первой пятерке. Технологии / ИТ (62), логистика / транспорт (59), автомобилестроение (56), коммунальные услуги (52) и юриспруденция замыкают первую десятку.

Исследование NordLocker также показало, что колоссальные 37% компаний по всему миру пострадали от программ-вымогателей в течение 2020 года, и, учитывая

широкий спектр задействованных отраслей и размеров компаний, поставщик услуг VPN подчеркнул, что ни один бизнес или учреждение не может чувствовать себя защищенным от этой угрозы.

Другие заметки из исследования NordLocker:

Средняя общая стоимость восстановления после атаки программы-вымогателя выросла с 761000 долларов в 2020 году до 1,85 миллиона долларов на момент публикации отчета NordLocker.

Группой вымогателей, ответственной за наибольшее количество атак с начала 2020 года, была Conti, к которой с начала 2020 года приписали 450 атак. За ними следуют REvil (210), DopplePaymer (200) и PYSA (188).

Наиболее атакованными странами являются США (732 случая), Великобритания (74), Канада (62), Франция (58) и Германия (39).

Большинство банд вымогателей действуют на постсоветском пространстве». ***(Mike Hockett. Top Industries Attacked by Ransomware Include Manufacturing, Construction [Report] // Thomas Publishing Company (https://www.thomasnet.com/insights/top-industries-attacked-by-ransomware-include-manufacturing-construction-report/). 17.11.2021).***

***

«Атаки программ-вымогателей являются одними из самых серьезных киберугроз, с которыми сегодня сталкиваются организации. Согласно исследованию Gartner, программы-вымогатели являются наивысшим приоритетом (78 процентов) и наиболее важными возникающими рисками, которые необходимо отслеживать. Тем не менее, организации все еще не знают, где и как начать защищаться от злоумышленников.

CISA, NIST и многие другие делятся общими руководящими принципами о том, как организациям следует защищаться от программ-вымогателей, но их часто можно свести к «исправлению всего». Вместо этого необходимо сосредоточить внимание на реальных действиях, которые приведут к снижению реального риска и улучшению понимания различных методов, используемых злоумышленниками.

Сделать первый шаг

Упреждающий подход необходим в сегодняшней быстро развивающейся и сложной ИТ-среде. Итак, с чего начать?

Инвентаризация активов - это список всех корпоративных ИТ-активов, существующих в сети. Все они содержат программное обеспечение, которое в любой момент может быть уязвимо для атаки. Без списка, который дает целостное представление об окружающей среде, невозможно опередить злоумышленников. В конце концов, вы не можете защитить то, чего не видите.

Этот процесс должен быть автоматизированным и непрерывным, а не полагаться на ручное специальное сканирование, которое может легко упасть на дно кучи. Такие инструменты, как QualysCyberSecurity Asset Management (CSAM), предоставляют обзор известных и, что более важно, неизвестных активов в вашей среде, а также наличие каких-либо известных рисков, связанных с каждым активом.

После того, как инвентаризация создана, пора оценить текущий уровень риска. Это включает в себя поиск актуальных проблем. Например, согласно недавнему

исследованию Qualys, существует 110 записей о распространенных уязвимостях и уязвимостях (CVE), которые были связаны с программами-вымогателями за последние пять лет. С помощью этого списка организации могут получить полную картину этих CVE, если они присутствуют в среде, и какие из CVE должны быть приоритетными при установке исправлений.

Организации могут дополнять свои данные об активах и программном обеспечении контекстной информацией, чтобы облегчить процесс обнаружения. Например, они могут идентифицировать и устанавливать предупреждения для активов, на которых запущено неавторизованное программное обеспечение или не используются антивирусные программы или средства защиты конечных точек. Эти проблемы можно изучить и принять соответствующие меры для их решения.

Приоритеты и общая картина

При таком большом количестве потенциальных рисков в сегодняшнем ландшафте безопасности важно понимать, как расставить приоритеты.

На практике не все риски равны. Могут быть обнаружены тысячи проблем, некоторые из которых необходимо будет устранить немедленно, но другие могут оказаться исключительно нишевыми или трудными для использования. Имея возможность добавлять бизнес-контекст к активам, организации могут сосредоточиться на наиболее критических рисках для своего бизнеса и позволить управлять теми, которые находятся ниже в списке, с течением времени.

Само исправление часто упускается из виду как важная часть этого процесса, обычно потому, что оно выходит за рамки границ команды и отдела, что в конечном итоге приводит к конфликтам или задержкам. Чтобы решить эту проблему, организации должны внедрить метрики, которые могут отслеживать успешные развертывания, и сделать их обязанностью бизнеса, а не только ИТ-групп.

Программы-вымогатели - это не проблема безопасности, это проблема бизнеса

Затраты и нарушение бизнеса в результате атаки программ-вымогателей привели к улучшению поддержки и увеличению бюджета для групп безопасности. Однако увеличения бюджета безопасности или инвестирования в дополнительные инструменты недостаточно. Gartner прогнозирует, что к 2025 году 40 процентов советов директоров назначат специальный комитет по кибербезопасности (по сравнению с 10 процентами). В рамках этого бизнес-команды захотят увидеть значительные улучшения в обеспечении безопасности корпоративной среды.

Некоторые организации уже проделали этот путь, но многие все еще отстают, несмотря на возрастающие угрозы. Специалисты по безопасности могут активизировать свои усилия, обучаясь друг у друга и следя за развитием отрасли, чтобы услышать передовой опыт и понять ценность новых технологических достижений.

В этом году на ежегодной конференции Qualys Security Conference, которая состоится 15-18 ноября в Лас-Вегасе и в Интернете, участники услышат от клиентов, отраслевых практиков и экспертов Qualys о том, как создать свой учебник по программам-вымогателям, чтобы защитить себя от современных атак и изощренных злоумышленников.

Наряду с основными докладами Криса Кребса, бывшего директора CISA, и Сумеда Такара, генерального директора Qualys, мероприятие будет посвящено

изучению роли безопасности в цифровых проектах и тому, как встроить автоматизацию безопасности от конечных точек до центра обработки данных и облака.

Ключевые сессии будут охватывать инвентаризацию активов, исправление с использованием контекста угроз, обнаружение и реагирование с использованием контекста предотвращения, а также оптимизацию управления соответствием». ***(Paul Baird. Designing a Proactive Ransomware Playbook for Today's Threat Landscape // Threatpost (https://threatpost.com/proactive-ransomware-playbook-threat-landscape/176224/). 11.11.2021).***

***

«Если вы похожи на большинство ИТ-специалистов, угроза атаки программы-вымогателя может не дать вам спать по ночам. И у вас есть веская причина для беспокойства - программы-вымогатели не делают различий. Организации во всех отраслях, государственных или частных, являются потенциальными жертвами, если они еще не были жертвами.

Фактически, недавнее исследование Veritas Technologies показывает, что в среднем в организации было 2,57 атак с использованием программ-вымогателей, которые привели к значительным простоям за последние 12 месяцев, при этом 10% из них испытали простои, которые повлияли на бизнес более чем в пять раз.

Хотя программы-вымогатели могут нанести серьезный ущерб вашему бизнесу и репутации, они не являются непобедимыми. Фактически, он настолько силен, насколько сильное звено вашей организации. Хорошая новость заключается в том, что ваша организация может предпринять четкие шаги, чтобы не стать целью киберпреступности и снизить вероятность того, что атака может разрушить ваш бизнес.

Давайте рассмотрим 10 наиболее эффективных передовых методов, которые вы можете реализовать сегодня, чтобы защитить свои данные и обеспечить устойчивость бизнеса.

1. Оперативное обновление систем и обновлений программного обеспечения

Использование устаревшего программного обеспечения может позволить злоумышленникам использовать явные уязвимости системы безопасности. Чтобы уменьшить вероятность атаки, регулярно обновляйте и обновляйте всю инфраструктуру, операционные системы и программные приложения. Также важно обновить приложение резервного копирования. Не сражайтесь с сегодняшними программами-вымогателями с помощью вчерашних технологий.

2. Реализуйте правило резервного копирования 3-2-1-1.

Если вы часто выполняете резервное копирование данных, системных образов и конфигураций, у вас всегда будет актуальное место для возобновления операций, если программа-вымогатель все-таки нанесет удар. А еще лучше сделать еще один шаг и избежать единой точки отказа, рассредоточив данные с помощью правила резервного копирования 3-2-1.

Это означает хранение трех или более копий в разных местах, использование двух разных носителей и хранение одной копии за пределами предприятия. Это уменьшит шансы злоумышленника получить доступ ко всему. Такой подход 3-2-1

также гарантирует, что уязвимость в одной из этих копий не скомпрометирует все ваши копии, и предоставляет варианты, если атака затрагивает весь центр обработки данных.

Многие организации теперь делают еще один шаг к 3-2-1-1, сохраняя по крайней мере одну копию в неизменяемом (не может быть изменен) и нестираемом (не может быть удален) хранилище.

3. Реализуйте модель нулевого доверия.

Модель нулевого доверия - это образ мышления, который фокусируется на том, чтобы не доверять никаким устройствам - или пользователям - даже если они по умолчанию находятся внутри корпоративной сети.

Вместо того, чтобы просто запрашивать пароль (да, даже если он длинный и сложный), также требуются многофакторная аутентификация (MFA) и управление доступом на основе ролей (RBAC), отслеживание и смягчение вредоносной активности, а также шифрование данных на лету. и в состоянии покоя, что делает исключенные данные непригодными для использования.

Он гарантирует, что громко и открыто сообщайте, что вы никогда не должны нигде использовать заводские пароли.

Кроме того, если вы ограничите доступ к резервным копиям, вы отключите наиболее распространенный метод входа для программ-вымогателей. Многие организации переходят к практике обеспечения безопасности «точно в срок» (JIT), когда доступ предоставляется по мере необходимости или на заранее определенный период времени, что необходимо учитывать для критически важных для бизнеса данных.

4. Сегментация сети

Злоумышленники любят единую непрерывную плоскую сеть. Это означает, что они могут легко распространяться по всей вашей инфраструктуре.

Эффективный способ остановить злоумышленников и значительно уменьшить их поверхность атаки - это сегментация сети и микросегментация. В этой модели сети делятся на несколько зон меньших сетей, а доступ управляется и ограничивается, особенно для наиболее важных данных.

Также распространенной практикой является отключение от Интернета наиболее важных функций инфраструктуры. Кроме того, в рамках модели нулевого доверия вашей компании рассмотрите возможность сегментирования сторонних поставщиков, поскольку было много заметных атак на цепочки поставок в результате неправильного управления поставщиками. Хак Sunburst и Colonial нападение трубопровода две большие примеры.

5. Видимость конечной точки

В большинстве организаций отсутствует видимость удаленных конечных точек. В настоящее время стало обычной практикой для злоумышленников обходить передовую охрану и зависать - оставаться в бездействии достаточно долго, чтобы обнаружить слабые места и найти подходящий момент для атаки. Крайне важно, чтобы вы внедрили инструменты, которые обеспечивают полную видимость всей вашей среды, обнаруживают аномалии, а также выявляют и предупреждают вас о злонамеренных действиях в вашей сети, не давая вымогателям возможности

спрятаться. Это поможет вам уменьшить как угрозы, так и уязвимости, прежде чем злоумышленники получат возможность принять меры.

6. Неизменяемое и несмываемое хранение

Как упоминалось ранее, один из лучших способов защитить ваши данные от программ-вымогателей - реализовать неизменяемое и нестираемое хранилище, которое гарантирует, что данные не могут быть изменены, зашифрованы или удалены в течение определенного периода времени. Однако в наши дни термин «неизменяемое хранилище» стал модным словечком среди поставщиков резервного копирования. Ищите неизменяемость, которая не только логична, но также включает физическую неизменность, и важно включать встроенные уровни безопасности.

Индустрия движется к двум типам неизменности. В Veritas мы называем их режимом предприятия и режимом соответствия. Режим предприятия известен как подход «четырех глаз» - это означает, что вам нужны две пары глаз для проверки любых изменений. Например, первая пара глаз - это глаза администратора резервного копирования, а вторая пара глаз - администратора безопасности. Без одобрения обоих вариантов внесение изменений невозможно. Режим соответствия относится к неизменяемой неизменности, то есть к данным, которые нельзя изменить ни при каких обстоятельствах. Оба режима включают часы соответствия, которые полностью независимы от ОС, так что если часы ОС подделаны, это не повлияет на выпуск данных.

7. Быстрое восстановление

Большинство злоумышленников надеются на две вещи: время для распространения атаки; и деньги (от вас), чтобы остановить это. Исторически восстановление могло занимать недели или даже месяцы, когда это был чрезвычайно ручной и трудоемкий процесс, охватывающий несколько заинтересованных сторон внутри организации. Теперь восстановление можно организовать и автоматизировать с помощью гибких и альтернативных вариантов, таких как быстрое включение центра обработки данных в провайдера общедоступного облака, что может сократить время простоя и предоставить альтернативы уплате выкупа. При наличии правильных систем время восстановления может быть сокращено до секунд, если это необходимо.

8. Регулярное тестирование и проверка.

Создание комплексного плана защиты данных не означает, что ваша работа закончена. Тестирование гарантирует, что ваш план будет работать тогда, когда он вам понадобится. И хотя первоначальное тестирование может подтвердить, что все аспекты плана действительно работают, очень важно проводить регулярное тестирование, потому что ИТ-среда постоянно меняется.

Важно отметить, что любой план хорош настолько, насколько хорош в последний раз, и если вы не протестируете его, то нет никакой гарантии, что вы сможете быстро восстановиться! Также жизненно важно внедрять решения, которые тестируют в изолированной среде восстановления или изолированной среде без прерывания работы.

9. Образованные сотрудники

Общеизвестно, что сотрудники часто становятся воротами для атаки. Не обвиняйте своих сотрудников - ошибки случаются. Современные фишинговые атаки

и социальная инженерия настолько развиты, что часто обманывают специалистов по безопасности.

Вместо этого сосредоточьтесь на обучении сотрудников выявлению тактик фишинга и социальной инженерии; создавать надежные пароли; просматривать безопасно; использовать MFA; и всегда используйте безопасные VPN, а не общедоступный Wi-Fi. Также убедитесь, что сотрудники знают, что делать и кого предупреждать, если они станут жертвами.

10. Пособия по кибератакам

Представьте себе, если бы все в вашей организации точно знали, что и когда делать перед лицом атаки программы-вымогателя. В этом нет ничего невозможного, если вы создадите стандартную книгу действий для кибератак, которая проясняет роли, а также объединяет и расширяет возможности кросс-функциональных команд с четкими путями связи и протоколами реагирования в случае чрезвычайных ситуаций.

Отличный совет - настроить канал экстренной связи в защищенном приложении для обмена текстовыми сообщениями, чтобы высшее руководство вашей организации могло общаться в случае кибератаки, поскольку в результате атаки могут быть отключены корпоративная электронная почта или системы чата. Также неплохо нанять стороннее агентство для аудита стратегии вашей команды и проверки вашей работы.

У вас есть возможность предпринять важные шаги для борьбы с программами-вымогателями и изменить положение киберпреступников. Составив многоуровневую стратегию устойчивости к программам-вымогателям, которая включает в себя приведенные выше передовые практики и безупречную гигиену кибербезопасности, вы можете остановить злоумышленников до того, как они закрепятся». ***(Sonya Duffin. Top 10 Cybersecurity Best Practices to Combat Ransomware // Threatpost (https://threatpost.com/cybersecurity-best-practices-ransomware/176316/). 12.11.2021).***

***

«Кибервымогательская группировка Pysa (другое название Mespinoza) одновременно выложила на своем сайте утечек десятки жертв, сразу после того, как правительство США объявило о принятии ряда мер против кибервымогательских группировок.

В настоящее время на сайте утечек Pysa представлено 50 компаний, университетов и организаций. Однако у многих специалистов истинное время осуществления атак вызывает вопросы, поскольку Pysa обычно добавляет жертв на свой сайт через некоторое время после атаки.

Как сообщил изданию ZDNet эксперт в области вымогательского ПО ИБ-компании Recorded Future Аллан Лиска (Allan Liska), скорее всего, не все опубликованные на сайте жертвы являются новыми.

«Они (участники Pysa - ред.) публикуют данные жертв через шесть, а то и больше месяцев после первоначальной атаки. Это могут быть все жертвы, у которых они похитили и опубликовали данные, но их однозначно больше, чем мы наблюдали

в другие периоды нынешнего года. Множество разных организаций по всему миру, без какой-либо темы», - сообщил Лиска.

Мнение коллеги поддерживает аналитик ИБ-компании Emsisoft Бретт Кэллоу (Brett Callow). По его словам, Pysa раскрывает имена своих жертв через несколько недель или даже месяцев после атаки, что отличает ее от других кибервымогательских группировок.

Почему вымогатели ждали так долго, прежде чем опубликовать данные своих жертв, непонятно. Также неясно, почему вдруг они решили разом выложить столько информации.

В последнее время правительство США сотрудничает с Европолом, Евроюстом, Интерполом и другими правоохранительными органами в борьбе с кибервымогательскими группировками. В рамках операции GoldDust за последние шесть месяцев был ликвидирован целый ряд кибревымогательских группировок. В операции приняли участие 17 стран мира, и в Европе были арестованы десятки человек, подозреваемых в связях с кибервымогателями. В частности, совместными усилиями была захвачена инфраструктуры REvil, в результате чего группировке пришлось "прикрыть лавочку" во второй раз.

И Кэллоу, и Лиска отмечают, что публикация группировкой Pysa данных атакованных организаций оказалась весьма неожиданной, учитывая, какие меры принимают правоохранительные органы.

«Ничего другого не остается, как только предположить, что они сделали это в ответ на новости о REvil с целью либо показать властям средний палец, либо продемонстрировать уверенность в себе на случай, если их партнеры вдруг начнут идти на попятную», - пояснил Кэллоу». ***(Вымогатели Pysa показали «средний палец» правоохранителям // SecurityLab.ru (https://www.securitylab.ru/news/526547.php). 15.11.2021).***

***

«Неудивительно, что наше последнее исследование кибербезопасности показывает, что университеты считают программы-вымогатели главной угрозой в этом году. Наблюдался огромный всплеск атак этого типа на наш сектор, при этом количество инцидентов в первой половине 2021 года превысило общее количество за весь 2020 год. кибератака, но когда.

Jisc и партнерские агентства, включая Национальный центр кибербезопасности, в течение некоторого времени консультировали поставщиков высшего образования о том, как защитить себя. Несмотря на это, разрушительные атаки продолжаются - системы выходят из строя, данные теряются, а уровень стресса для сотрудников и студентов резко возрастает. Восстановление может занять несколько месяцев и стоить миллионы.

Жизненно важно, чтобы мы работали вместе, чтобы снизить риски и укрепить безопасность, и очень важно, чтобы в этом участвовали руководители высшего звена. Роль Jisc заключается в предоставлении информации об угрозах и руководстве, а также в защите национальной исследовательской и образовательной сети Janet, на которую полагаются наши участники.

Вице-канцлеры и советы директоров несут ответственность за обеспечение защиты киберпространств в своих учреждениях, но наш опрос показывает, что не все руководители высшего звена настолько вовлечены, насколько им необходимо.

Хотя 86 процентов высших учебных заведений (ВУЗов) регулярно отчитываются о рисках кибербезопасности и устойчивости перед своим исполнительным советом, и примерно такой же процент сообщает, что кибербезопасность является стратегическим приоритетом в их университете, это по-прежнему оставляет значительное меньшинство, если это не так.

Маловероятно, что у этих организаций будут достаточно надежные процессы и технические решения, чтобы остановить или смягчить атаку, когда она произойдет, и очень маловероятно, что у них будут планы восстановления.

Для этой проблемы нет серебряной пули. Снижение риска многослойно и требует ряда вмешательств. Нам нужна постоянная государственная поддержка критически важной инфраструктуры, финансовые вложения сектора в специалистов и услуги, а также руководство со стороны старших команд, чтобы создать условия, позволяющие изменениям происходить в их учреждениях.

Учитывая финансовые последствия пандемии, инвестиции будут проблемой, но они, вероятно, будут значительно дешевле, чем разрушительные последствия значительного и устойчивого сбоя системы и / или утечки данных.

Нет сомнений в том, что набор квалифицированного персонала в области безопасности и ИТ затруднен из-за нехватки технических навыков в Великобритании. В то время как правительство решает проблему нехватки навыков несколькими способами, включая развертывание бесплатных курсов по предметам STEM, таким как кибербезопасность, государственный сектор не может легко конкурировать с гораздо более высокими зарплатами, предлагаемыми коммерческими организациями.

Политика удаленной или гибридной работы поможет расширить круг кандидатов за пределы географических границ, но привлечение и удержание нужных людей останется проблемой для сектора.

Университеты могут предпринять эффективные шаги, чтобы защитить себя с точки зрения процессов и услуг. Мы призываем все старшие команды взаимодействовать со своими технологическими лидерами, чтобы убедиться, что эти вещи происходят в их учреждениях, отмечая, что для их реализации вполне могут потребоваться значительные инвестиции:

Управление уязвимостями и процедуры установки исправлений важны для всех систем, при этом приоритет отдается критически важным и доступным извне службам.

Сегментирование и изоляция всей критически важной сервисной инфраструктуры помогает предотвратить переход злоумышленников к одной системе к другим.

Внедрение раздельного централизованного ведения журнала и мониторинга критически важных систем позволяет заранее предупреждать о потенциальных проблемах и помогает в расследовании инцидентов.

Обеспечение сегментации, защиты и регулярного тестирования резервных копий имеет первостепенное значение, как и частое повторение планов и процедур

реагирования на инциденты. Практика не сделает безопасность идеальной, но она гарантирует, что ваш ответ в случае атаки будет эффективным, и вы сможете как можно быстрее восстановиться.

Контроль доступа к системе тоже жизненно важен. Он должен быть только у тех, кому нужен доступ. Многофакторная аутентификация (MFA) играет важную роль в более широком контроле доступа к системе и, следовательно, снижает риск успешной атаки программы-вымогателя.

Во время пандемии произошло резкое увеличение количества развертываний MFA, но это еще не все. Мы рекомендуем развернуть его во всех системах, всем сотрудникам и всем учащимся. Наше исследование показывает, что 87% вузов в настоящее время внедряют МИД для некоторых или всех сотрудников (рост на 15% в 2020 г.), а в 49% - для некоторых или всех студентов (рост на 27% по сравнению с 2020 г.).

Точно так же обучение по вопросам безопасности является ключевым инструментом в предотвращении инцидентов безопасности, вызванных фишингом и другими «человеческими ошибками», которые в исследовании признаются второй и третьей по значимости угрозой в этом году после программ-вымогателей.

Чтобы способствовать обмену знаниями и их поддержанию, мы выступаем за обязательное обучение для всех. Опрос показывает, что это область возможностей для сектора: 73% университетов проводят обязательную подготовку персонала, но только 9% настаивают на прохождении студентами курса.

Продолжая тенденцию последних пяти лет, восприятие защиты кибербезопасности в вузах невысокое: только 17% (16 из 93 респондентов) оценили себя на 8 или более баллов из 10. Средний балл составляет 6,3.

Итак, хотя последние статистические данные показывают, что траектория движется в правильном направлении, мы считаем, что, как и многие из вас, можно было бы сделать больше. И Джиск здесь, чтобы помочь». ***(Heidi Fraser-Kraus. Cybersecurity remains a critical issue that universities must face // Times Higher Education (https://www.timeshighereducation.com/campus/cybersecurity-remains-critical-issue-universities-must-face). 09.11.2021).***

***

«Программы-вымогатели популярны среди киберпреступников, потому что они эффективны и приносят настолько большую прибыль, что появился новый бренд атак программ-вымогателей «большой игры». Основываясь на данных с конечных точек WatchGuard, наша лаборатория ожидает, что к 2021 году количество вымогателей увеличится как минимум до 150% от общего количества 2020 года. Что еще хуже, мы также стали свидетелями роста изощренности и профессионализма программ-вымогателей (наряду с их значительным увеличением).

Этот более изощренный вымогатель «большой игры» связан с увеличением количества целевых атак, направленных на крупные компании и организации, у которых есть критические требования к времени безотказной работы - в таких секторах, как здравоохранение, правительство, производство, образование и поставщики управляемых услуг (MSP). Более того, киберпреступники применяют

новые формы шантажа. Теперь они также извлекают данные и вымогают у жертв, публикуя их на форумах в темной сети, что они называют «двойным вымогательством». Некоторые группы даже практикуют «тройное вымогательство», извлекая данные о клиентах жертвы и преследуя этих клиентов напрямую.

Добавьте к этому рост подпольной профессионализации программ-вымогателей как услуги (RaaS). RaaS - это продажа программ-вымогателей, разработанных профессионалами, где даже нетехнические преступники, не имеющие опыта написания программ-вымогателей, могут получить их и использовать против выбранной ими цели. Это совокупное повышение сложности и профессионализма подпольных программ-вымогателей привело к значительному увеличению воздействия атак программ-вымогателей «большой игры».

Яркий пример произошел 7 мая, когда Колониальный трубопровод подвергся крупнейшей кибератаке на нефтяную инфраструктуру в Соединенных Штатах. Используя простые украденные учетные данные, злоумышленники проникли в системы компании и загрузили программы-вымогатели, похитив и заблокировав 100 ГБ данных и вызвав нехватку топлива. В этот момент президент Байден объявил в этом районе чрезвычайное положение, чтобы предотвратить дальнейшие разрушения.

Итак, как же выжить после крупных атак программ-вымогателей? На мой взгляд, единственный реальный способ остановить эту угрозу - перестать платить выкуп. Почему киберпреступное подполье приложило столько усилий для профессионализации программ-вымогателей? Проще говоря, они зарабатывают на этом кучу денег. Но также важно понимать, как это можно предотвратить. Как всегда, вам необходимо убедиться, что у вас есть уже написанный и действующий план обеспечения непрерывности бизнеса и аварийного восстановления (BC / DR), который гарантирует, что вы сможете быстро восстановить критически важные бизнес-системы в случае любой кибер-катастрофы.

К сожалению, не существует единой защиты, которая полностью защитит компанию от программ-вымогателей. Но наличие нескольких уровней защиты - лучший способ остановить все киберугрозы в целом, включая программы-вымогатели. Некоторые необходимые меры безопасности для программ-вымогателей включают защиту конечных точек и ответ (EDR), многофакторную аутентификацию (поскольку хакеры не взламывают, они входят в систему, как атака Colonial Pipeline) и расширенную защиту от вредоносных программ. Если вы включите эти уровни в свою защиту вместе с проверенным планом BC / DR, вымогатели редко будут успешными, и вы сможете быстро восстановиться, не платя даже в худшем случае». ***(Corey Nachreiner. Tips for Surviving Big Game Ransomware Attacks // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/tips-for-surviving-big-game-ransomware-attacks-p-3146). 16.11.2021).***

***

«Сообщения о данных Национальной службы здравоохранения (NHS) в Англии, разоблаченных в результате атаки программ-вымогателей на британскую компанию по сбору и хранению данных Stor-a-File, неверны,

сообщил Information Security Media Group представитель NHS England. В число клиентов Stor-a-File входят больничные тресты NHS, врачи общей практики, местные советы и другие, но представитель сообщает ISMG: «Большая часть данных NHS была сохранена в автономном режиме и не пострадала от взлома Stor-a-file».

Это противоречит более раннему сообщению британской газеты The Daily Mail, в которой утверждалось, что записи NHS, содержащие конфиденциальные медицинские документы, были размещены в даркнете.

«Трасты NHS несут ответственность за обеспечение безопасного хранения записей и данных. Пока полиция продолжает расследование, Stor-A-File Ltd связалась со всеми клиентами, пострадавшими от этого нарушения, включая небольшое количество трастов, чтобы они могли примите соответствующие меры», - сказал представитель NHS England.

Компания, занимающаяся хранением данных, подтвердила это заявление, сообщив ISMG: «950 000 ящиков с документами, которые хранятся в Stor-a-File для клиентов, не были затронуты, включая различные данные, доверенные NHS». Представитель компании говорит, что компания всегда очень серьезно относилась как к локальной безопасности, так и к кибербезопасности, и добавляет: «Национальное агентство по борьбе с преступностью предлагало поддержку и советы некоторым из тех, кто пострадал от этого инцидента».

ISMG связалась с агентством, которое заявило: «NCA известно об инциденте с утечкой данных, который затронул Stor-A-File Ltd., и он предложил свой опыт и поддержку партнерам».

За дополнительной информацией NCA направило ISMG в полицейское управление Лестершира, которое, как оно подтвердило, расследует инцидент. Департамент полиции не предоставил подробностей о достигнутом прогрессе, просто сообщив ISMG, что он «получил отчет, касающийся утечки данных в компании в Систоне, Лестере, и расследование продолжается».

Что случилось

«В начале сентября нам стало известно, что мы стали жертвой изощренной атаки с использованием программ-вымогателей, совершенной преступной организацией», - сообщил ISMG представитель Stor-a-File. В общей сложности пострадали 13 компаний, шесть из которых были связаны со здоровьем, добавляет пресс-секретарь.

К ним относятся Lister Fertility Clinic и Nuffield Health Leicester Hospital, согласно британскому информационному агентству BBC, а также клиники, которыми управляет Мэри Стоупс и Британская консультативная служба по беременности, согласно отчету The Daily Mail. Клиника Lister заявила, что ее медицинские записи включают формы согласия, историю болезни и результаты анализов, рекомендации по лечению и записи о лечении бесплодия, но не включают финансовую информацию, такую как данные кредитной или дебетовой карты.

Группа вымогателей Cl0p была идентифицирована как причастная к этой атаке, сообщил ISMG представитель Stor-a-File, сославшись на первоначальные выводы специалистов по кибербезопасности и полицейского управления, расследующего инцидент.

Stor-a-File сообщает, что, похоже, киберпреступники получили доступ через уязвимость в системе безопасности Serv-U FTP стороннего производителя SolarWinds. Он не раскрывает точных деталей уязвимости, поэтому любая оценка является спекулятивной, но, согласно июльскому сообщению SolarWinds, уязвимость, помеченная как CVE-2021-35211, в случае эксплуатации дает привилегированный доступ к машине, на которой размещено программное обеспечение Serv-U.

«Эта атака представляет собой атаку с возвратно-ориентированным программированием (ROP)», - говорится в сообщении. «При использовании уязвимости продукт Serv-U генерирует исключение, а затем перехватывает код обработки исключений для выполнения команд».

Уязвимость, обнаруженная Microsoft Threat Intelligence Center, затрагивала Serv-U версии 15.2.3 HF1 и все предыдущие сборки. MSTIC в то время отметила, что злоумышленники активно нацеливались на эту уязвимость, но в блоге по безопасности не упоминалось о группе вымогателей Cl0p.

Stor-a-File подтвердил, что не платил выкуп злоумышленникам и вместо этого использовал свои резервные копии данных, чтобы вернуться в нормальное состояние. «Мы очистили, восстановили и исправили наши уязвимые системы с помощью резервных копий, и теперь Stor-a-File работает в обычном режиме», - сказал представитель компании. В качестве контрмеры и во избежание подобных инцидентов в будущем компания удалила все стороннее программное обеспечение из своих критически важных систем.

Офис комиссара по информации, NCA и Департамент полиции Лестершира были проинформированы сразу после обнаружения из-за проблем с соблюдением GDPR. ICO признало это и сообщает ISMG: «Люди имеют право ожидать, что организации будут обращаться с их личной информацией безопасно и ответственно. Таким образом, мы расследуем этот инцидент, чтобы такие инциденты не повторялись».

Претензии к дампу данных

В отличие от того, что скомпрометированная компания и власти сообщили ISMG, в более раннем отчете Daily Mail утверждалось, что записи NHS, содержащие конфиденциальные медицинские документы, были сброшены в темную сеть, ссылаясь на решение Stor-a-File не платить выкуп как причина этого.

Известно, что группа вымогателей Cl0p публикует или сбрасывает такие записи на своем собственном веб-сайте Clop Leaks, размещенном на Tor. ISMG не обнаружила свалок данных, связанных с NHS или соответствующими трастами на этом сайте утечки, когда мы проверили его перед публикацией, но мы действительно обнаружили сообщение, размещенное на его домашней странице, в котором операторы предупреждают посетителей сайта о других группах, выдающих себя за него, и используя свою торговую марку для выкачивания денег». ***(Mihir Bagwe. NHS Denies Data Was Exposed in Stor-a-File Hack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/nhs-denies-data-was-exposed-in-stor-a-file-hack-a-17971). 22.11.2021).***

***

«В Азиатско-Тихоокеанском регионе (APAC) программы-вымогатели стали серьезной проблемой для организаций во всех отраслях. Средняя стоимость на ликвидацию в вымогателей атаку вырос более чем US $ 1 миллиона, при этом расходы на восстановительные работы, в том числе бизнес - простои, потерю заказов, эксплуатационные расходы и более, увеличиваясь от в среднем US $ 1,16 млн 2020 до $ 2,34 млн долларов США в 2021 году. Фактически, организации Азиатско-Тихоокеанского региона на 80% чаще, чем в среднем по миру, становятся целью кибератаки.

Мы должны бороться не только с предрасположенностью, но и с характером атак, поскольку все больше киберпреступников нацелены на клиентов и цепочки поставок и нападают на правительственные организации или крупные частные компании (такие как Kaseya). Ранее в этом году сингапурское агентство кибербезопасности (CSA) сообщило о росте на 154% случаев вымогательства, затронувших малые и средние предприятия в таких секторах, как производство, розничная торговля и здравоохранение. Совсем недавно, в августе 2021 года, атака программы-вымогателя в городе-государстве затронула личные данные и клиническую информацию более 73000 пациентов частной глазной клиники. Кроме того, в том же месяце жертвами атак программ-вымогателей стали ведущая страховая компания Tokio Marine Insurance Singapore и технологическая компания Pine Labs.

Развитие программ-вымогателей - главная проблема в Азиатско-Тихоокеанском регионе

В 2021 году киберпреступные группы действовали аналогично компании, занимающейся технологиями SaaS, в том, что можно охарактеризовать как выкуп как услуга, чтобы они могли осуществлять атаки и максимально монетизировать их.

Это свидетельствует об огромном изменении по сравнению с традиционными программами-вымогателями, поскольку эти атаки больше не полагаются только на автоматизированное вредоносное ПО, и в результате они не так предсказуемы. Часто мы не видим этого, пока не становится слишком поздно, что оставляет нас в положении, когда нам необходимо сначала понять, а затем изолировать злоумышленников в нашей среде как можно быстрее, прежде чем вредоносное ПО обнаружится. RansomOps - это отход от традиционного вредоносного ПО, которое доставляется гораздо более предсказуемым и автоматизированным способом.

Более того, пандемия привела к широкому распространению облака, и наряду с этим мы видели, как филиалы RansomOps ищут новые способы таргетинга через общедоступные облачные платформы, такие как AWS и Azure. Это дает злоумышленникам возможность перейти от первоначального доступа к выкупу даже быстрее, чем за уже быстрые 8–30 дней. Фактически, эти атаки могут быть завершены в течение дня.

С каждым днем становится все более очевидным, что нам нужны надежные системы и решения кибербезопасности, чтобы не только защитить наши данные, но и все наши бизнес-операции и, по сути, средства к существованию наших людей. Во всем, что касается кибербезопасности, нет серебряной пули. Однако в качестве отправной точки организациям необходимо иметь сильную политику киберустойчивости. Чтобы достичь этого, необходимо сместить мышление с «если»

мы пойдем на компромисс к «когда» мы пойдем на компромисс. Как только это изменение мышления произойдет, политика должна учитывать людей, процессы и технологии, чтобы группы безопасности имели четкую видимость всех активов в сети, включая облако и инфраструктуру центра обработки данных.

Лучшие практики безопасности для борьбы с программами-вымогателями

Высокий уровень прозрачности является ключом к выявлению поверхностей атаки, которым подвержена организация. Чтобы подготовиться, вы должны убедиться, что ваша организация может быстро выявлять нарушения. Это означает регулярное участие в строгих упражнениях, направленных на изучение мер безопасности, существующих процессов и процедур, а также на выявление любых пробелов. Убедитесь, что вы исправили хорошо и старательно, а также запустите новейшее программное обеспечение безопасности с четкой стратегией в сети и на конечных точках.

Организации Азиатско-Тихоокеанского региона также должны постоянно инвестировать в обучение своего персонала вопросам кибербезопасности. Мы должны убедиться, что советы директоров осведомлены о рисках, связанных с RansomOps, и о возможных последствиях для бизнеса. Эффективным методом является отработка того, как организация будет реагировать на инцидент с программой-вымогателем, с помощью настольных упражнений со всеми руководителями и членами совета директоров. В нем будут обозначены обязанности, которые должен обеспечить бизнес при возникновении таких инцидентов, и, в конечном итоге, ускориться время реагирования на реальное событие.

С технологическим партнером, специализирующимся на обнаружении угроз и реагировании, вы можете разбить все на очень подробные этапы атаки - командование и управление, разведку, боковое движение - и эксфильтрацию. Вы можете далее разбить это на конкретные действия на этих этапах, чтобы определить, что потенциально может быть инцидентом с вымогательством, на ранней стадии и обеспечить нормальную работу. В целом организациям необходимо создать корпоративную культуру, которая понимает риски, а затем внедряет меры по снижению рисков, подкрепленные процедурами выявления, реагирования и восстановления после киберинцидентов, таких как RansomOps». ***(CHRIS FISHER. Ransomware to RansomOps: Why APAC Enterprises are Increasingly Vulnerable // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/ransomware-to-ransomops-why-apac-enterprises-are-increasingly-vulnerable/). 18.11.2021).***

***

«Государственный департамент США предлагает до 10 миллионов долларов в качестве вознаграждения за информацию, позволяющую идентифицировать или определить местонахождение любых лиц, занимающих ключевые руководящие должности в бандах вымогателей REvil или Sodinokibi.

Аналогичное вознаграждение было предложено группе вымогателей DarkSide, ответственной за атаку вымогателя Colonial Pipeline, нарушившую поставку топлива на восточном побережье США.

Точно так же вознаграждение в размере 5 миллионов долларов доступно за любую информацию, ведущую к аресту или осуждению аффилированных лиц в

любой стране, планирующих совершить атаки с использованием программ-вымогателей REvil.

Банда вымогателей REvil провела несколько атак в США, включая инциденты кибербезопасности Coop, Grupo Fleury, GSMLaw, JBS, Kaseya, Kenneth Cole и Travelex.

Обвинение предъявлено нескольким членам банды вымогателей REvil

Схема вознаграждения Госдепартамента совпала с раскрытием Министерством юстиции США двух обвинительных заключений в отношении ролей, которые два подозреваемых, находящихся в настоящее время под стражей, сыграли в атаках программ-вымогателей REvil.

Сотрудники правоохранительных органов задержали семерых членов банды вымогателей REvil, в том числе причастных к атаке программы-вымогателя Kaseya. Трое из подозреваемых, ответственных за более чем 7000 атак, принадлежат к банде вымогателей REvil, операторам вымогателей GandGrab.

«Это [] особенно удачный момент, поскольку он извлекает выгоду из недавнего проникновения REvil со стороны правоохранительных органов», - сказал Джейк Уильямс, соучредитель и технический директор BreachQuest.

22-летний гражданин Украины Ярослав Васинский является подозреваемым аффилированным лицом REvil за инцидентом с Касеей. Васинский был арестован на границе с Польшей в ходе операции с участием 19 правоохранительных органов на пяти континентах. Ему грозит экстрадиция в США.

Аналогичным образом, филиал REvil и 28-летний гражданин России Евгений Полянин также был обвинен в нападении на 22 муниципалитета Техаса в 2019 году.

Минюст также установил, что Полянин выплачивал выкуп в размере 6,1 миллиона долларов. Как сообщается, он живет в Барнауле, Сибирь, и его активность на российских хакерских форумах насчитывает более десяти лет.

К сожалению, в большинстве арестов участвуют одноразовые аффилированные лица и младшие члены банд вымогателей, в то время как главные авторитеты продолжают мирно пользоваться доходами от киберпреступности.

Следовательно, правоохранительные органы полны решимости задержать ключевых лидеров сети киберпреступлений, чтобы оказать ощутимое воздействие.

Однако большинство национальных государственных субъектов защищают ключевых лидеров банд вымогателей и используют их инфраструктуру и опыт для кибершпионажа.

Банды вымогателей меняют свой бренд, чтобы избежать правосудия

Большинство групп программ-вымогателей часто меняют свой бренд, чтобы избежать усилий правоохранительных органов, на фоне повышенного внимания и ресурсов, направленных на борьбу с международной киберпреступностью.

Например, в 2019 году GandGrab была переименована в банду вымогателей REvil, а DarkSide - на BlackMatter. Точно так же BitPaymer переименовал себя в DoppelPaymer, а Nefilim стал Karma.

Однако Госдепартамент признает гибкость банд вымогателей в изменении личности. Следовательно, награда распространяется на все варианты вымогателя Sodinokibi, связанные с международной организованной преступной группировкой.

Госдепартамент отметил, что награда продемонстрировала приверженность Соединенных Штатов защите жертв программ-вымогателей от эксплуатации.

Примечательно, что награда является частью Программы вознаграждений за транснациональную организованную преступность (TOCRP). Программа сыграла решающую роль в аресте 75 транснациональных преступников, включая торговцев наркотиками, и выдала вознаграждение на сумму более 135 миллионов долларов.

Для сравнения, награда за Усаму бен Ладена составила всего 25 миллионов долларов, что подчеркивает растущее внимание правительства США к атакам программ-вымогателей.

США предложили аналогичные награды за попытки остановить киберпреступников от взлома компьютерных систем и кражи конфиденциальной информации.

В июле 2021 года власти США предложили вознаграждение в размере 10 миллионов долларов за информацию для выявления субъектов угроз, контролируемых иностранными правительствами. Аналогичная награда в августе 2020 года была направлена на выявление кибер-акторов, пытающихся помешать выборам в США. Точно так же США предложили вознаграждение в размере 5 миллионов долларов за информацию, разоблачающую северокорейских хакеров и их операции.

«Будет интересно посмотреть, будут ли предложены дополнительные награды для других известных участников программ-вымогателей в зависимости от успеха (или неудачи) этой инициативы», - сказал Шон Никкель, старший аналитик Intel по киберугрозам в Digital Shadows. «Все это происходит вслед за продолжающимися действиями администрации Байдена по усилению борьбы с программами-вымогателями, особенно с учетом недавних санкций, создания целевых групп и новых агентств, а также других недавних тем для обсуждения».

Вероятно, одни преступники могли попытаться разоблачить других и получить денежное вознаграждение. Точно так же программа вознаграждений вызовет подозрения в и без того чувствительной отрасли, вынудив некоторых преступников пересмотреть свое участие в подпольной киберпреступности.

«При таком большом вознаграждении у этих преступников есть существенный стимул нападать друг на друга», - отметил Уильямс. «Возможно, что более важно, чем конкретное воздействие на DarkSide, это действие подрывает доверие к программе-вымогателю как модели партнерской службы».

«Действия правоохранительных органов против REvil в июле уже вызвали серьезные проблемы с доверием среди операторов. Это углубляет этот клин и выйдет далеко за пределы DarkSide (переименованного в BlackMatter и, предположительно, закрытого на этой неделе)», - продолжил он.

Джон Бамбенек, главный охотник за угрозами в Netenrich, отметил, однако, что эта инициатива, хотя и новая, может потерпеть неудачу из-за отсутствия охотников за головами.

«Однако в отсутствие охотника за головами, желающего отправиться в свою юрисдикцию, положить свое бессознательное тело в мешок и сбросить его в ближайшем посольстве США, я сомневаюсь, что это окажет большое влияние. Честно говоря, это тоже точно не повредит. Я просто не ожидаю увидеть в

ближайшее время пресс-конференцию, на которой госсекретарь раздаст большой картонный чек на 10 миллионов долларов». ***(ALICIA HOPE. US State Department Offers a $10 Million Reward for Information on REvil and Darkside Ransomware Gang Leaders // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/us-state-department-offers-a-10-million-reward-for-information-on-revil-and-darkside-ransomware-gang-leaders/). 23.11.2021).***

***

«Сегодняшний ландшафт киберугроз чрезвычайно сложен. Выкуп за это, выкуп за это, выкуп повсюду - профессионалы в области информационных технологий (ИТ) должны работать, чтобы защитить организации от следующей крупной атаки программ-вымогателей. С годами изощренность атак программ-вымогателей возросла, а также увеличились суммы денег, требуемых и выплачиваемых в обмен на хранящуюся в выкупе информацию. Вот почему чрезвычайно важно, чтобы организации снабжали своих сотрудников знаниями и осведомленностью, необходимыми для выявления действий, которые приводят к таким атакам.

Осведомленность о кибербезопасности

Предотвращение атак программ-вымогателей и реагирование на них требует осведомленности о векторах угроз программ-вымогателей, а также подхода к снижению связанных с ними рисков, основанному на человеческих процессах и технологиях. Сотрудники должны понимать, как обнаруживать и избегать распространенных векторов атак. Это требует серьезной осведомленности о кибербезопасности и обучения. В рамках обучения сотрудникам должна быть представлена политика, которая инструктирует их:

Выявление и предотвращение распространенных векторов атак (например, попыток фишинга)

Удаляйте подозрительные письма, содержащие ссылки

Избегайте посещения вредоносных веб-сайтов

Есть некоторые свидетельства того, что сотрудники США могут не знать об увеличении числа атак с использованием программ-вымогателей, а также о более разрушительном и разрушительном характере и масштабах атак. В июне 2021 года Армис сообщил о результатах опроса более 2000 респондентов со всех концов Соединенных Штатов. На основании результатов было очевидно, что конечные пользователи не обращают внимания на крупные атаки кибербезопасности, поражающие операционные технологии и критически важную инфраструктуру по всей стране, что свидетельствует о важности того, чтобы предприятия уделяли приоритетное внимание безопасности по мере того, как сотрудники возвращаются в офис. В отчет включены выводы по следующим четырем направлениям:

Просвещение и осведомленность о кибератаках

Серьезность и стойкость атак

Атаки, нацеленные на здравоохранение

Принесите свое собственное устройство (BYOD)

Результаты показали, что респонденты не знали о самых недавних и разрушительных кибератаках, несмотря на заголовки новостей и внимание,

уделяемое СМИ, при этом было отмечено, что более 21% респондентов не знали о кибератаке Colonial Pipeline. Что касается долгосрочных последствий атаки, 24% респондентов полагали, что инцидент не будет иметь долгосрочных последствий для топливной промышленности нашей страны. В ходе опроса также рассматривалось использование личных устройств сотрудников для выполнения работы для своего работодателя и выяснилось, что

26% компаний не имеют политики для защиты как рабочих, так и личных устройств,

Более 71% сотрудников намерены приносить свои устройства для работы из дома (WFH) обратно в офис, и

54% не верят, что их личные устройства представляют угрозу безопасности их организации.

Человеческий фактор

Человеческий фактор играет большую роль в выявлении или невыявлении киберинцидентов. Люди также играют важную роль в сообщении об инцидентах. Следовательно, организации должны инвестировать в обучение своих сотрудников тому, как выявлять подозреваемые инциденты и сообщать о них. Таким образом, рекомендуется сосредоточить внимание на обучении и предотвращении наиболее распространенных источников заражения вредоносным ПО. Недостаточно просто установить антивирусное программное обеспечение на компьютеры сотрудников. Их поведение является ключом к защите от заражения вредоносным ПО. Почему? Потому что в сегодняшнем высокоорганизованном киберпреступном мире существуют целые организации, постоянно занимающиеся разработкой вредоносных программ, которые невозможно обнаружить.

Организации также должны вкладывать средства во внедрение передовых методов, направленных на предотвращение заражения вредоносными программами, таких как регулярное сканирование уязвимостей для выявления и устранения уязвимостей, установка исправлений и обновления программного обеспечения, а также обеспечение правильной настройки устройств и включения функций безопасности.

Заключение

В дополнение к эффективному информированию и обучению кибербезопасности (например, обучению людей выявлять фишинговые атаки) использование технологий может значительно снизить риски. Например, управление конфигурацией безопасности (SCM) и мониторинг целостности файлов (FIM) — это инструменты, которые автоматизируют поддержание безопасных конфигураций. Хотя SCM уведомляет и предлагает подробные инструкции по исправлению, чтобы вернуть неправильно настроенную систему в соответствие, FIM — это технология, которая отслеживает и обнаруживает изменения в файлах, которые могут указывать на кибератаку. Поскольку предприятия инвестируют в повышение осведомленности о кибератаках, оба этих инструмента помогут организациям защититься от них». ***(Ambler. Invest in Cyber Awareness to Prevent Attacks // Tripwire, Inc. (https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/invest-in-cyber-awareness-to-prevent-attacks/). 10.11.2021).***

***

«Атака программ-вымогателей происходит уже давно. Атаки с помощью программ-вымогателей совершаются с целью нанести ущерб странам, особенно высокопоставленным отделам, которые содержат важную информацию. При атаках программ-вымогателей происходит утечка конфиденциальных и важных документов, а затем хакеры взамен просят огромную сумму денег, чтобы больше не наносить ущерба.

Чтобы предположить, как в этом году могли быть совершены атаки программ-вымогателей, в каких странах и в каких отделах и насколько сильно пострадали, Black Fog решил завершить исследование.

Отчет об исследовании называется «Состояние программ-вымогателей в 2021 году» и содержит процент атак с использованием программ-вымогателей, через которые прошла каждая страна с начала этого года до октября 2021 года.

Для начала список возглавила одна из ведущих сверхдержав мира Соединенные Штаты Америки. Однако очевидно, что когда кто-то входит в число самых могущественных стран в мире, такие атаки, как правило, направлены на вас, чтобы получить доступ к личным данным страны.

В этом году в Америке было зарегистрировано почти 52% атак с использованием программ-вымогателей. Самый высокий в списке. Многие известные компании подверглись нападениям и серьезно пострадали, что в конечном итоге привело к потере поставок компании на миллионы долларов и недель.

Следующей в списке идет Великобритания, считая, что она также является одной из могущественных стран мира. Однако по процентному соотношению все же далеко позади США. В Великобритании было зарегистрировано около 11% атак программ-вымогателей. Одна из главных атак этого года в стране не очень старая и произошла только в прошлом месяце. Преступная группировка слила почти 69000 документов, содержащих информацию о многих важных и известных людях. Затем потребовали огромную сумму, чтобы остановить нападение.

В Канаде уровень атак составил 4,51 процента, что кажется намного меньше, но нанесенного ущерба не было. В феврале банда вымогателей DarkSide атаковала одну из огромных канадских компаний по аренде, а затем разместила на своем сайте утечки информацию о том, что они получили доступ к почти 120 ГБ корпоративных, банковских и франчайзинговых данных компании.

Вслед за этим многие другие страны, такие как Франция, Япония, Австралия и т. д., также столкнулись с атаками программ-вымогателей.

В то время как страны подвергались нападению, вопрос в том, какое именно статус-кво или агентство стран подверглись нападению.

Очевидно, что атаки изначально и наиболее целенаправленно были направлены на правительства всех стран. Правительство имеет доступ к большому количеству данных как о людях, так и о его планах, а также о том, что нужно сделать. Также сохраняется информация о деньгах и казначействе. Получение доступа к такой важной информации может дать любому злоумышленнику власть и власть в считанные секунды.

Затем были атакованы учебные заведения. В этом году нападению подверглись 35 учебных заведений. Наибольший подход к хакерам в систему образования приходился на студентов, которые использовали множество онлайн-платформ и были для них легкой мишенью, позволяющей им проникнуть в систему.

Кроме того, 33 процента атак были совершены через медицинские учреждения, а 22 процента - на другие службы…». ***(Arooj Ahmed. Black Fog concludes a ransomware report on how many attacks were observed this year // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/11/black-fog-concludes-ransomware-report.html). 17.11.2021).***

***

«Новая группа программ-вымогателей под названием Memento применяет необычный подход к блокировке файлов в архивах, защищенных паролем после того, как их метод шифрования постоянно обнаруживается программным обеспечением безопасности.

В прошлом месяце группа стала активной, когда они начали использовать уязвимость веб-клиента VMware vCenter Server для первоначального доступа к сетям жертв.

Уязвимость vCenter отслеживается как CVE-2021-21972 и представляет собой ошибку удаленного выполнения кода без проверки подлинности с рейтингом серьезности 9,8 (критический).

Этот недостаток позволяет любому, у кого есть удаленный доступ к TCP / IP-порту 443 на открытом сервере vCenter, выполнять команды в базовой ОС с правами администратора.

Патч для этой уязвимости вышел в феврале, но, как показала работа Memento, многие организации не исправили свои установки.

Memento эксплуатирует эту уязвимость с апреля, а в мае был замечен другой субъект, использующий ее для установки майнеров XMR с помощью команд PowerShell.

Использование vCenter для развертывания программ-вымогателей

Memento запустила операцию по вымогательству в прошлом месяце, запустив vCenter для извлечения административных учетных данных с целевого сервера, обеспечения устойчивости с помощью запланированных задач, а затем использования RDP через SSH для горизонтального распространения в сети.

После этапа разведки актеры использовали WinRAR для создания архива украденных файлов и его эксфильтрации.

Наконец, они использовали утилиту очистки данных BCWipe от Jetico, чтобы удалить любые оставленные следы, а затем использовали штамм вымогателя на основе Python для шифрования AES.

Однако первоначальные попытки Memento зашифровывать файлы, поскольку системы имели защиту от программ-вымогателей, вынуждали обнаруживать и останавливать этап шифрования до того, как был нанесен какой-либо ущерб.

Обходной путь

Чтобы преодолеть обнаружение обычных программ-вымогателей программным обеспечением безопасности, Memento придумал интересную тактику - полностью отказаться от шифрования и переместить файлы в архивы, защищенные паролем.

Для этого группа теперь перемещает файлы в архивы WinRAR, устанавливает неверный пароль для защиты доступа, шифрует этот ключ и, наконец, удаляет исходные файлы.

«Вместо шифрования файлов код «crypt» теперь помещает файлы в незашифрованном виде в архивные файлы, используя копию WinRAR, сохраняя каждый файл в отдельном архиве с расширением файла.vaultz», - объясняет аналитик Sophos Шон Галлахер.

«Пароли генерировались для каждого файла по мере его архивирования. Затем сами пароли были зашифрованы».

В выписке с требованием выкупа жертва должна заплатить 15,95 BTC (940 000 долларов США) за полное восстановление или 0,099 BTC (5850 долларов США) за файл.

В случаях, расследованных Sophos, эти попытки вымогательства не привели к выплате выкупа, поскольку жертвы использовали свои резервные копии для восстановления файлов.

Однако Memento - это новая группа, которая только что нашла нетипичный подход, который работает, поэтому они, вероятно, попробуют его против других организаций.

Таким образом, если вы используете VMware vCenter Server и / или Cloud Foundation, обязательно обновите свои инструменты до последней доступной версии, чтобы устранить известные уязвимости». ***(Bill Toulas. New Memento ransomware switches to WinRar after failing at encryption // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-memento-ransomware-switches-to-winrar-after-failing-at-encryption/). 18.11.2021).***

***

«Операторы вымогателя Conti пострадали от утечки данных: швейцарская ИБ-компания Prodaft смогла определить реальный IP-адрес одного из серверов группы и оставалась в системе более месяца.

Пострадавший сервер являлся платежным порталом (или так называемым «сервером восстановления») группы, на который хакеры приглашали своих жертв для проведения переговоров о выплате выкупа. Сервер хостился у украинского хотсера ITL LLC и размещался на IP-адресе 217.12.204.135.

«Наша команда обнаружила уязвимость в серверах восстановления, которые использует Conti, и использовала эту уязвимость для обнаружения реальных IP-адресов hidden service, где был размещен сайт», — гласит отчет Prodaft.

Исследователи сохраняли доступ к серверу в течение нескольких недель и отслеживали весь сетевой трафик и IP-адреса. Хотя некоторые из адресов принадлежали жертвам и их посредникам, Prodaft также отследила SSH-соединения, которые, скорее всего, относились к самим хакерам. Увы, все IP-адреса SSH были

связаны с выходным узлам Tor, то есть использовать их для идентификации участников хак-группы не представлялось возможным…

Также в отчете исследователей представлена другая ценная информация, включая сведения об ОС сервера Conti и файле htpasswd, который содержал хешированную версию пароля сервера. Компания Prodaft подчеркивает, что поделилась всеми своими выводами с правоохранительными органами, и некоторые детали хранятся в тайне, чтобы дать правоохранителям время на принятие мер.

Публикация отчета не прошла незамеченной не только среди ИБ-экспертов, но и среди самих хакеров. Дело в том, что утечка IP-адреса и хешированного пароля сервера потенциально открывали сервер для конкурирующих хак-групп. В итоге уже через несколько часов после публикации отчета исследователи MalwareHunterTeam заметили, что Conti отключила свой платежный портал. Внезапный простой сервера лишил недавних жертв Conti возможности связаться с хакерами и заплатить выкуп, размер которого все увеличивался…

В итоге платежный портал Conti вернулся в онлайн спустя более 24 часов после отключения, а в блоге хак-группы появилось гневное сообщение, которое гласит, что «европейцы, похоже, решили забыть о своих манерах и повели себя как гопники, пытаясь взломать наши системы».

Также хакеры опровергли утверждение Prodaft, сделанное на прошлой неделе: исследователи писали, что с июля 2021 года вымогатели «заработали» около 25,5 миллиона долларов. Операторы Conti заявили, что на самом деле их прибыль составила более 300 000 000 долларов. Впрочем, скорее всего, это лишь хвастовство, которое вымогатели используют для саморекламы и повышения прибыльности своих атак.

Интересно, что некоторые эксперты уже раскритиковали Prodaft за публичное раскрытие информации, которое привело лишь к тому, что Conti усилила безопасность своих серверов». ***(Мария Нефёдова. Операторы шифровальщика Conti стали жертвой утечки данных // Хакер (https://xakep.ru/2021/11/22/conti-leak-2/). 22.11.2021).***

***

«Кибервымогательская группировка, называющая себя Everest, выставила на продажу доступ к IT-сетям правительства Аргентины за $200 тыс.

«Доступ к правительственным системам Аргентины. Доступ к различным сервисам интранета (внутренней частной сети организации - ред.). Доступ к базам данных с полным редактированием тоже включен. Документы отдельно не продаются, только доступ», - приводят сообщение Everest специалисты ИБ-компании DarkTracer.

Продавцы не предоставили ни доказательств того, что у них действительно есть доступ к системам правительства Аргентины, ни каких-либо сведений о том, как они могли его получить.

Как сообщает аргентинская газета El Litoral, на этой неделе Everest также выставила на продажу предполагаемый доступ к правительственным системам Перу и бразильским организациям за $30 тыс. и $50 тыс. долларов соответственно. Как и

в случае с правительством Аргентины, киберпреступники не предоставили никаких доказательств наличия у них доступа к системам.

В начале октября нынешнего года некий продавец выставил на продажу на хакерских форумах учетные данные сетевого администратора с прямым доступом к контроллеру домена, доступному через VPN. В конце того же месяца продавец предлагал купить или обменять доступ через VPN к базам данных в Аргентине». ***(Кибервымогатели Everest выставили на продажу доступ к IT-сетям правительства Аргентины // SecurityLab.ru (https://www.securitylab.ru/news/526835.php). 24.11.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Міністерство юстиції США звинуватило українця Ярослава Васинського та росіянина Євгена Поляніна у кібератаках REvil з використанням хакерської програми-вимагача. Їм загрожує по понад 100 років ув'язнення…

Деталі

Повідомляється, що у липні цього року 22-річний українець Ярослав Васинський зламав американську софтверну компанію Kaseya, за допомогою якої розповсюджував віруси-вимагачі. У результаті жертвами стали близько 1500 підприємств та організацій по всьому світу.

Хакерське угруповання вимагало викуп у 70 млн доларів за розблокування даних, зашифрованих в результаті атаки. Через три тижні Kaseya допомогла користувачам повернути доступ до даних ключем дешифрування.

Повідомляється, що Васинського вдалося затримати. Він заарештований у Польщі і очікує на екстрадицію до США, де його притягнуть до кримінальної відповідальності. Васинського звинувачують у змові з метою шахрайства, пошкодженні комп'ютерів та крадіжці грошей. Йому загрожує покарання у вигляді позбавлення волі терміном до 115 років.

Євгена Поляніна затримати не вдалося. Проте Мін'юст США конфіскував у нього 6,1 млн доларів. Передбачається, що він отримав ці гроші після проведення атак хакерів за допомогою програм-вимагачів Sodinokibi/REvil в 2019 році як викуп. За даними джерел, йому загрожує до 145 років ув'язнення.

Тим часом Міністерство фінансів США наклало санкції на Васинського та Полянина, а також на криптовалютну біржу, яку хакери могли використовувати для переказу коштів.

Держдепартамент США оголосив про винагороду у 10 млн доларів за інформацію про осіб чи місцезнаходження лідерів хакерського угрупування REvil. Влада США також пропонує до 5 млн доларів за інформацію, яка допоможе заарештувати або засудити хакерів за змову та участь в атаках з використанням програмного забезпечення REvil…». ***(Єлизавета Калітвенцева. США звинуватили***

українця та росіянина через кібератаку REvil: їм загрожує по понад 100 років ув'язнення // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1951622-ssha-zvinuvatili-ukrayintsya-ta-rosiyanina-cherez-kiberataku-revil-yim-zagrozhuye-po-ponad-100-rokiv-uvyaznennya). 09.11.2021).

***

«…Госдепартамент США объявил о награде в размере до 10 миллионов долларов «за информацию, позволяющую установить личность или местонахождение любого человека (лиц), занимающего ключевую руководящую позицию в транснациональной организованной преступности, являющейся разновидностью вымогателя Sodinokibi (также известного как REvil)».

Также предлагается вознаграждение в размере до 5 миллионов долларов «за информацию, ведущую к аресту и / или осуждению в любой стране любого лица, участвовавшего в сговоре с целью участия или попытки участия в инциденте с вымогателем Sodinokibi».

В четверг были объявлены аналогичные награды, связанные с конкурирующей компанией-вымогателем DarkSide, позже возрожденной как BlackMatter.

Как показывает это, западные правительства уделяют все больше времени, внимания и ресурсов борьбе с киберпреступностью и особенно с программами-вымогателями после лета разрушительных атак, в том числе против Colonial Pipeline в США, бразильского мясоперерабатывающего гиганта JBS, поставщика программного обеспечения под управлением ИТ. Касея, Национальная служба здравоохранения Ирландии и многие другие.

Конечно, приветствуется делать что-либо, чтобы уменьшить ущерб, причиняемый программами-вымогателями. Хотя в совокупности это не приносит наибольших потерь, связанных с киберпреступностью - это различие связано с множеством различных видов атак с взломом корпоративной электронной почты, включая мошенничество со стороны генерального директора, - программы-вымогатели могут нанести серьезный ущерб не только предприятиям, но и потребителям. Следовательно, США рассматривают это как угрозу национальной безопасности наравне с терроризмом.

12 вызовов для борьбы с программами-вымогателями

К сожалению, правительства, пытающиеся бороться с программами-вымогателями, сталкиваются с многочисленными проблемами, в том числе:

Масштаб: По крайней мере, в том, что касается программ-вымогателей, плохие парни выигрывают. По данным аналитической компании Chainalysis, в 2020 году злоумышленники, использующие программы-вымогатели, заработали не менее 350 миллионов долларов от выкупа. И хотя не все группы программ-вымогателей имеют сайты утечки данных, количество жертв, размещаемых на таких сайтах, не снижается.

Безопасные убежища: многие преступники, осуществляющие онлайн-атаки, базируются в России или за ее пределами, которая никогда не выдает граждан для

предъявления обвинений иностранным гражданам. Хотя администрация Байдена призывает Москву принять жесткие меры, пока не ясно, пойдет ли она на это.

Автоматизация: разработчики программ-вымогателей продолжают совершенствовать свои вредоносные программы, чтобы облегчить их использование филиалами и повысить эффективность криптоблокировки большого количества систем с минимальными усилиями.

Инновации: крупные игроки в программах-вымогателях продолжают находить новые инновационные способы избавления от жертв и увеличения прибыли. REvil, например, на основе проблем, с которыми столкнулись аффилированные лица предшественника GandCrab, добавил новые функции управления, чтобы упростить атаку на поставщика управляемых услуг, заразить каждого из его клиентов и удовлетворить требование выкупа каждой жертвы индивидуально. И если одна группа вводит новшества, другие неизбежно следуют за ней.

Специалисты. Бизнес-модель «программа-вымогатель как услуга» облегчает операторам набор аффилированных лиц, которые являются специалистами, поскольку чем больше жертв они могут заразить, тем больше заработают и операторы, и партнер.

Услуги. Еще одним нововведением, применяемым операторами программ-вымогателей, является предоставление таких услуг, как портал для утечки данных, где жертвы могут называть имена, стыдить и заставлять их платить. Некоторые также ведут переговоры с жертвами или даже заключают контракты с третьими сторонами, чтобы позвонить жертвам или отправить электронное письмо клиентам жертв, чтобы усилить давление.

Скрытность: по словам одной группы программ-вымогателей, «молчание - золото». Если власти не знают, что компания стала жертвой, и если компания платит, полиция не может отследить платеж в криптовалюте, что усложняет усилия по выявлению и пресечению атак или непосредственной помощи жертве.

Самообслуживание: некоторые группы используют порталы для выплаты выкупа, чтобы позволить жертвам автоматически самостоятельно предоставлять дешифратор после того, как они переведут достаточно криптовалюты для удовлетворения требования о выкупе. Такая функциональность помогает им поражать больше целей.

Оборачиваемость: операции с программами-вымогателями приходят и уходят. Сейчас активны более десятка крупных групп, которые запускают сайты утечки данных, каждая из которых имеет легионы филиалов, как и ряд других операций, которые не запускают сайты утечки данных. Есть также много мелких игроков, которые покупают готовые программы-вымогатели или перенаправляют утечку кода для самостоятельного проведения атак.

Криптовалюта. В то время как западные правительства тщательно охраняют способность «следить за деньгами» при отслеживании выплат выкупа и перемещении и отмывании виртуальной валюты преступниками, криптовалюта создает еще один уровень сложности.

Партнеры: в отличие от традиционных, иерархических преступных группировок, таких как мафия, большинство операций с программами-

вымогателями сегодня выполняются как услуги, предоставляющие портал, на котором филиалы получают вредоносное ПО для использования против жертв в обмен на долю каждого выкупа, который они платят. Эта децентрализованная модель, опираясь на эквивалент подрядчиков, делает такие операции труднее нарушить.

Сдерживание: Там нет никаких доказательств того, что арестовав часть текущего урожая киберпреступников диски следующего поколения, чтобы подумать дважды перед входом в бой.

Время на стороне правоохранительных органов

С другой стороны, как продолжают доказывать многочисленные аресты, у многих киберпреступников невероятно низкая операционная безопасность, как продолжают подчеркивать Брайан Кребс и другие наблюдатели за безопасностью.

Повторное использование адреса электронной почты и пароля по-прежнему широко распространено. Даже одна ошибка - например, если вы забыли активировать VPN - может оставить реальный IP-адрес пользователя незащищенным, что позволит полиции разоблачить его. Или доказательства могут появиться позже, например, когда подозреваемый переворачивается или когда следователи обнаруживают новые данные, связанные с перемещениями криптовалюты.

Для США и их союзников, когда подозреваемые в киберпреступности базируются или посещают юрисдикции, дружественные ФБР, их могут арестовать.

Правоохранительным органам не нужно сразу арестовывать подозреваемых. Вместо этого они могут отслеживать свои расписания отпусков. Других заманили - например, в США - поддельными предложениями о работе или консультациях.

Война на истощение

На этой неделе Европол и Министерство юстиции США совместно объявили, что с февраля в Кувейте, Польше, Румынии и Южной Корее были арестованы семь аффилированных лиц REvil и GandCrab. В их числе 22-летний гражданин Украины Ярослав Васинский, которого обвиняют в том, что он является аффилированным лицом REvil, который 2 июля ударил поставщика программного обеспечения под управлением ИТ Касею. Васинский был арестован на границе с Польшей 8 октября, и ему грозит экстрадиция в США.

В понедельник министерство юстиции также обнародовало обвинительное заключение, в котором обвиняется 28-летний гражданин России Евгений Полянин, который «предположительно находится в России, возможно, в Барнауле», в том, что он является аффилированным лицом REvil, которое поразило 22 муниципалитета Техаса в 2019 году через своего поставщика управляемых ИТ-услуг.

Также в этом году шесть подозреваемых в участии в операции по вымогательству Clop были арестованы в Украине по обвинениям, частично связанным с атаками 2019 года на южнокорейские компании.

К сожалению, как и в случае с арестом аффилированных лиц REvil, эти подозреваемые оказались в лучшем случае игроками среднего звена, а не основными операторами.

С другой стороны, одного из, возможно, полдюжины основных администраторов REvil, известного под именем UNKN (Unknown), другие участники

не видели и не слышали с июля. Некоторые предполагают, что он мертв. Или, может быть, он увидел надпись на стене и решил отказаться от киберпреступности. Возможно, он арестован и потихоньку работает с правоохранительными органами.

По мере того как западные правоохранительные органы активизируют свои усилия по борьбе с программами-вымогателями, все больше киберпреступников столкнутся с такими возможностями. Однако еще неизвестно, снизит ли это количество или серьезность атак программ-вымогателей». ***(Mathew J. Schwartz. Feds Offer $10 Million Reward for REvil Ransomware Gang // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/feds-offer-10-million-reward-for-revil-ransomware-gang-p-3137). 09.11.2021).***

***

«Министерство юстиции США добивается экстрадиции из Нидерландов московского бизнесмена, который якобы отмывал деньги от имени операции по вымогательству Ryuk.

29-летний гражданин России Денис Дубников был арестован 2 ноября властями Нидерландов после того, как его выслали из Мексики, где он пытался отдыхать, и отправили в Нидерланды, говорит Аркадий Бух, его адвокат из Нью-Йорка.

В запросе США об экстрадиции цитируется запечатанный обвинительный акт, поданный в августе большим жюри в Портленде, штат Орегон, в котором Дубников получил биткойны на сумму 400000 долларов в 2018 году от злоумышленников, связанных с Рюком, который получил криптовалюту от жертв, заплативших выкуп, сообщает The Wall Street Journal, просмотревший запрос об экстрадиции.

Дубников был обвинен США в заговоре с целью отмывания денег, сообщает Бух Журналу, добавляя, что его клиент «не признает себя виновным, потому что он не знал, что кто-то участвует в преступной деятельности».

Московская юридическая фирма Briefcase, генеральным директором которой является Дубников, утверждает, что отслеживает это дело. Как сообщает новостной сайт The Record компании по анализу угроз Recorded Future, неясно, могут ли обвинения США быть связаны со средствами, которые были переведены на криптовалютные биржи Coyote Crypto или EggChange, основанные Дубниковым.

Распространенность Рюка в адресной сфере здравоохранения

Предполагаемая сумма, полученная Дубниковым, составляла бы небольшую часть заработка Рюка. По данным аналитической компании Chainalysis, в 2020 году сумма известных выкупов в пользу Рюка составила почти 100 миллионов долларов.

В январе два исследователя безопасности сообщили, что они определили, что по крайней мере 150 миллионов долларов прибыли от криптовалют были получены Рюком от своих жертв с момента создания группы в октябре 2018 года. Брайан Картер, главный исследователь компании по безопасности HYAS, и Виталий Кремез, Генеральный директор Advanced Intelligence объявил об этих результатах, заявив, что они идентифицировали 61 биткойн-адрес, используемый операторами Ryuk и аффилированными лицами.

Злоумышленники уже давно использовали Ryuk для нацеливания на критически важные секторы, включая здравоохранение.

В октябре 2020 года предупреждение правительства США о кибербезопасности предупредило, что злоумышленники, вооруженные Рюком, представляют «возросшую и неминуемую» угрозу для больниц и медицинских учреждений.

Злоумышленники, которые владеют Рюком, являются частью группы, получившей название FIN12 исследователями безопасности. Хотя у группы есть история «многочисленных атак с использованием программ-вымогателей», еще большее беспокойство, по словам компании по кибербезопасности Mandiant, вызывает то, что почти 20% известных жертв Рюка были в секторе здравоохранения, не в последнюю очередь во время продолжающейся пандемии COVID-19.

В третьем квартале компания Coveware, занимающаяся реагированием на инциденты с вымогательством, сообщает, что Ryuk был связан с 2% расследованных инцидентов, что поместило его в 10 ведущих групп вымогателей за квартал по распространенности. По данным Coveware, по состоянию на июль, когда жертва Ryuk платила выкуп, в среднем она платила 692000 долларов.

Белый дом выступает против программ-вымогателей

Обвинение против Дубникова является лишь последним свидетельством все более активных действий администрации Байдена по сокращению ущерба, причиняемого программами-вымогателями. Эти усилия активизировались после лета, когда серьезные атаки разрушили поставщика топлива на восточном побережье Colonial Pipeline, мясоперерабатывающего гиганта JBS и разработчика программного обеспечения, управляемого ИТ-отделом, Касею, среди многих других.

Работая с союзными странами, Белый дом пытается координировать срыв и, если возможно, арест как разработчиков программ-вымогателей, так и аффилированных лиц. Эти бизнес-партнеры получают копию вредоносного ПО для криптоблокировки группы, используют его для заражения жертв и получают долю от любого выкупа, выплачиваемого жертвой.

На прошлой неделе полиция Европы объявила, что с февраля они арестовали еще шестерых подозреваемых, обвиняемых в сотрудничестве с REvil или его предшественником GandCrab.

Также на прошлой неделе Министерство юстиции объявило об аресте гражданина Украины в Польше, который обвиняется в совершении нападения на Касею, среди других атак REvil. 22- летний Ярослав Васинский был арестован 8 октября в Польше, и США добиваются его экстрадиции. Министерство юстиции также объявило, что гражданин России обвиняется в нескольких атаках REvil, но остается на свободе.

«Наше послание к преступникам-вымогателям однозначно: если вы нацелены на жертв здесь, мы будем нацелены на вас», - заявила заместитель генерального прокурора США Лиза Монако на пресс-конференции на прошлой неделе.

В настоящее время ФБР предлагает вознаграждение в размере до 10 миллионов долларов «за информацию, ведущую к идентификации или местонахождению любого человека (лиц), занимающего ключевую руководящую позицию» либо в операции вымогателя REvil, также известной как Sodinokibi, либо в операции DarkSide, которая была переименована в как BlackMatter. Кроме того,

ФБР предлагает вознаграждение в размере до 5 миллионов долларов за информацию, связанную со всеми, кто работает с этими группами, включая его филиалы.

Министерство финансов США также наложило санкции на две криптовалютные биржи за распространение программ-вымогателей.

«Очень простое» сообщение

По словам Джейсона Стира, стратега безопасности Recorded Future, арест таких подозреваемых, как Дубников и Васинский, посылает «очень простое» сообщение другим группам вымогателей. А именно: «Облегчите оплату программ-вымогателей как услуги в любой форме и приготовьтесь к аресту, если вы поедете куда-нибудь в отпуск с соглашением об экстрадиции с США или ЕС».

По его словам, многие преступники осознают, что привязанность к программам-вымогателям может создать угрозу их передвижениям или личной безопасности, особенно если они расстраивают не тех людей.

Например, ранее в этом месяце русскоязычная программа-вымогатель Conti атаковала лондонский ювелирный бизнес The House of Graff и пригрозила утечь личную информацию о своих клиентах, если она не получит выкуп. Но Daily Mail сообщила, что злоумышленники «извинились и очень быстро отозвали» свою угрозу, пообещав исключить любую информацию о клиентах из Саудовской Аравии, ОАЭ или Катара из раскрываемой информации, говорит Стир.

Следуй за деньгами

Прокуратура, обвиняющая Дубникова в получении некоторых из жертв биткойнов, выплаченных Рюку, показывает, как западные правоохранительные органы продолжают совершенствовать свои возможности по отслеживанию преступных доходов, говорит Алан Вудворд, приглашенный профессор факультета информатики в Университете Суррея.

«Слежение за деньгами - это испытанный метод отслеживания преступников», - говорит он. «Проблема заключалась в том, что криптовалюты усложняли эту технику. Однако с новыми инструментами вы можете получить некоторое представление о том, куда ушли деньги, а затем в сочетании с другими методами это может привести вас к тем, кто обналичивает преступников или даже сети денежных мулов, которые настолько эффективно распределяют деньги, чтобы предотвратить отслеживание ».

Но проблема уничтожения программ-вымогателей остается существенной, учитывая потенциальную прибыль для специалистов-практиков, а также относительную простоту таких атак - по сравнению, например, с попыткой физического ограбления банка, - говорит Вудворд.

Но даже в этом случае «правоохранительные органы направили свои большие пушки на эту тему» и начали уделять зачастую значительное количество времени и усилий, которые требуются для сбора доказательств, выявления подозреваемых и создания дел, говорит он.

«Любой, кто участвует в цепочке поставок программ-вымогателей, теперь является мишенью для правоохранительных органов. Любого, кто поддерживает, поддерживает и содействует этим преступникам, так же важно поймать, как и тех, кто запускает атаки», - говорит Вудворд. «Суть в том, что если ваша способность управлять инфраструктурой для запуска атаки или получения прибыли за счет

обналичивания выкупа будет лишена, преступники должны искать в другом месте». ***(Mathew J. Schwartz. Russian National Charged With Laundering Ryuk Ransoms // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russian-national-charged-laundering-ryuk-ransoms-a-17910). 15.11.2021).***

***

«8 ноября 2021 года правоохранительные органы США и Европейского союза объявили, что в отношении связанной с Россией группы программ-вымогателей REvil был предпринят ряд действий, включая ряд арестов. Министерство юстиции США («Министерство юстиции») обнародовало документы, относящиеся к августовскому обвинительному заключению против двух человек в Далласе по обвинению в причастности к атакам программы-вымогателя REvil на несколько американских предприятий. Европейские власти, Европол, также объявили, что полиция Румынии и Южной Кореи арестовала пять человек, предположительно связанных с REvil.

REvil, сокращение от Ransowmare-Evil, - одна из самых печально известных банд вымогателей. Группу обвиняют в организации в этом году нескольких атак на крупные компании и организации, включая поставщика мяса JBS S.A. и технологическую компанию Kaseya. JBS заплатила выкуп в размере 11 миллионов долларов, а Касея заявила, что отказалась платить хакерам.

Арест Европолом филиалов REvil стал результатом международного расследования GoldDust, в котором участвовали правоохранительные органы 17 стран, включая США, Великобританию, Францию и Германию. Предполагаемые хакеры подозреваются в причастности к примерно 5000 заражениям с помощью программ-вымогателей. Согласно двум обвинительным заключениям Далласа, предполагаемые хакеры, гражданин Украины и гражданин России, обвиняются в заговоре с целью совершения мошенничества и отмывания денег, а также других компьютерных преступлений против нескольких американских предприятий. Министерство юстиции также объявило, что оно конфисковало выкуп в размере 6,1 миллиона долларов за одного из обвиняемых хакеров. Министерство финансов США объявило о действиях, направленных на предотвращение атак программ-вымогателей и обменов виртуальной валютой, отмывающих незаконные доходы. Например, он ввел санкции против двух лиц, которым были предъявлены обвинения, а также против Chatex, связанной с Россией криптовалютной биржи, которая якобы способствовала платежам программ-вымогателей». ***(Russia-Linked REvil Hackers and Their Affiliates Hit with Arrests by the U.S. and International Allies // Hunton Andrews Kurth LLP (https://www.huntonprivacyblog.com/2021/11/09/russia-linked-revil-hackers-and-their-affiliates-hit-with-arrests-by-the-u-s-and-international-allies/). 09.11.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«По словам исследователей из подразделения 42 компании Palo Alto Networks, злоумышленники взламывают критически важные системы на международном уровне, используя недавно исправленную уязвимость в продукте Zoho ManageEngine ADSelfService Plus. Отчет об исследовании был опубликован в сотрудничестве с Центром сотрудничества в области кибербезопасности Агентства национальной безопасности.

По данным Unit 42, злоумышленники, вероятно, китайская группа угроз, использовали арендованную инфраструктуру в США для сканирования сотен уязвимых организаций в Интернете, которые не пропатчили свои системы исправлением, выпущенным для CVE-2021-40539.

В среду CISA выпустила директиву под названием «Обязательная операционная директива 22-01 для снижения «значительного риска известных эксплуатируемых уязвимостей »для всех федеральных, исполнительных органов власти, департаментов и агентств в целях защиты федеральной информации и информационных систем и планирует каталогизировать Известные эксплуатируемые уязвимости. Согласно текущему каталогу, 17 ноября все федеральные агентства должны исправить уязвимость CVE-2021-40539 и применить исправление.

Директива призывает все федеральные департаменты и агентства обновить перечисленные затронутые технологии или программное обеспечение - если они используются - в течение установленного периода.

Жертвы Зохо

Кампания Zoho, начавшаяся 17 сентября, как сообщается, продолжалась до первой половины октября и поставила под угрозу как минимум девять неопознанных глобальных организаций в секторах технологий, обороны, здравоохранения, энергетики и образования. По словам исследователей, злоумышленники атаковали не менее 370 серверов Zoho ManageEngine только в США.

Считается, что идентифицированные жертвы - всего лишь «острие копья», и ожидается, что в ближайшее время их станет больше, - сказал новостной портал CNN Райан Олсон, высокопоставленный руководитель Palo Alto Networks. Он добавляет, что только одна из подтвержденных жертв - американская компания.

Используя шпионаж в качестве основного мотива, «хакеры украли пароли у некоторых целевых организаций с целью поддержания долгосрочного доступа к этим сетям», - сказал Олсон CNN.

Атрибуция

В сообщении блога говорится, что тактика и инструменты, используемые в кампании, основанные на анализе сигнатур кода и полезной нагрузки

исследователями, вероятно, принадлежат китайской группе угроз 3390, также известной как TG-3390, Emissary Panda и APT27.

«Мы видим, что TG-3390 использовал веб-эксплойт и другую популярную китайскую веб-оболочку под названием ChinaChopper в качестве исходной точки опоры, прежде чем использовать законные украденные учетные данные для бокового перемещения и атак на контроллер домена», - говорят исследователи. Хотя веб-оболочки и эксплойты могут показаться разными, инструменты извлечения, используемые после того, как злоумышленники получили доступ в среду жертвы, были похожими, добавляют они.

Эксплуатация

По словам исследователей, после первоначального использования уязвимости CVE-2021-40539 злоумышленник развертывает полезную нагрузку, которая устанавливает веб-оболочку Godzilla в систему жертвы. Затем функционально богатая веб-оболочка анализирует входящие HTTP-запросы POST, расшифровывает данные с помощью секретного ключа, выполняет расшифрованное содержимое для выполнения дополнительных функций и возвращает результат через HTTP-ответ, добавляют они.

По словам исследователей, хотя Godzilla была последовательно развернута во всех системах-жертвах, небольшая группа взломанных организаций получила модифицированную версию нового бэкдора под названием NGLite.

Исследователи отмечают, что злоумышленники использовали веб-оболочку или полезную нагрузку NGLite для выполнения команд и латерального перемещения к другим системам в сети, в то же время извлекая интересующие файлы, просто загружая их с веб-сервера.

Наконец, получив доступ к контроллерам домена, злоумышленники развертывают KdcSponge, новый инструмент для кражи учетных данных. Исследователи говорят: «KdcSponge внедряется в процесс службы подсистемы Local Security Authority и перехватывает определенные функции для сбора имен пользователей и паролей от учетных записей, пытающихся пройти аутентификацию в домене через Kerberos».

Фирма по кибербезопасности SophosLabs сообщила в воскресенье, что получила отчеты от клиентов о том, что злоумышленники использовали уязвимость Zoho ManageEngine ADSelfServicePlus.

Профилактика

Роб Джойс, директор по кибербезопасности Агентства национальной безопасности США, призывает клиентов просмотреть сообщение блога Unit 42 на предмет индикаторов взлома и защиты.

Zoho ранее выпустила ADSelfService Plus build 6114, чтобы исправить эту проблему.

История повторяется

Военные подрядчики являются повторяющейся мишенью для иностранных противников, как это было свидетель в начале этого года.

Когда уязвимость ManageEngine впервые обнаружилась, Агентство по кибербезопасности и безопасности инфраструктуры в сентябрьском предупреждении отметило, что продвинутые постоянные злоумышленники активно

используют недавно обнаруженные уязвимости в решении для самообслуживания управления паролями ManageEngine ADSelfService Plus и что нападениями становятся подрядчики по защите. исполнителями угроз.

«Любая компания, ведущая дела с Пентагоном, может иметь в своих электронных письмах ряд данных об оборонных контрактах, которые могут быть интересны иностранным шпионам. В целом доступ к этой информации может быть действительно ценным», - сказал Олсон CNN. И он сказал, что это не означает только секретную информацию: «Даже если это просто информация о том, как обстоят дела в бизнесе, она ценна». ***(Mihir Bagwe. NSA Reports: Espionage Group Breaches Critical Systems // Information Security Media Group, Corp. (https://www.govinfosecurity.com/nsa-reports-espionage-group-breaches-critical-systems-a-17860). 08.11.2021).***

***

«Исследователи из Forescout Research Labs обнаружили набор из 13 новых уязвимостей программного обеспечения медицинских устройств, влияющих на стек TCP / IP Siemens Nucleus. Пакет программного обеспечения используется в критически важных устройствах, включая мониторы пациента, рентгеновские аппараты, устройства для анестезии и ультразвуковые устройства.

В случае эксплуатации уязвимости могут привести к атакам типа «отказ в обслуживании» (DoS), утечке информации и удаленному выполнению кода.

Исследователи обнаружили, что тысячи медицинских устройств полагаются на программное обеспечение Nucleus. Государственные, розничные и финансовые поставщики также полагаются на Nucleus. Агентство кибербезопасности и безопасности инфраструктуры (CISA) выпустило рекомендации относительно уязвимостей, и с тех пор Siemens выпустила исправления для всех 13 уязвимостей.

Исследователи протестировали каждую уязвимость в лабораториях Forescout. В ходе одного моделирования исследователи смогли успешно манипулировать уязвимостями и полностью отключить имитацию больницы, сообщает CNN. Уязвимости позволили им выключить свет в больнице и отключить ее систему отопления, вентиляции и кондиционирования воздуха после получения доступа к ее сети.

Недавнее исследование Армиса показало, что ИТ-специалисты больше всего озабочены безопасностью систем отопления, вентиляции и кондиционирования воздуха и электрических систем, машин визуализации, киосков регистрации, оборудования для выдачи лекарств и оборудования для мониторинга жизненно важных функций. Несмотря на поток новостей о программах-вымогателях и уязвимостях медицинских устройств, риски инфраструктуры больниц также создают значительные риски для безопасности пациентов.

Forescout призвал организации исправлять устройства для защиты от уязвимостей. Установка исправлений на медицинские устройства может быть чрезвычайно сложной задачей, особенно потому, что многим организациям сложно определить, сколько устройств находится в их сетях. Кроме того, устаревшие устаревшие устройства может быть сложно или невозможно обновить. Очень важно,

чтобы организации вели точную инвентаризацию своих подключенных устройств, чтобы избежать негативного воздействия на безопасность.

Forescout рекомендовал организациям обнаружить и провести инвентаризацию всех устройств, на которых установлено программное обеспечение Nucleus. В отчете говорится, что организациям здравоохранения следует также рассмотреть возможность применения «средств контроля сегментации и надлежащей сетевой гигиены для снижения риска, связанного с уязвимыми устройствами».

«Ограничьте внешние пути связи и изолируйте или удерживайте уязвимые устройства в зонах в качестве смягчающего контроля, если они не могут быть исправлены или пока они не могут быть исправлены».

Затронутые организации должны постоянно отслеживать прогрессивные исправления, выпускаемые поставщиками затронутых устройств, и создавать план исправления для уязвимых активов, а также отслеживать весь сетевой трафик на предмет вредоносных пакетов, которые могут попытаться использовать эти уязвимости.

CISA призвала организации принять защитные меры, включая минимизацию уязвимости сети для всех устройств системы управления, чтобы гарантировать, что они недоступны из Интернета. CISA также рекомендовала организациям размещать сети систем управления и удаленные устройства за межсетевыми экранами, а затем изолировать их от бизнес-сети.

Агентство также напомнило затронутым организациям использовать VPN, признавая при этом, что сами VPN могут иметь уязвимости и безопасны только на уровне подключенных устройств.

«Организации, наблюдающие за любой предполагаемой вредоносной деятельностью, должны следовать установленным внутренним процедурам и сообщать о своих выводах в CISA для отслеживания и сопоставления с другими инцидентами», - заключил CISA. «Нет известных публичных эксплойтов, специально предназначенных для этих уязвимостей». ***(Jill McKeon. Researchers Discover 13 Medical Device Security Vulnerabilities // TechTarget, Inc. (https://healthitsecurity.com/news/researchers-discover-13-medical-device-security-vulnerabilities). 12.11.2021).***

***

«Пара экспертов по безопасности из TrojanSource нашла новый способ атаковать исходный код компьютера, который заставляет компилятора (и человека-рецензента) думать, что код безопасен. Николас Баучер и Росс Андерсон, оба из Кембриджского университета, разместили на веб-странице TrojanSource статью, в которой подробно описаны уязвимость и способы ее устранения.

Как описывают Баучер и Андерсон, уязвимость включает в себя состязательные атаки, совершаемые гнусными типами, использующими управляющие символы Unicode для изменения порядка символов в исходном коде, который программистам кажется законным. В частности, уязвимость связана с использованием алгоритма «Bidi» в Unicode (международный стандарт кодирования,

который может использоваться на разных языках), где символы можно размещать как слева направо, так и справа налево, потому что некоторые языки, такие как Иврит и арабский пишутся и читаются справа налево.

Уязвимость существует потому, что алгоритмы, обрабатывающие такой код, не учитывают, что некоторые символы, которые читаются слева направо, могут иметь другое значение или назначение, если они читаются справа налево. Поскольку практически все самые популярные языки программирования, используемые сегодня - C, C +, Java, Python, Go, Rust и JavaScript - поддерживают Unicode, это означает, что практически все программы потенциально подвержены риску.

В качестве примера Баучер и Андерсон показывают такую строку кода, как:

/ * только начинающие администраторы * / if (isAdmin) {

Может быть изменено на:

/ * if (isAdmin) {только для начинающих администраторов * /

Первая строка - это безобидный комментарий, вставленный программистом, вторая - это код, который может быть использован хакером для достижения желаемого результата. Исследователи предполагают, что уязвимость представляет собой серьезную угрозу для цепочек поставок программного обеспечения - если такие уязвимости будут использованы, они могут повлиять на последующее программное обеспечение, позволив им унаследовать ту же уязвимость.

Поскольку уязвимость существует для такого большого количества языков программирования, ее раскрытие было сначала согласовано с должностными лицами, отвечающими за соблюдение правил для таких языков, что дало им время для внесения изменений в компиляторы и интерпретаторы для учета и смягчения такой угрозы». ***(Bob Yirka. 'Trojan Source' bug a novel way to attack program encodings // Tech Xplore (https://techxplore.com/news/2021-11-trojan-source-bug-encodings.html). 03.11.2021).***

***

«Исследователи из ETH Zurich обнаружили серьезные уязвимости в устройствах памяти DRAM, которые широко используются в компьютерах, планшетах и смартфонах. Уязвимости опубликованы совместно с Национальным центром кибербезопасности, который впервые присвоил ей идентификационный номер.

Когда мы просматриваем Интернет на портативном компьютере или пишем сообщения на смартфоне, нам всем нравится думать, что мы достаточно защищены от хакерских атак, если у нас установлены последние обновления программного обеспечения и антивирусное программное обеспечение. Но что, если проблема не в программном обеспечении, а в оборудовании? Группа исследователей под руководством Кавеха Разави из ETH Zurich вместе с коллегами из Vrije Universiteit Amsterdam и Qualcomm Technologies недавно обнаружили фундаментальные уязвимости, влияющие на компонент памяти, называемый DRAM, в основе всех современных компьютерных систем.

Результаты их исследования были приняты для публикации на флагманской конференции по ИТ-безопасности, а Швейцарский национальный центр кибербезопасности (NCSC) выпустил номер Common Vulnerabilities and Exposures

(CVE). Это первый случай, когда удостоверение личности CVE было выдано NCSC в Швейцарии (см. Вставку ниже). По шкале от 0 до 10 серьезность уязвимости была оценена как 9.

Слабость DRAM

«Основная хорошо известная проблема с DRAM называется Rowhammer и известна уже несколько лет», - объясняет Разави. Rowhammer - это атака, которая использует фундаментальную слабость современной памяти DRAM. DRAM - это сокращение от динамической памяти с произвольным доступом, где «динамический» означает, что все данные, хранящиеся в ней, являются энергозависимыми и должны обновляться довольно часто - на самом деле, более десяти раз в секунду. Это связано с тем, что микросхемы DRAM используют только одну пару конденсатор-транзистор для хранения и доступа к одному биту информации.

У конденсаторов утечка заряда с течением времени, и как только они потеряли слишком много заряда, компьютер больше не знает, было ли значение сохраненного бита «1» (что может соответствовать высокому заряду) или «0» (низкому заряду). Вдобавок ко всему, каждый раз, когда строка памяти активируется для считывания или записи (биты расположены в виде шахматной доски из строк и столбцов), токи, протекающие внутри микросхемы, могут вызвать разряд конденсаторов. соседние ряды для более быстрой утечки заряда…

«Это неизбежное следствие постоянно увеличивающейся плотности электронных компонентов на микросхемах DRAM», - говорит Патрик Джаттке, доктор философии. студент в группе Разави на факультете информационных технологий и электротехники. Это означает, что, многократно активируя - или «забивая» - строку памяти («агрессор»), злоумышленник может вызвать битовые ошибки в соседней строке, также называемой строкой «жертвы». Эта битовая ошибка в принципе может быть использована для получения доступа к закрытым областям внутри компьютерной системы, не полагаясь на какие-либо программные уязвимости.

«После того, как Rowhammer был впервые обнаружен около десяти лет назад, производители микросхем внедрили меры по смягчению последствий внутри модулей DRAM, чтобы решить эту проблему, - говорит Разави: - К сожалению, проблема до сих пор не решена». Средство предотвращения обновления целевой строки (TRR), на которое ссылается Razavi, состоит из различных схем, встроенных в память, которые могут обнаруживать необычно высокие частоты активации определенных строк и, следовательно, угадывать, где запускается атака. В качестве контрмеры схема управления преждевременно обновляет предполагаемую строку-жертву и, следовательно, предотвращает возможные битовые ошибки.

Сложная обработка молотком

Разави и его коллеги обнаружили, что эта аппаратная «иммунная система» обнаруживает только довольно простые атаки, такие как двусторонние атаки, при которых нацелены две строки памяти, смежные со строкой жертвы, но их все еще можно обмануть более изощренным ударом. Они разработали программное обеспечение, удачно названное «Blacksmith», которое систематически пробует сложные схемы удара, в которых активируется разное количество рядов с разными

частотами, фазами и амплитудами в разных точках цикла молотка. После этого он проверяет, не привел ли определенный шаблон к битовым ошибкам.

Результат был ясным и тревожным: «Мы увидели, что для всех 40 различных модулей памяти DRAM, которые мы тестировали, Blacksmith всегда мог найти шаблон, который вызывал битовые ошибки Роухаммера», - говорит Разави. Как следствие, текущая память DRAM потенциально подвержена атакам, для которых нет линии защиты - на долгие годы. Пока производители микросхем не найдут способы обновить меры по смягчению последствий для будущих поколений микросхем DRAM, компьютеры будут оставаться уязвимыми для атак Rowhammer.

Этический аспект

Разави хорошо осведомлен об этическом аспекте своего исследования: «Мы, очевидно, хотим сделать мир более безопасным, и мы считаем, что важно, чтобы потенциальные жертвы знали об этой угрозе, чтобы они могли сделать осознанный выбор». К счастью, добавляет он, эти жертвы вряд ли будут обычными пользователями, поскольку есть гораздо более простые способы взломать большинство компьютеров (напоминание о том, что использование новейшего антивирусного программного обеспечения и обновления устройств по-прежнему важны). Тем не менее, вполне возможно, что национальные государства или влиятельные организации могут использовать такие атаки для важных целей. Чтобы дать производителям время отреагировать на новые уязвимости, Разави и его коллеги уже проинформировали их несколько месяцев назад. Они также тесно сотрудничали с NCSC, который отвечает за скоординированную публикацию обнаруженных уязвимостей в Швейцарии.

В будущем исследователи ETH хотят изучить еще более изощренные способы создания битовых ошибок. Это может помочь производителям микросхем протестировать свои устройства и отреагировать на все возможные атаки молотком. «Конечно, хотя мы выпускаем код, который показывает, как запускать битовые ошибки, в настоящее время мы не раскрываем код, который злоупотребляет этими ошибками», - говорит Разави». ***(Oliver Morsch. Serious security vulnerabilities in DRAM memory devices // Tech Xplore (https://techxplore.com/news/2021-11-vulnerabilities-dram-memory-devices.html). 16.11.2021).***

***

«Сегодня Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило Руководства по реагированию на инциденты кибербезопасности и реагирования на уязвимости федерального правительства. Разработанные в соответствии с Указом 14028 «Повышение кибербезопасности нации», учебные пособия предоставляют федеральным гражданским агентствам стандартный набор процедур для реагирования на уязвимости и инциденты, влияющие на сети федеральной гражданской исполнительной власти.

«Публикации, которые мы выпускаем сегодня, предназначены для улучшения и стандартизации подходов, используемых федеральными агентствами для выявления, устранения и восстановления уязвимостей и инцидентов, влияющих на их системы», - сказал Мэтт Хартман, заместитель исполнительного помощника

директора по кибербезопасности. «Этот важный шаг, начатый в соответствии с Указом президента Байдена о кибербезопасности, позволит проводить более всесторонний анализ и устранять уязвимости и инциденты на гражданском предприятии. Мы призываем наших партнеров из государственного и частного секторов пересмотреть инструкции, чтобы оценить свою собственную уязвимость и методы реагирования на инциденты».

Пособие по реагированию на инциденты применяется к инцидентам, которые связаны с подтвержденной злонамеренной деятельностью в киберпространстве и для которых серьезный инцидент был объявлен или еще не был разумно исключен. Пособие по реагированию на уязвимости применяется к любой уязвимости, которая, по наблюдениям, используется злоумышленниками для несанкционированного доступа к вычислительным ресурсам. Этот сценарий основан на обязательной операционной директиве 22-01 CISA и стандартизирует высокоуровневый процесс, которому следует следовать при реагировании на эти уязвимости, которые представляют значительный риск для федерального правительства, частного и государственного секторов.

Опираясь на уроки, извлеченные из предыдущих инцидентов, и внедряя передовой опыт отрасли, CISA намеревается использовать эти два сценария для улучшения практики реагирования на кибербезопасность и операционных процедур не только для федерального правительства, но также для организаций государственного и частного секторов. Пособия содержат контрольные списки для реагирования на инциденты, подготовки реагирования на инциденты и реагирования на уязвимости, которые могут быть адаптированы для любой организации для отслеживания необходимых действий до их завершения.

Для получения дополнительных сведений о сценариях и роли CISA в поддержке указа президента Байдена о кибербезопасности, посетите Указ о повышении кибербезопасности страны». ***(CISA RELEASES INCIDENT AND VULNERABILITY RESPONSE PLAYBOOKS TO STRENGTHEN CYBERSECURITY FOR FEDERAL CIVILIAN AGENCIES // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen). 16.11.2021).***

***

«Киберпреступники становятся все более продвинутыми, поскольку они продолжают находить новые способы проведения атак, и некоторые теперь готовы покупать уязвимости нулевого дня, что более традиционно ассоциируется с национальными государствами.

Знание об уязвимостях и эксплойтах может дорого обойтись на подпольных форумах, потому что возможность воспользоваться ими может быть очень прибыльной для киберпреступников. Это особенно важно, если речь идет об уязвимости нулевого дня, о которой не знают исследователи кибербезопасности, потому что злоумышленники знают, что у потенциальных жертв не будет возможности применить обновления безопасности для защиты от нее.

Например, через несколько недель после того, как в начале этого года были обнаружены уязвимости Microsoft Exchange, киберпреступники поспешили

воспользоваться ими как можно быстрее, чтобы воспользоваться возможностью проводить атаки до того, как патчи безопасности были широко применены.

Уязвимости нулевого дня обычно развертываются с помощью хорошо обеспеченных ресурсами и поддерживаемых государством хакерских операций, но анализ, проведенный исследователями кибербезопасности из Digital Shadows, подробно описывает, как на досках объявлений в темной сети все чаще говорят о криминальном рынке нулевого дня.

«Этот рынок чрезвычайно дорогой и конкурентный, и обычно он был прерогативой спонсируемых государством групп угроз. Однако некоторые известные киберпреступные группы (читай: банды вымогателей) накопили невероятные состояния за последние годы и теперь могут конкурировать с традиционными покупателями эксплойтов нулевого дня», - сказал Digital Shadows.

«Государства могут законным образом приобретать эксплойты нулевого дня у компаний, которые занимаются исключительно созданием этих инструментов», - сказал ZDNet Стефано Де Блази, исследователь угроз из Digital Shadows.

«Однако, когда эти инструменты разрабатываются киберпреступниками вне закона, вероятно, легче идентифицировать клиентуру из мира киберпреступников; однако есть лишь горстка киберпреступников, которые могут позволить себе стоимость эксплойта нулевого дня».

Подобные уязвимости могут стоить даже миллионы долларов, но это цена, которая может быть доступной для успешной группы программ-вымогателей, которая зарабатывает миллионы на каждой успешной атаке программ-вымогателей, и они могут легко вернуть свои затраты, если уязвимость сработает так, как задумано, предоставив надежные средства проникновения в сети.

Но есть еще один метод заработка на исследуемых уязвимостях, который может передать их в руки менее искушенных киберпреступников - так называемый «эксплойт как услуга».

Вместо того, чтобы сразу продать уязвимость, киберпреступник, обнаруживший ее, может сдать ее в аренду другим. Это потенциально начинает приносить им деньги быстрее, чем если бы они прошли через сложный процесс продажи, и они могли бы продолжать зарабатывать на этом деньги в течение долгого времени. У них также есть возможность в конечном итоге продать «нулевой день», если они устанут сдавать его в аренду.

«Эта модель позволяет разработчикам нулевого дня получать значительную прибыль, сдавая в аренду эксплойт нулевого дня в ожидании окончательного покупателя. Кроме того, с помощью этой модели арендаторы могут протестировать предлагаемый нулевой день, а затем решить, стоит ли покупать эксплойт на на исключительной или неисключительной основе», - говорится в сообщении.

Продажа поддерживаемым государством хакерским группам по-прежнему является предпочтительным вариантом для некоторых разработчиков нулевого дня, но растущий интерес к подобным эксплойтам на подпольных форумах указывает на то, что некоторые киберпреступные группы приближаются к уровню поддерживаемых государством операций.

«Развитие бизнес-модели использования как услуги подтверждает, что киберпреступная среда постоянно растет как с точки зрения изощренности, так и с

точки зрения профессионализма. Некоторые известные преступные группы теперь могут конкурировать с точки зрения технических навыков с участниками, спонсируемыми государством; в частности, многие известные группы программ-вымогателей накопили достаточно финансовых ресурсов для покупки рекламы нулевого дня, рекламируемой в незаконных средах», - пояснил Де Блази.

Природа уязвимостей нулевого дня означает, что защита сетей от них - сложная задача, но методы кибербезопасности, такие как применение критических обновлений безопасности сразу после их выпуска, могут помешать киберпреступникам получить длительное окно, чтобы воспользоваться уязвимостями. У организаций также должен быть план действий в случае обнаружения нарушений.

«Хорошо продуманные и задокументированные стратегии реагирования на инциденты могут иметь решающее значение для реагирования на любого злоумышленника, который мог получить доступ к среде цели», - сказал Де Блази». ***(Danny Palmer. Ransomware gangs are now rich enough to buy zero-day flaws, say researchers // ZDNet (https://www.zdnet.com/article/ransomware-gangs-are-now-rich-enough-to-buy-zero-day-flaws-say-researchers/). 16.11.2021).***

***

«Агентства по кибербезопасности из Австралии, Великобритании и США в среду выпустили совместное консультативное предупреждение об активной эксплуатации уязвимостей Fortinet и Microsoft Exchange ProxyShell спонсируемыми государством Ирана субъектами для получения первоначального доступа к уязвимым системам для последующих действий, включая кражу данных. и программы-вымогатели.

По данным Агентства США по кибербезопасности и безопасности инфраструктуры (CISA), Федерального агентства США по кибербезопасности и безопасности инфраструктуры (CISA), злоумышленник, как полагают, использовал несколько уязвимостей Fortinet FortiOS, начиная с марта 2021 года, а также уязвимость удаленного выполнения кода, влияющую на серверы Microsoft Exchange Server с октября 2021 года. Бюро расследований (ФБР), Австралийский центр кибербезопасности (ACSC) и Национальный центр кибербезопасности Великобритании (NCSC).

К целевым жертвам относятся австралийские организации и широкий круг организаций в различных критически важных инфраструктурных секторах США, таких как транспорт и здравоохранение. Список используемых недостатков приведен ниже -

CVE-2021-34473 (оценка CVSS: 9,1) - уязвимость удаленного выполнения кода в Microsoft Exchange Server (также известная как « ProxyShell»).

CVE-2020-12812 (оценка CVSS: 9,8) - обход FortiOS SSL VPN 2FA путем изменения регистра имени пользователя

CVE-2019-5591 (оценка CVSS: 6,5) - конфигурация FortiGate по умолчанию не проверяет идентичность сервера LDAP.

CVE-2018-13379 (оценка CVSS: 9,8) - утечка системных файлов FortiOS через SSL VPN через специально созданные запросы ресурсов HTTP.

Помимо использования недостатков FortiOS для получения доступа к уязвимым сетям, CISA и ФБР заявили, что они наблюдали, как злоумышленник злоупотреблял устройством Fortigate в мае 2021 года, чтобы закрепиться на веб-сервере, на котором размещен домен для муниципального правительства США. В следующем месяце участники APT «использовали устройство Fortigate для доступа к сетям экологического контроля, связанным с американской больницей, специализирующейся на охране здоровья детей», - говорится в сообщении.

Разработка знаменует собой второй раз, когда правительство США предупреждает о продвинутых постоянных группах угроз, нацеленных на серверы Fortinet FortiOS, используя CVE-2018-13379, CVE-2020-12812 и CVE-2019-5591 для компрометации систем, принадлежащих государственным и коммерческим организациям…». ***(Ravie Lakshmanan. U.S., U.K. and Australia Warn of Iranian Hackers Exploiting Microsoft, Fortinet Flaws // The Hacker News (https://thehackernews.com/2021/11/us-uk-and-australia-warn-of-iranian.html). 17.11.2021).***

***

«Отчет за третий квартал 2021 года показал, что количество CVE, связанных с программами-вымогателями, увеличилось на 4,5%, а количество семейств программ-вымогателей - на 3,4% по сравнению со вторым кварталом 2021 года.

В этом квартале при атаках программ-вымогателей было использовано десяток новых уязвимостей, в результате чего общее количество ошибок, связанных с программами-вымогателями, достигло 278. По данным исследователей, это на 4,5% больше, чем во втором квартале.

Пять из новичков могут использоваться для достижения удаленного выполнения кода (RCE), а два могут использоваться для использования веб-приложений и запуска атак типа «отказ в обслуживании» (DoS). Это никогда не бывает хорошими новостями, но это особенно неприятно, учитывая, что в этом квартале также были отмечены распространенные DoS-атаки (DDoS), которые побили все рекорды, согласно отдельному исследованию.

Новости о новых уязвимостях, которые были обнаружены операторами программ-вымогателей, поступают из отчета Ivanti за третий квартал 2021 года, посвященного индексу вымогателей, опубликованного во вторник и проведенного совместно с Cyber Security Works и Cyware.

Ежеквартальный анализ программ-вымогателей также показал, что группы программ-вымогателей все еще находят и используют уязвимости нулевого дня до того, как будут вылуплены и исправлены CVE. Показательный пример: критикуемая банда вымогателей REvil обнаружила и использовала недостатки в программном обеспечении Kaseya VSA, поскольку служба безопасности компании все еще работала над тремя исправлениями.

2 июля банда REvil вскрыла три нулевых дня в платформе Virtual System / Server Administrator (VSA) Касеи в более чем 5000 атак. По состоянию на 5 июля всемирная атака была начата в 22 странах, охватив не только клиентскую базу поставщика управляемых услуг (MSP) Kaseya, но и учитывая, что многие из них

используют VSA для управления сетями других предприятий, цепляясь за этих MSP». собственные клиенты.

Число программ-вымогателей растет на всех фронтах

В третьем квартале также было обнаружено девять новых уязвимостей с более низким рейтингом опасности, связанных с программами-вымогателями. Кроме того, обновление индекса вымогателей за третий квартал за 2021 год выявило группы вымогателей, расширяющие свой арсенал атак за счет 12 новых ассоциаций уязвимостей в третьем квартале,

Анализ третьего квартала также выявил пять новых семейств программ-вымогателей, в результате чего общее количество программ-вымогателей достигло 151. Новые группы программ-вымогателей быстро воспользовались некоторыми из наиболее опасных уязвимостей всего через несколько недель после того, как они начали набирать популярность, например PrintNightmare, PetitPotam и ProxyShell.

Методы, используемые в атаках программ-вымогателей, также становятся все более изощренными. Одним из примеров, приведенных в анализе Ivanti, является дроппер как услуга - услуга, которая позволяет технически не подкованным / криминальным субъектам распространять вредоносное ПО с помощью программ-дропперов, которые могут выполнять вредоносную полезную нагрузку на компьютере жертвы.

Другой - «троян как услуга», также известный как «вредоносное ПО как услуга»: услуга, которая позволяет любому, у кого есть подключение к Интернету, арендовать специализированные вредоносные услуги, позволяя им приобретать, внедрять и получать прибыль от этой услуги. облако с нулевой установкой.

Кажется, что все плохое можно арендовать: программа-вымогатель как услуга (RaaS), например, способствует распространению программ-вымогателей, избавляя мошенников от необходимости связываться с кодом.

Старое вино, новые бутылки с программами-вымогателями

В отчете также обнаружено, что три уязвимости, относящиеся к 2020 году или ранее, были вновь связаны с программами-вымогателями в третьем квартале 2021 года, в результате чего общее количество старых уязвимостей, связанных с программами-вымогателями, достигло 258: колоссальные 92,4 процента всех уязвимостей, связанных с программами-вымогателями.

Анализ показал, что группа программ-вымогателей Cring является ярким примером: банда нацелена на две старые уязвимости ColdFusion - CVE-2009-3960 и CVE-2010-2861, которые исправлялись в течение 11 лет.

Шринивас Муккамала, старший вице-президент Ivanti по продуктам безопасности, сказал в пресс-релизе, что автоматизация может спасти ваш бекон: «Очень важно, чтобы организации применяли упреждающий, основанный на оценке рисков подход к управлению исправлениями и использовали технологии автоматизации, чтобы сократить среднее время на обнаружение., обнаруживать, устранять и реагировать на атаки программ-вымогателей и другие киберугрозы».

Анудж Гоэль, генеральный директор Cyware, сказал «да» автоматизации, а также обмену данными для защиты организаций от программ-вымогателей: «Это исследование подчеркивает, что программы-вымогатели продолжают развиваться и становятся все более опасными из-за катастрофического ущерба, который они могут

нанести. целевые организации. Более сложным для многих организаций является неспособность вертикальных отраслей быстро обмениваться конкретными IOC независимо от их отрасли таким образом, чтобы их было легко курировать, вводить в действие и распространять, чтобы принять меры до того, как произойдет атака.

«Управление организационными рисками означает, что компании должны искать стратегию коллективной защиты, чтобы иметь постоянный обзор атак и поверхностей риска соответственно, чтобы уменьшить огромные потери для репутации, клиентов и финансов. Чем больше кибер-команды смогут подключиться к автоматизации и процессам ИТ, тем лучше и эффективнее они будут бороться с программами-вымогателями». ***(Lisa Vaas. 12 New Flaws Used in Ransomware Attacks in Q3 // Threatpost (https://threatpost.com/12-new-flaws-used-in-ransomware-attacks-in-q3/176137/). 09.11.2021).***

***

«Самый крупный реестр программного обеспечения пакетов Node.js, npm, обнаружил множество недостатков безопасности, которые были обнаружены и исправлены недавно.

Первый недостаток связан с утечкой имен частных пакетов npm на «реплике» сервера npmjs.com - каналы с которых потребляются сторонними службами.

Принимая во внимание, что второй недостаток позволяет злоумышленникам публиковать новые версии любого существующего пакета npm, которым они не владеют или не имеют прав, из-за неправильной проверки авторизации.

Утечка имен приватных пакетов npm

На этой неделе материнская компания npm, GitHub, раскрыла два недостатка безопасности, которые были выявлены и исправлены в реестре npm в период с октября по этот месяц.

Первый - это утечка данных на сервере репликации npmjs, вызванная «плановым обслуживанием». Утечка раскрыла список имен частных пакетов npm, но не содержимое этих пакетов во время окна обслуживания.

«Во время обслуживания базы данных, которая поддерживает общедоступную реплику npm на сайте replicate.npmjs.com, были созданы записи, которые могут раскрывать имена частных пакетов», - заявляет в своем блоге директор по безопасности GitHub Майк Хэнли.

«Это на короткое время позволило потребителям replicate.npmjs.com потенциально идентифицировать имена частных пакетов из-за записей, опубликованных в общедоступной ленте изменений. Никакая другая информация, включая содержимое этих частных пакетов, не была доступна в любое время».

Обратите внимание: хотя содержимое частных пакетов не было раскрыто, зная имена частных пакетов, злоумышленникам достаточно для проведения целенаправленных атак путаницы зависимостей и типосквоттинга в автоматическом режиме, что мы видели снова и снова.

Утечка особенно касается частных библиотек npm с ограниченными областями видимости, которые выглядят как « @ owner / package » и были созданы до 20 октября. Имена таких библиотек были раскрыты «между 21 октября 13: 12: 10Z UTC и 29 октября 15: 51: 00Z UTC», согласно GitHub.

Утечка данных была обнаружена GitHub 26 октября, а 29 октября все записи, содержащие имена частных пакетов, были удалены из базы данных репликации npm. Хотя GitHub предупреждает, что, несмотря на это, сервис replicate.npmjs.com используется третьими сторонами, которые, следовательно, могут продолжать хранить копию или «могли реплицировать данные в другом месте».

Чтобы такая проблема не повторялась, GitHub внес изменения в процесс создания общедоступной базы данных репликации, что, как ожидается, устранит возможность утечки имен частных пакетов в будущем.

Недостаток мог позволить несанкционированную публикацию новых версий.

Кроме того, GitHub обнаружил серьезную ошибку, которая могла «позволить злоумышленнику публиковать новые версии любого пакета npm с использованием учетной записи без надлежащей авторизации».

Эта уязвимость возникла из-за неправильных проверок авторизации и проверки данных между несколькими микросервисами, которые обрабатывают запросы к реестру npm.

«В этой архитектуре служба авторизации должным образом проверяла авторизацию пользователя для пакетов на основе данных, передаваемых в путях URL-адресов запроса. Однако служба, выполняющая базовые обновления данных реестра, определяла, какой пакет публиковать, на основе содержимого загруженного файла пакета, - объясняет Хэнли.

«Это несоответствие предоставило возможность, с помощью которой запросы на публикацию новых версий пакета будут разрешаться для одного пакета, но на самом деле будут выполняться для другого и потенциально неавторизованного пакета. Мы решили эту проблему, обеспечив согласованность как для службы публикации, так и для служба авторизации, чтобы гарантировать, что один и тот же пакет используется как для авторизации, так и для публикации».

Исследователи Каетан Гржибовски и Мацей Пьехота были признаны за ответственное сообщение об ошибке через программу вознаграждений за ошибки безопасности GitHub.

И пока похоже, что свидетельств эксплуатации нет. Уязвимость существовала в реестре npm «сверх временного интервала, в течение которого у нас есть телеметрия, позволяющая определить, использовалась ли она когда-либо злонамеренно», но есть некоторые заверения.

GitHub с большой уверенностью заявил, что уязвимость не использовалась злонамеренно, по крайней мере, с сентября 2020 года, то есть примерно в то время, когда стала доступна телеметрия.

«Мы быстро утвердили отчет, начали наши процессы реагирования на инциденты и устранили уязвимость в течение шести часов после получения отчета», - говорится в сообщении GitHub.

npm с 2022 года потребует двухфакторную аутентификацию

Оба анонса последовали вскоре после того, как популярные библиотеки npm, ua-parser-js, coa и rc были захвачены в серии атак, направленных на заражение потребителей программного обеспечения с открытым исходным кодом троянами и крипто-майнерами.

Эти атаки были связаны с компрометацией учетных записей npm [1, 2], принадлежащих разработчикам этих библиотек. По данным GitHub, ни у одного из сопровождающих этих популярных библиотек для своих учетных записей не была включена двухфакторная аутентификация (2FA).

Злоумышленники, которым удастся захватить учетные записи npm сопровождающих, могут легко опубликовать новые версии этих легитимных пакетов после заражения их вредоносным ПО.

Таким образом, чтобы свести к минимуму вероятность повторения таких компромиссов в ближайшем будущем, GitHub начнет требовать от специалистов по поддержке npm для включения 2FA где-то в первом квартале 2022 года.

Что касается случаев, когда вредоносное ПО для опечаток и путаницы зависимостей публикуется в npm из учетной записи, принадлежащей злоумышленнику, а не из захваченной учетной записи, GitHub продолжает инвестировать в ресурсы и улучшения безопасности для автоматизации обнаружения вредоносных программ в режиме реального времени в недавно опубликованных версиях пакетов npm». ***(Ax Sharma. NPM fixes private package names leak, serious authorization bug // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/npm-fixes-private-package-names-leak-serious-authorization-bug/). 16.11.2021).***

***

«Корпорация Intel выявила две уязвимости высокой степени серьезности, которые затрагивают широкий спектр семейств процессоров Intel, что позволяет злоумышленникам и вредоносным программам получать более высокие уровни привилегий на устройстве.

Дефекты были обнаружены SentinelOne и отслеживаются как CVE-2021-0157 и CVE-2021-0158, и оба имеют оценку CVSS v3 8,2 (высокий).

Первый касается недостаточного управления потоком управления в прошивке BIOS для некоторых процессоров Intel, а второй полагается на неправильную проверку ввода на том же компоненте.

Эти уязвимости могут привести к повышению привилегий на машине, но только в том случае, если злоумышленник имеет физический доступ к уязвимым устройствам.

Согласно рекомендациям Intel, затронутыми продуктами являются следующие:

Семейство процессоров Intel® Xeon® E
Семейство процессоров Intel® Xeon® E3 v6
Семейство процессоров Intel® Xeon® W
Масштабируемые процессоры Intel® Xeon® 3-го поколения
Процессоры Intel® Core ™ 11-го поколения
Процессоры Intel® Core ™ 10-го поколения
Процессоры Intel® Core ™ 7-го поколения
Процессоры Intel® Core ™ серии X
Процессор Intel® Celeron® серии N
Серия процессоров Intel® Pentium® Silver

Intel не поделилась многими техническими подробностями об этих двух недостатках, но они советуют пользователям исправлять уязвимости, применяя доступные обновления BIOS.

Это особенно проблематично, потому что производители материнских плат не часто выпускают обновления BIOS и не поддерживают свои продукты обновлениями безопасности в течение длительного времени.

Учитывая, что процессоры Intel Core 7-го поколения вышли пять лет назад, сомнительно, что производители MB все еще выпускают для них обновления безопасности BIOS.

Таким образом, у некоторых пользователей не останется практического способа исправить вышеуказанные недостатки.

К сожалению, установка пароля BIOS не защитит вас полностью от этой атаки, поскольку уязвимость также может быть использована удаленно, если злоумышленник имеет точку опоры в системе.

Ассаф Карловы Вары из SentinelOne сказал BleepingComputer:

Обнаруженные нами уязвимости - это ошибки LPE, которые позволяют злоумышленникам повысить свои привилегии до SMM. Код SMM считается привилегированным и обычно изолирован от «внешнего мира». Для достижения этой изоляции код SMM запускается из собственного пространства памяти, известного как SMRAM, которое не доступно для чтения и записи ОС.

Используя обнаруженные нами уязвимости, злоумышленники, работающие с привилегиями уровня ОС, могут управляемым образом инициировать повреждение памяти SMRAM. Используя повреждение памяти, они могут в конечном итоге добраться до точки, когда они смогут установить имплант уровня BIOS, таким образом получая очень стабильную и скрытую персистентность на зараженном устройстве.

Третья уязвимость касается автомобилей

Третий недостаток, по которому Intel в тот же день выпустила отдельное уведомление, - это CVE-2021-0146, также являющийся недостатком повышения привилегий высокой степени серьезности (CVSS 7.2).

«Аппаратное обеспечение позволяет активировать логику тестирования или отладки во время выполнения для некоторых процессоров Intel (R), что может позволить неаутентифицированному пользователю потенциально включить повышение привилегий через физический доступ». - Консультации Intel…

Корпорация Intel выпустила обновление прошивки, чтобы устранить этот недостаток, и пользователи получат его с помощью исправлений, предоставленных производителем системы.

Компания Positive Technologies, обнаружившая и сообщившая об ошибке в Intel, утверждает, что уязвимость может позволить злоумышленникам получить доступ к очень конфиденциальной информации.

«Один из примеров реальной угрозы - утерянные или украденные ноутбуки, содержащие конфиденциальную информацию в зашифрованном виде», - говорит Марк Ермолов.

«Используя эту уязвимость, злоумышленник может извлечь ключ шифрования и получить доступ к информации в портативном компьютере. Ошибка также может быть использована в целевых атаках по всей цепочке поставок».

«Например, сотрудник поставщика устройств на базе процессоров Intel теоретически может извлечь ключ встроенного ПО Intel CSME и развернуть шпионское ПО, которое не обнаружит программное обеспечение безопасности».

Positive Technologies заявляет, что недостаток также затрагивает несколько моделей автомобилей, использующих Intel Atom E3900, включая Tesla Model 3.

Пользователи должны применить обновление BIOS от производителя устройства, чтобы устранить этот недостаток, поэтому регулярно проверяйте веб-сайт производителя.

Помните, что всегда рекомендуется делать резервную копию ваших данных на отдельной системе или съемном носителе перед применением любого из этих исправлений, так как всегда есть вероятность, что с обновлением что-то пойдет не так. Эти недостатки в основном затрагивают системы в промышленных и корпоративных средах, подверженных воздействию физический доступ для многих людей.

Что касается автомобилей, это должно быть доступно только сервисным центрам и автомеханикам, которые будут иметь доступ к внутренним устройствам автомобиля». ***(Bill Toulas. High severity BIOS flaws affect numerous Intel processors // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/high-severity-bios-flaws-affect-numerous-intel-processors/). 15.11.2021).***

***

«Palo Alto выпустила обновление, исправляющее серьёзную уязвимость CVE-2021-3064, после того, как в сентябре была уведомлена об этой проблеме.

Исследователи из фирмы Randori, занимающейся кибербезопасностью, обнаружили её в брандмауэрах Palo Alto Networks использующих GlobalProtect Portal VPN примерно год назад.

Эта недоработка, получившая рейтинг опасности 9.8 из 10 возможных, затрагивает многие версии PAN-OS 8.1 до 8.1.17. Она позволяет получать корневые привилегии и удалённо выполнять любой код без проверки его подлинности. По мнению Randori, на чёрном рынке незакрытая (zero-day) CVE-2021-3064 стоила бы несколько сотен тысяч долларов.

Чтобы воспользоваться уязвимостью, злоумышленник должен иметь сетевой доступ к устройству через служебный порт GlobalProtect (по умолчанию 443), который у порталов VPN часто остаётся открытым.

Randori заявила, что обнаружила многочисленные уязвимые экземпляры на более, чем 70 тыс. активах, подключенных к Интернету. Часть из них принадлежит компаниям из списка Fortune 500 и другим глобальным предприятиям.

Аарон Портной (Aaron Portnoy), главный научный сотрудник Randori, сказал, что на большинстве аппаратных устройств с включенной рандомизацией адресного пространства (Address Space Layout Randomization, ASLR) эксплуатация бага затруднительна, но возможна. Взлом же виртуализированных устройств (межсетевые экраны серии VM) существенно проще из-за отсутствия ASLR.

Портной сказал, что его команда смогла использовать shell-интерфейс скомпрометированной цели, получить доступ к конфиденциальным настройкам и учётным данным, и продвигаться горизонтально во внутренней сети.

В дополнение к патчу Randori предлагает затронутым организациям сигнатуры предотвращения угроз 91820 и 91855, предоставленные Palo Alto Networks. Их включение поможет предотвратить взлом, пока организации планируют обновление ПО Тем, кто не использует VPN-функциональность брандмауэра, Randori рекомендовала её отключить». ***(Palo Alto Networks исправила критическую уязвимость в своих брандмауэрах // Компьютерное Обозрение (https://ko.com.ua/palo_alto_networks_ispravila_kriticheskuyu_uyazvimost_v_svoih_brandmaujerah_139373). 15.11.2021).***

***

«Компания Google сообщила в своем блоге ошеломляющие новости: за последние две недели в браузере Chrome было обнаружено 25 новых уязвимостей, затрагивающих пользователей Linux, macOS и Windows. Семь из них отмечены как высокоопасные.

Как обычно, Google не раскрывает подробности об уязвимостях, чтобы дать пользователям достаточно времени на установку обновлений. О высокоопасных уязвимостях пока доступна только следующая информация:

CVE-2021-38007 – несоответствие вводимых типов данных в V8;

CVE-2021-38008 – использование памяти после высвобождения в медиа;

CVE-2021-38009 – некорректная реализация в кэше;

CVE-2021-38006 – использование памяти после высвобождения в хранилище;

CVE-2021-38005 – использование памяти после высвобождения в загрузчике;

CVE-2021-38010 – некорректная реализация в сервисах;

CVE-2021-38011 – использование памяти после высвобождения в хранилище.

Как видно из представленного выше списка, наиболее часто встречаются уязвимости использования памяти после высвобождения. Они представляют собой проблемы, возникающие, когда программа не может удалить указатель на область памяти после ее высвобождения.

Эксплоиты для уязвимостей такого типа возглавляли первую десятку успешных эксплоитов в сентябре и октябре нынешнего года, а также использовались в нескольких атаках через уязвимости нулевого дня.

Google выпустила исправления для уязвимостей с выходом версии Chrome 96.0.4664.45, но предупредила, что рассылка пользователям будет происходить в ближайшие дни/недели, а значит, пользователи не смогут защитить себя сию же минуту.

После установки обновления нужно перезапустить браузер (обычно пользователи об этом забывают), чтобы его применить». **(В Chrome обнаружено сразу 25 новых уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/526644.php). 18.11.2021).**

***

«Федеральное бюро расследований США обнаружило APT-группировку, эксплуатирующую уязвимость нулевого дня в сетевых устройствах FatPipe MPVPN с целью взлома компьютерных систем компаний и получения доступа к их внутренним сетям.

Преступники эксплуатируют уязвимости в FatPipe MPVPN как минимум с мая 2021 года. Уязвимость позволила неназванной хакерской группировке использовать функцию загрузки файлов в прошивке устройства и установить web-оболочку с корневым доступом.

Атаки были направлены только на устройства FatPipe MPVPN, но уязвимость также затрагивает и другие продукты, в том числе IPVPN и WARP. Они представляют собой разные типы VPN-серверов, которые компании устанавливают по периметру своих корпоративных сетей и используют для предоставления сотрудникам удаленного доступа к внутренним приложениям через интернет, действуя как гибрид между сетевыми шлюзами и межсетевыми экранами.

Как отметили в ФБР, обнаруженная уязвимость нулевого дня в настоящее время не имеет собственного идентификатора CVE. FatPipe выпустила исправление и дополнительную информацию об уязвимости. По словам экспертов, 0Day-уязвимость может быть использована для перезаписи файла конфигурации затронутого устройства, позволяя злоумышленникам получить полный контроль над незащищенными системами.

По результатам поискового запроса Shodan, в настоящее время к Сети подключено около 800 устройств FatPipe MPVPN». ***(APT-группировка шесть месяцев использовала 0Day-уязвимость в FatPipe VPN // SecurityLab.ru (https://www.securitylab.ru/news/526675.php). 18.11.2021).***

***

«Киберпреступники стали эксплуатировать критическую уязвимость в системе управления контентом Sitecore Experience Platform (Sitecore XP).

Уязвимость (CVE-2021-42237) была впервые описана 8 октября, когда компания Sitecore представила своим клиентам инструкции по снижению ее влияния.

Уязвимость удаленного выполнения кода существует из-за небезопасной десериализации в файле Report.ashx, использующемся для «управления панелью мониторинга Executive Insight (отчета Silverlight), которая устарела в первоначальном выпуске 8.0».

Проблема затрагивает версии Sitecore XP 7.5 и 8.0 до 8.2.7. В случае с версиями Sitecore XP с 8.0.0 по 8.2.7 решением может стать удаление файла Report.ashx. Версии Sitecore XP с 7.5.0 по 7.5.2 сначала нужно обновить до релизов 8.0 или 9.0, а затем удалить файл.

На прошлой неделе исследователи безопасности ИБ-компании Assetnote опубликовали подробную информацию об уязвимости и PoC-код для ее эксплуатации, позволяющий киберпреступникам создать рабочий эксплоит для атак на сайты под управлением Sitecore XP.

Центр кибербезопасности Австралии предупредил о существовании PoC-кода и попытках злоумышленников использовать уязвимость в атаках на австралийские организации.

Успешная эксплуатация уязвимости позволяет удаленно выполнить код, благодаря чему злоумышленник может установить вредоносное ПО (web-оболочку) и выполнять другие действия». ***(Киберпреступники вооружились уязвимостью в Sitecore XP // SecurityLab.ru (https://www.securitylab.ru/news/526455.php). 10.11.2021).***

***

«Переход в облако - это гибкость и скорость, но эта гибкость часто достигается за счет безопасности, подвергая риску организации, клиентов и их данные. По мере того, как все больше и больше организаций внедряют стратегии с несколькими облаками и гибридными облаками, это создает дополнительные проблемы и векторы угроз во все более сложной среде.

Четыре уязвимости общего облака

Общественные экспозиции: Это самая старая ошибка в book- прядильного вверх новый облачный ресурс, но оставляя его в открытом доступе и полностью необеспеченный. В настоящее время хакеры обычно используют автоматизированные инструменты, которые сканируют целевые сети на предмет любых незащищенных активов, а это означает, что ваши незащищенные общедоступные активы будут обнаружены.

По данным Gartner, к 2021 году более 50% предприятий по незнанию и по ошибке будут иметь некоторые устройства хранения данных IaaS, сети, приложения или API, напрямую подключенные к общедоступному Интернету.

Избыточные разрешения. Одним из основных преимуществ перехода в облако является то, что он позволяет быстро выполнять бизнес-операции. Однако из соображений целесообразности учетные данные часто выдаются поспешно и излишне; многие пользователи получают чрезмерные разрешения, в которых они не нуждаются для бизнеса. Проблема в том, что если какие-либо из этих учетных данных попадут в чужие руки, злоумышленники получат широкий доступ к конфиденциальным данным.

По данным Gartner, к 2023 году 75% отказов облачной безопасности будут происходить из-за неадекватного управления учетными данными, идентификаторами и привилегиями для входа в систему, по сравнению с 50% в 2020 году.

Слишком много предупреждений: это может показаться нелогичным, в конце концов, обнаружение подозрительных действий - это хорошо, не так ли? Смотря как. Помогают ли эти предупреждения обнаруживать злонамеренные действия или они погружают вас в шум?

Согласно исследованию компании Bricata, занимающейся информационной безопасностью, в среднем SOC получает более 10 000 предупреждений каждый день. Это огромная фигура, с которой ни один человек (или группа людей) не может реально справиться. Это означает, что менеджеры по безопасности должны просеять

море чрезмерных предупреждений и ложных срабатываний, чтобы найти важные предупреждения, указывающие на злонамеренную активность.

Недостаточный контекст: все говорят о «контексте», но что это означает? Одна из ключевых проблем безопасности заключается в том, что просмотр любого отдельного предупреждения мало о чем говорит.

Этот логин посреди ночи - это хакер или админ, работающий допоздна?

Это первый вызов API - это разведка или DevOps-инженер занимается своими делами?

Является ли этот доступ к сегменту конфиденциального хранилища новой выпускаемой функцией или последним шагом в утечке данных?

Практически любое действие пользователя может быть законным или незаконным, и просмотр только этой активности практически ничего не говорит вам.

Вместо этого вам нужно иметь возможность интеллектуально соотносить события по нескольким поверхностям угроз, уровням приложений и временному интервалу, чтобы иметь возможность связывать событие А с событием В с событием С - даже если они разнесены на несколько месяцев - и видеть, когда вы находитесь под атакой и вовремя ее заблокировать.

Резюме

Облако не является «более» или «менее» безопасным; это другое. Это означает, что вам нужны средства защиты, специально адаптированные к облаку и к уникальным угрозам, с которыми вы там сталкиваетесь.

Хотя список уязвимостей бесконечен, работа по устранению этих четырех распространенных уязвимостей в облаке значительно поможет вам сделать ваше облако более безопасным». ***(Eyal Arazi. 4 Common Cloud Vulnerabilities Which Lead to a Breach // Techstrong Group Inc. (https://securityboulevard.com/2021/11/4-common-cloud-vulnerabilities-which-lead-to-a-breach/). 15.11.2021).***

***

«В рамках своей добровольной программы согласованного раскрытия уязвимостей (CVD) Philips предупредила отрасль здравоохранения о двух новых уязвимостях медицинских устройств, которые могут позволить использовать устройства для мониторинга пациентов и сопряжения с медицинскими устройствами. Уязвимости затрагивают концентратор Philips IntelliBridge EC40 и EC80, а также его информационный центр для пациентов iX (PIC iX) и Efficia CM Series.

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) также выпустило две рекомендации, в которых излагаются риски и методы смягчения каждой уязвимости.

В электронном письме, отправленном в HealthITSecurity, Philips подтвердила, что версии C.00.04 и более ранние системы IntelliBridge EC40 и EC80, решение для взаимодействия с медицинскими устройствами, содержат жестко закодированные учетные данные и обход аутентификации с использованием альтернативного пути или канала.

«Анализ Philips показал, что для использования этих проблем требуется низкий уровень навыков. Успешное использование этих проблем может позволить

злоумышленнику несанкционированный доступ к концентратору Philips IntelliBridge EC40 / 80 и может разрешить доступ для запуска программного обеспечения, изменения конфигурации устройства или просмотра / обновления файлов, включая неидентифицируемые данные пациента», - говорится в электронном письме.

«Уязвимости потенциально могут быть использованы в сети мониторинга пациентов Philips, которая должна быть физически или логически изолирована от локальной сети больницы (LAN)».

Philips не получала сообщений об эксплуатации и заявляла, что уязвимость вряд ли повлияет на клиническое использование, поскольку концентратор устройства не предназначен для использования в связи с активным мониторингом пациентов. Хаб используется для интеграции данных с устройств в пунктах оказания медицинской помощи с информационными системами больниц.

Ожидается, что Philips выпустит обновления программного обеспечения и исправления для этой уязвимости в 4 квартале 2021 года. CISA, следуя предложениям Philips, рекомендовала организациям использовать все развернутые продукты Philips в соответствии с утвержденными спецификациями Philips и изолировать сети медицинских устройств организации от более крупной сети больниц.

Вторая уязвимость затрагивает устройства мониторинга пациентов Philips, в частности Philips Patient Information Center iX (PIC iX) версий B.02, C.02, C.03 и Efficia CM Series редакций с A.01 по C.01 и 4.0.

«Успешное использование этих уязвимостей может позволить злоумышленнику несанкционированный доступ к данным (включая данные пациентов) и отказ в обслуживании, что приведет к временному прерыванию просмотра физиологических данных на центральной станции. Эксплуатация не позволяет модифицировать или изменять устройства на месте», - сказал Филипс.

Philips уже выпустила исправление в третьем квартале 2021 года и планирует выпустить дополнительные обновления к концу четвертого квартала 2022 года.

Тем временем Philips и CISA призвали организации не отключать поставляемое Philips оборудование с шифрованием Bitlocker Drive Encryption, которое было включено по умолчанию. Кроме того, Philips рекомендовала клиентам следовать NIST SP 800-88 в отношении дезинфекции носителей перед утилизацией системы и изолировать сеть мониторинга пациентов от локальной сети больницы.

Philips также выпустила небольшое обновление для ранее сообщенного мониторинга сердечно-сосудистых заболеваний пациента с августа 2020 года. Вместо того, чтобы выпускать обновления для PerformanceBridge Focal Point в третьем квартале 2021 года, Philips теперь планирует выпустить меры по смягчению последствий в четвертом квартале 2021 года.

В начале ноября Philips также обнаружила две уязвимости безопасности в своей системе TASY EMR HTML5, которые могут позволить раскрыть данные пациентов. Кроме того, независимые исследователи недавно обнаружили 13 новых уязвимостей безопасности медицинских устройств, проистекающих из стека TCP / IP Siemens Nucleus, которые могут сделать возможными атаки типа «отказ в обслуживании» и их использование». ***(Jill McKeon. Philips Discloses Additional Medical Device Security Vulnerabilities // TechTarget, Inc.***

(https://healthitsecurity.com/news/philips-discloses-additional-medical-device-security-vulnerabilities). 24.11.2021).

***

«В новом документе исследователи выделили ряд атак, которые демонстрируют риски, связанные с беспроводными принтерами, которые были защищены ненадлежащим образом.

Отчет, составленный аналитиками по безопасности Джампаоло Белла и Пьетро Бионди, раскрывает три вектора атаки (вместе именуемые Printjack), которые могут быть использованы для взлома многих тысяч принтеров с общедоступным TCP-портом 9100, который упрощает сетевые задания печати.

В частности, одна атака, описанная как «отказ в обслуживании на бумаге (DoS)», может быть использована для троллинга владельцев принтеров путем удаленного запуска заданий до тех пор, пока у них не закончатся расходные материалы для бумаги и / или чернил. Предположительно, эту атаку можно провести с помощью простого скрипта Python.

По словам исследователей, по сравнению с другими устройствами, подключенными к Интернету, меры по защите даже самых современных принтеров чрезвычайно просты. И хотя бумажные DoS-атаки относительно безвредны, есть более зловещие способы, которыми хакер может злоупотребить уязвимыми машинами.

Например, злоумышленник может захватить уязвимые принтеры с целью запуска распределенных атак типа «отказ в обслуживании» (DDoS), объединив известную уязвимость с широкодоступным экспериментальным эксплойтом.

Помимо того факта, что в этом сценарии принтер стал частью киберпреступной кампании, сама машина также пострадает от падения производительности, потребит больше энергии и выйдет из строя быстрее, чем обычно.

В документе также демонстрируется атака, при которой уязвимый принтер используется для перехвата содержимого печатных документов в виде открытого текста, что может иметь серьезные последствия для любого бизнеса, работающего с секретными данными.

«За пределами технических деталей атак лежит ясный урок. Принтеры должны быть защищены так же, как и другие сетевые устройства, такие как ноутбуки, - написали Белла и Бионди.

Простые меры включают требование аутентификации перед тем, как кому-либо будет разрешен доступ к панели администратора принтера или запуск заданий на печать. Ряд проблем также можно решить, разрешив подключение к принтеру только по протоколу IPSec.

«Поскольку доступна соответствующая технология для снижения рисков, связанных с атаками семейства Printjack, самое большое усилие, которое нам предстоит сделать, - это научить пользователей принимать меры безопасности и конфиденциальности, в том числе при выполнении повседневных задач печати», - говорится в отчете». ***(Joel Khalili. Mischievous hackers could use a simple trick to send***

printers berserk // Future US, Inc. (https://www.techradar.com/news/mischievous-hackers-could-use-a-simple-trick-to-send-printers-berserk). 24.11.2021).

***

«Около шести миллионов клиентских маршрутизаторов Sky Broadband в Великобритании были затронуты критической уязвимостью, исправление которой потребовалось более 17 месяцев для клиентов.

Обнаруженная уязвимость представляет собой ошибку повторного связывания DNS, которую злоумышленники могут легко использовать, если пользователь не изменил пароль администратора по умолчанию или злоумышленник может подобрать учетные данные.

Результатом эксплуатации может стать компрометация домашней сети клиента, изменение конфигурации маршрутизатора и, возможно, переключение на другие внутренние устройства.

Атака повторного связывания DNS на маршрутизаторах Sky

Атаки повторного связывания DNS используются для обхода меры безопасности браузера, называемой Same Origin Policy (SOP), которая блокирует отправку сайтом запросов на сайты, отличные от его собственного. Этим источником обычно является домен, который вы посетили в браузере.

Эта мера безопасности была введена, чтобы заблокировать один веб-сайт от кражи файлов cookie с другого сайта, доступа к данным на других сайтах или выполнения других междоменных атак.

Поскольку SOP фокусируется на доменном имени, а не на IP-адресе, цель состоит в том, чтобы обмануть браузер, заставив его думать, что сценарий обращается к исходному домену, но на самом деле обращается к внутреннему IP-адресу (127.0.01 / 192.168.0.1).

Именно здесь в игру вступают атаки DNS Rebinding, которые при правильном проведении приводят к целому ряду атак.

Чтобы атака сработала, жертву необходимо обманом заставить перейти по вредоносной ссылке или посетить вредоносный веб-сайт. Это может быть легко сделано злоумышленником, который рассылает клиентам Sky фишинговые электронные письма, сообщения в социальных сетях и текстовые SMS-сообщения, содержащие ссылки на вредоносный сайт.

После того, как жертва зайдет на сайт, отобразится iframe, который запрашивает данные из поддомена, управляемого злоумышленником.

Затем этот сценарий загружает полезные данные JavaScript в iframe, который выполняет последовательные HTTP-запросы к серверу, при этом последний отвечает своим IP-адресом.

Через несколько секунд сервер перестает отвечать на эти запросы, и это вызывает повторную инициацию подключения браузера к домену, поэтому отправляется новый запрос DNS.

Однако на этот раз сервер отвечает IP-адресом цели (192.168.0.1), который является маршрутизатором жертвы.

Поскольку браузер считает, что он все еще обменивается данными с исходным доменом, он позволит сценарию удаленного веб-сайта отправлять запросы на внутренний IP-адрес маршрутизатора (192.168.0.1).

«После того, как соединение от полезной нагрузки JavaScript к целевому маршрутизатору было установлено, злоумышленник мог общаться с внутренним веб-сервером и мог делать запросы, которые изменяли бы настройки так же, как это обычно происходит в веб-браузере клиента», - пояснил PenTestPartners в их отчет.

Используя эту уязвимость, исследователи создали PoC-эксплойт, который мог выполнять различные вредоносные действия на маршрутизаторе, в том числе:

Войти в систему как администратор с учетными данными по умолчанию (пользователь: admin - пароль: sky)

Изменить пароль администратора (необходимо для включения удаленного управления)

Выполнить сбор и отображение имени SSID и пароля WPA2

Включить удаленное управление…

Этот PoC работает на следующих моделях маршрутизаторов, которые соответствуют примерно шести миллионам пользователей:

Sky Hub 3, 3.5 и Booster 3 (ER110, ER115, EE120)

Sky Hub 2 и бустер 2 (SR102, SB601)

Sky Hub (SR101)

Sky Hub 4 и Booster 4 (SR203, SE210) - ограниченное влияние из-за доставки со случайными паролями

На развертывание исправления потребовалось 17 месяцев

Команда PenTestPartners сообщила о своих выводах 11 мая 2020 года, и Sky признала проблему и назначила дату исправления на ноябрь 2020 года.

Это превышало стандартные 90 дней раскрытия уязвимости, но исследователи приняли это без возражений, поскольку интернет-провайдер имел дело с необычной нагрузкой на трафик из-за блокировки COVID-19.

Патч для исправления так и не появился, и Sky в конечном итоге пересмотрела план, пообещав исправить 50% затронутых моделей к маю 2021 года, что было выполнено.

Поскольку другая половина по-прежнему уязвима, а сотрудники PenTestPartners считают, что Sky не действует срочно, в августе исследователи связались с прессой, чтобы оказать дополнительное давление.

В конце концов, 22 октября 2021 года Sky отправила электронное письмо, чтобы сообщить, что Sky исправила 99% всех уязвимых маршрутизаторов с помощью обновления.

С момента первоначального раскрытия информации прошло более 17 месяцев, что сделало пользователей уязвимыми для атак повторного связывания DNS в период, когда многие из них работали из дома». ***(Bill Toulas. Six million Sky routers exposed to takeover attacks for 17 months // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/six-million-sky-routers-exposed-to-takeover-attacks-for-17-months/). 19.11.2021).***

***

«Microsoft представила управляемую искусственным интеллектом систему обнаружения атак программ-вымогателей для клиентов Microsoft Defender для конечных точек, которая дополняет существующую облачную защиту, оценивая риски и блокируя участников по периметру.

Поскольку атаки программ-вымогателей, управляемые человеком, характеризуются особым набором методов и поведения, Microsoft считает, что они могут использовать управляемый данными подход ИИ для обнаружения этих типов атак.

Предотвращение начальной точки опоры

Злоумышленники обычно закрепляются в целевой системе, внедряя двоичный файл вредоносной программы, который обеспечивает удаленный доступ к устройству.

Однако не все двоичные файлы, используемые в атаках, известны как вредоносные, и многие исполняемые файлы, используемые в атаках, являются законными программами, включая встроенные команды Windows.

Индикаторы, генерируемые этими двоичными файлами, могут считаться низкоприоритетными и игнорироваться защитниками.

Добавление управляемой искусственным интеллектом системы адаптивной защиты, которая будет обнаруживать необычное поведение даже в законных двоичных файлах, может сыграть решающую роль в предотвращении дальнейшего взлома устройства и предоставить отвечающим группам ценное время для предотвращения атак.

«В клиентской среде функция адаптивной защиты, управляемая ИИ, оказалась особенно успешной в предотвращении проникновения людей в сеть, остановив двоичный файл, который предоставил бы им доступ», - объяснил Microsoft о своей системе защиты, управляемой ИИ.

«Учитывая индикаторы, которые в противном случае считались бы низкоприоритетными для исправления, адаптивная защита остановила цепочку атак на ранней стадии, так что общее воздействие атаки было значительно снижено».

«Угрозой оказался Cridex, банковский троян, обычно используемый для кражи учетных данных и кражи данных, которые также являются ключевыми компонентами многих кибератак, включая программы-вымогатели, управляемые человеком».

В отличие от облачной защиты, которую администраторы настраивают вручную, новая система является адаптивной, что означает, что она может автоматически повышать и понижать агрессивность решений о блокировке, доставляемых через облако, на основе данных в реальном времени и прогнозов машинного обучения.

Блокирование последующих шагов атаки

Даже если алгоритм не сможет оценить риск в его реальной величине и злоумышленник найдет путь в целевую сеть, система останется для них препятствием.

Как объясняет Microsoft, адаптивная защита может обнаруживать и блокировать кажущиеся безобидными операции, такие как перечисление сетей, которые субъекты программ-вымогателей используют на этапе разведки.

Точно так же инструменты с открытым исходным кодом часто используются для бокового перемещения или могут быть обнаружены и заблокированы слегка модифицированные массовые вредоносные программы, не имеющие идентифицируемой сигнатуры.

«Гипотетически, в атаках, где атаки на ранней и средней стадии не обнаруживаются и не блокируются, адаптивная защита, управляемая ИИ, может по-прежнему демонстрировать огромную ценность, когда дело доходит до конечной полезной нагрузки вымогателя». Microsoft объясняет

«Учитывая, что устройство уже взломано, наша система адаптивной защиты, управляемая искусственным интеллектом, может легко и автоматически переключиться в наиболее агрессивный режим и заблокировать фактическую полезную нагрузку программ-вымогателей, предотвращая шифрование важных файлов и данных, поэтому злоумышленники не смогут потребовать выкуп. для них."

Держать щиты поднятыми

По мере того, как защитные механизмы становятся более изощренными, субъекты с гораздо большей вероятностью попытаются деактивировать их, вместо того, чтобы пытаться уклониться от них или обойти их.

Это означает, что администраторы должны регулярно проверять состояние своих защитных инструментов, чтобы они всегда были в рабочем состоянии.

Облачная защита включена по умолчанию, а усовершенствованные средства искусственного интеллекта теперь автоматически включаются в Microsoft Defender для конечных точек в качестве «постоянно включенной» функции.

Если какая-либо из этих функций теперь отключена, администраторы должны немедленно провести дальнейшее расследование, чтобы определить, не были ли они скомпрометированы». ***(Bill Toulas. Microsoft adds AI-driven ransomware protection to Defender // Bleeping Computer® (https://www.bleepingcomputer.com/news/microsoft/microsoft-adds-ai-driven-ransomware-protection-to-defender/). 16.11.2021).***

***

«Компания Keysight Technologies разработала программное решение для тестирования безопасности устройств интернета вещей (IoT), которое позволит производителям микросхем и устройств IoT, а также организациям, осуществляющим развертывание IoT-сетей, выполнять комплексную автоматизированную оценку кибербезопасности.

Увеличение числа подключаемых устройств IoT позволяет хакерам использовать уязвимости кибербезопасности для различных атак, в том числе с использованием вредоносных программ, шифровальщиков и эксфильтрации данных. По прогнозам Statista, общее количество установленных устройств,

подключаемых к интернету вещей, вырастет с 13,8 млрд единиц в 2021 г. до 30,9 млрд единиц к 2025 г.

Недавно исследователи из Сингапурского университета технологий и дизайна (SUTD) обнаружили группу уязвимостей, которые они назвали BrakTooth, в коммерческих чипсетах Bluetooth, которые используются в миллиардах устройств конечных пользователей. Финансирование исследования SUTD осуществлялось за счет гранта компании Keysight. Опубликованные SUTD результаты позволили усовершенствовать ПО Keysight для оценки безопасности устройств интернета вещей.

BrakTooth фиксирует основные векторы атаки на устройства, использующие стандартную базовую/ повышенную скорость передачи данных по Bluetooth (BR/EDR), и может оказывать влияние на чипсеты Bluetooth, которые не были протестированы командой SUTD.

Уязвимости, перечень которых включает 20 распространенных уязвимостей (CVE), а также четыре ожидающих назначения CVE, обнаружены в наборах Bluetooth-чипсетов, используемых в платах однокристальных систем (SoC). Они создают риски, к которым относятся удаленное выполнение кода, сбои и взаимоблокировки. Команда SUTD ответственно раскрыла результаты исследования поставщикам соответствующих чипсетов, предоставив средства для воспроизведения результатов и время для устранения уязвимостей.

Программное обеспечение Keysight для оценки безопасности устройств интернета вещей, созданное на основе более чем 20-летнего опыта компании в области разработки систем для тестирования безопасности сетей, позволяет обнаружить уязвимости в любой сетевой технологии. Оно предлагает возможности комплексного автоматизированного тестирования, позволяющего быстро выявлять большое количество известных и неизвестных уязвимостей. Средства для оценки безопасности устройств интернета вещей включают новые инструменты и методы кибербезопасности для беспроводных интерфейсов, таких как Wi-Fi, Bluetooth и Bluetooth с низким энергопотреблением (BLE), как для тестирования известных уязвимостей, так и для обнаружения новых.

Разработчики могут легко интегрировать API-решение Keysight с единым API для управления и формирования отчетности в свой процесс создания продукта. Организации, осуществляющие развертывание устройств интернета вещей, могут использовать программное обеспечение для проверки устройств интернета вещей до их поставки конечным пользователям, а также по мере появления новых уязвимостей. Текущие исследования, проводимые центром прикладных исследований и анализа угроз Keysight, предоставляют актуальную информацию об автоматизации тестирования безопасности протоколов и атаках». ***(Программное решение Keysight позволяет оценить безопасность устройств IoT // Компьютерное Обозрение (https://ko.com.ua/programmnoe_reshenie_keysight_pozvolyaet_ocenit_bezopasnost_ustrojstv_iot_139233). 02.11.2021).***

***

«Ленточные системы являются важной частью комплексной стратегии, обеспечивающей защиту данных и возможность их быстрого восстановления в случае атаки программы-вымогателя. Ленточные системы по своей природе более безопасны, чем системы хранения на жестких дисках (HDD) или SSD, поскольку данные на ленте не доступны из сети. Однако, поскольку ленточная библиотека сама по себе является устройством, подключенным к сети, всё же существует некоторый риск удаленного взлома.

Чтобы устранить эту угрозу, корпорация Quantum 2 ноября анонсировала пока единственную в своём роде инновацию: патентованная функция Scalar Ransom Block создает аппаратный «блок» между данными, хранящимися на магнитных лентах, и любым подключенным к сети устройством.

Scalar Ransom Block частично выталкивает магазин, поэтому ленты не могут быть выбраны роботом, пока оператор физически не вставит его обратно. Поскольку магазин извлекается не полностью, сканер робота все еще может считывать штрих-коды на ленте, и системные администраторы в ходе периодических проверок могут убедиться в наличии лент в библиотеке.

Кроме того Quantum представила логическую блокировку (Logical Tape Blocking), которая позволяет администраторам использовать команды для предотвращения загрузки лент в привод. Хотя эта новая возможность основана на программном обеспечении, она, тем не менее, уменьшает окно риска, пока не будет инициирована блокировка Scalar Ransom Block.

Ransom Block и Logical Tape Blocking — это новейшие из более чем 25 функций и возможностей, которые образуют комплексную структуру безопасности, делающую ленточные системы Scalar одними из самых безопасных систем хранения на рынке.

В числе других функций Quantum Scalar Security Framework для киберзащиты и целостности данных:

Scalar Active Vault позволяет перемещать ленты в безопасный, изолированный раздел хранилища, который не имеет сетевого подключения и не виден ни одному приложению или сети.

Scalar Media Security Alerts уведомляет администратора об (ожидаемом или непредвиденном) удалении носителя из библиотеки.

Многофакторная аутентификация — может быть установлена для логинов администратора и пользователя, обеспечивая дополнительный уровень контроля доступа.

Ожидается, что Ransom Block и Logical Tape Blocking будут предложены на новых ленточных библиотеках Scalar i6 и Scalar i3 в декабре 2021 года. Прочие компоненты Quantum Scalar Security Framework уже доступны на поддерживающих их моделях, частью — за дополнительную плату». ***(Scalar Ransom Block защитит ленточные архивы от кибератак // Компьютерное Обозрение (https://ko.com.ua/scalar_ransom_block_zashhitit_lentochnye_arhivy_ot_kiberatak_139309). 08.11.2021).***

***

«Чтобы противостоять растущей угрозе кибератак на промышленные системы управления, команда KAUST (Университет науки и технологий короля Абдаллы), в которую входят Фузи Харроу, Ву Ван и возглавляемая Ин Сунь, разработала улучшенный метод обнаружения злонамеренных вторжений.

Интернет-системы управления производством широко используются для контроля и управления предприятиями и критически важной инфраструктурой. В прошлом эти системы полагались на дорогие выделенные сети; тем не менее, перемещение их в Интернет сделало их более дешевыми и доступными. Но это также сделало их более уязвимыми для атак, опасность, которая растет вместе с растущим внедрением технологии Интернета вещей (IoT).

Обычные решения безопасности, такие как межсетевые экраны и антивирусное программное обеспечение, не подходят для защиты промышленных систем управления из-за их различных характеристик. Их явная сложность также затрудняет даже лучшим алгоритмам выявление аномальных явлений, которые могут означать вторжение.

Например, поведение системы, которое выглядит подозрительно, такое как резкий скачок напряжения или последовательный отказ автоматических выключателей, может иметь естественные причины. Вдобавок к этому изощренные кибератаки могут очень хорошо маскировать свои движения.

Там, где в прошлом алгоритмы терпели неудачу, отрасль машинного обучения, называемая глубоким обучением, оказалась гораздо более искусной в распознавании сложных шаблонов, описанных выше.

Глубокое обучение выполняется в схемах, называемых нейронными сетями, и обучается, а не программируется. Вместо того, чтобы писать закодированные инструкции, его создатели показывают глубокие обучения модели различных примеров, чтобы узнать с, что позволяет улучшить в точности с каждым шагом.

Команда Ин Сунь обучила и протестировала пять различных моделей глубокого обучения с данными, предоставленными Центром защиты критической инфраструктуры Университета штата Миссисипи. Это были общедоступные модели различных видов атак, таких как внедрение пакетов и распределенный отказ в обслуживании (DDOS), на энергосистемы и газопроводы.

Способность моделей глубокого обучения обнаруживать вторжения сравнивалась с современными алгоритмами. В то время как лучшие алгоритмы обычно имели точность от 80 до 90 процентов, каждая модель глубокого обучения набирала от 97 до 99 процентов.

Что особенно важно, когда все пять моделей глубокого обучения были «сложены», точность повысилась до более чем 99 процентов. Проще говоря, суммирование означает сложение результатов всех пяти моделей и их среднее значение. «Мы пробовали складывать две модели, затем три и четыре, пока пять не дали нам желаемой точности», - говорит Харроу.

Комплексный метод глубокого обучения команды обещает эффективную защиту от кибервойны, которую сегодня национальные правительства считают серьезной угрозой безопасности. Кибератаки, подобные атаке на украинскую электросеть в 2015 году, которая привела к отключениям в тысячах домов, могут

быть предотвращены». ***(Creating deeper defense against cyber attacks // Tech Xplore (https://techxplore.com/news/2021-11-deeper-defense-cyber.html). 23.11.2021).***

***

«Meta, материнская компания Facebook, отказалась от своих планов включить сквозное шифрование (E2EE) по умолчанию в Facebook Messenger и Instagram до 2023 года.

В наши дни чаты Messenger и Instagram находятся на одной платформе, что отражает стремление компании унифицировать свои продукты обмена сообщениями и согласовать их с WhatsApp, где E2EE по умолчанию, на основе протокола E2EE Signal.

В апреле Facebook заявил, что прямые сообщения в Messenger и Instagram не будут «полностью зашифрованы до 2022 года».

E2EE должен означать, что даже сотрудники Facebook, имеющие физический доступ к его оборудованию в центрах обработки данных, не могут получить доступ к содержанию сообщений, не позволяя фирме и сотрудникам предоставлять некоторые доказательства, даже когда это предписано судом.

Facebook развернул E2EE для WhatsApp в 2016 году с использованием протокола, разработанного платформой обмена сообщениями Signal, который привлек пользователей после того, как Facebook объявил о планах обмена пользовательскими данными между WhatsApp и Facebook, чтобы расширить свое предложение для предприятий на обеих платформах.

Антигона Дэвис, глобальный руководитель службы безопасности Meta, подробно рассказала о проблемах Meta с шифрованием в статье для британского The Telegraph.

«Продолжаются дискуссии о том, как технологические компании могут продолжать бороться со злоупотреблениями и поддерживать жизненно важную работу правоохранительных органов, если мы не можем получить доступ к вашим сообщениям», - написал Дэвис.

«Мы считаем, что людям не нужно выбирать между конфиденциальностью и безопасностью, поэтому мы встраиваем строгие меры безопасности в наши планы и взаимодействуем с экспертами по конфиденциальности и безопасности, гражданским обществом и правительствами, чтобы убедиться, что мы делаем это правильно».

Дэвис сказал, что у Meta есть три подхода к вопросу безопасности, включая обнаружение подозрительных шаблонов, например, когда кто-то создает несколько новых профилей и отправляет сообщения незнакомцам.

Она сказала, что эта система существует, и что «мы работаем над повышением ее эффективности».

Во-вторых, пользователи Instagram могут фильтровать прямые сообщения на основе оскорбительных слов. Третий - побуждает людей сообщать о вредоносных сообщениях.

Далее она указывает, что правоохранительные органы все еще имеют доступ к метаданным для уголовных расследований.

«Даже с учетом того, что миллиарды людей уже пользуются сквозным шифрованием, полиция может использовать больше данных, чем когда-либо, для расследования и преследования преступников, включая номера телефонов, адреса электронной почты и данные о местоположении», - отмечает она.

«Наш недавний обзор некоторых исторических случаев показал, что мы все равно были бы в состоянии предоставить властям важную информацию, даже если бы эти услуги были зашифрованы из конца в конец», - написал Дэвис.

«Хотя ни одна система не является совершенной, это показывает, что мы можем продолжать останавливать преступников и поддерживать правоохранительные органы.

«Мы не торопимся, чтобы сделать это правильно, и мы не планируем завершать глобальное развертывание сквозного шифрования по умолчанию для всех наших служб обмена сообщениями до 2023 года», - сказал Дэвис.

В 2019 году США, Великобритания и Австралия призвали Facebook создать бэкдор для доступа к зашифрованным сообщениям. Facebook сопротивлялся этим призывам.

Генеральный директор и соучредитель Facebook Марк Цукерберг объявил о смене имени на Meta в ноябре, через месяц после того, как бывший сотрудник Фрэнсис Хауген обнародовал обвинения в том, что алгоритмы компании используются для распространения вредоносного контента. Meta и ее бренды столкнулись с новыми законами в Великобритании, которые могут потребовать от них защиты пользователей от вредоносного контента». ***(Liam Tung. Facebook's Meta pushes back Messenger and Instagram encryption plans until 2023 // ZDNet (https://www.zdnet.com/article/facebooks-meta-pushes-back-messenger-and-instagram-encryption-plans-until-2023/). 22.11.2021).***

***

«Независимая австрийская организация AV-Comparatives, которая специализируется на тестировании антивирусных решений, представила результаты испытаний корпоративных и потребительских (по восемь в каждой категории) средств интернет-безопасности на предмет обеспечения защиты от сложных и целевых атак.

В тестах AV-Comparatives используются различные сценарии атак, от которых должны защищать испытуемые программы. В целевых атаках применяются различные методы, позволяющие избежать обнаружения защитными программными средствами. К ним относятся бесфайловые атаки, запутывание кода и использование легальных средств операционной системы. Маскировка вредоносного кода также затрудняет распознавание защитной программой. Злоупотребление легальными системными программами во вредоносных целях также облегчает киберпреступникам задачу держаться вне зоны досягаемости средств защиты.

Во всех испытаниях используется подмножество ТТП (тактика, технологии, процедуры), фигурирующее в информационной базе данных MITRE ATT&CK. В отчеты также включены результаты теста на ложное срабатывание. Все протестированные продукты – как потребительские, так и корпоративные – должны были обеспечивать защиту от 15 различных таргетированных атак.

В число протестированных средств защиты оконечных устройств корпоративного уровня вошли: Acronis Cyber Protect Cloud with Advanced Security Pack; Avast Business Antivirus Pro Plus; Bitdefender Gravity Zone Elite; CrowdStrike Falcon Pro; Eset Protect Entry with Eset Protect Cloud; G Data Endpoint Protection Business; Kaspersky Endpoint Security for Business – Select with KSC; Vipre Endpoint Cloud. Все перечисленные продукты заблокировали не менее восьми из пятнадцати таргетированных атак.

В число протестированных программ обеспечения безопасности потребительского уровня вошли: Avast Free Antivirus; AVG Free Antivirus; Bitdefender Internet Security; Eset Internet Security; G Data Total Security; Kaspersky Internet Security; McAfee Total Protection; Vipre Advanced Security. Из перечисленных потребительских продуктов Avast, AVG, Eset, Kaspersky и McAfee достигли наивысшего рейтинга Advanced+.

«Испытание на защиту от таргетированных атак обеспечивает проверку способности каждого защитного продукта обезопасить компьютер от целевых атак, называемых «таргетированными кибератаками» (APT). Это сложные, многоэтапные атаки, нацеленные на конкретное лицо или организацию. Хотя большинство таких атак могут быть в конечном итоге нацелены на проникновение в корпоративные сети, очевидно, что для этого требуется использовать персональные компьютеры сотрудников организации. Кроме того, киберпреступники могут совершать целенаправленные атаки на отдельных лиц по другим причинам. Это означает, что защита от таких атак должна осуществляться с помощью программ обеспечения безопасности потребительского уровня, а также корпоративных программных средств защиты оконечных устройств», – сообщил Петер Штельцхаммер». ***(Peter Stelzhammer), соучредитель AV-Comparatives. (Евгений Куликов. Защита конечных точек от целевых атак 2021 // Компьютерное Обозрение (https://ko.com.ua/zashhita_konechnyh_tochek_ot_celevyh_atak_2021_139513). 26.11.2021).***

***

«Positive Technologies представила онлайн-платформу для проведения полноценных киберучений. После завершения бета-тестирования она будет круглосуточно доступна этичным хакерам и специалистам по расследованию киберинцидентов со всего мира 365 дней в году.

Современное предприятие представляет собой среду, где все бизнес-процессы влияют друг на друга, а их зависимости между собой непрозрачны для топ-менеджмента, подразделений компаний и службы ИБ. Вдобавок для каждой организации существуют события, реализация которых нанесет непоправимый ущерб бизнесу. Чтобы компания работала без перебоев, необходимо определить такие события и обеспечить уровень ИБ, который будет гарантировать, что они не произойдут в результате кибератаки. Стоит отметить, что аналогичный подход применим ко всем отраслям экономики. Проверить их защищенность можно только на практике, в частности с помощью киберучений.

С появлением платформы The Standoff 365 любая компания сможет провести киберучения на модели своей инфраструктуры, узнав все возможные сценарии

реализации недопустимых для нее событий. Платформа стала ответом на появившийся в индустрии запрос на измеримую и результативную защищенность, подразумевающую, что критические риски для компании, отрасли или страны не могут быть реализованы. Здесь только реальная инфраструктура, а все сценарии атакующие определяют самостоятельно.

«В проекте The Standoff 365 мы видим будущее результативной кибербезопасности: сегодня речь идет не о повышении безопасности отдельными средствами защиты, а о построении защиты на основе недопустимых для бизнеса событий. Онлайн-платформа, позволяющая проводить киберучения в режиме 24/7/365, стала новой ступенью развития нашего ежегодного мероприятия — кибербитвы The Standoff. Для нее более пяти лет подряд мы создаем инфраструктуру киберполигона, используя нашу уникальную экспертизу и опыт реализации проектов по противодействию актуальным киберугрозам. В этом году киберполигон вырос до виртуального государства, где представлены энергетическая отрасль, объекты металлургии, транспорта, логистики, химической отрасли и городского хозяйства», — сказал директор департамента базы знаний и экспертизы Positive Technologies Михаил Помзов.

В настоящее время The Standoff 365 состоит из киберполигона, на котором воссозданы операционные и бизнес-процессы топливно-энергетического комплекса. В ближайших планах — запуск платформы bug bounty. С ее помощью будет удобно собирать отчеты об уязвимостях, а обнаружившие их хакеры смогут получать вознаграждения.

Непрогнозируемый вектор атак — ключевая особенность проекта The Standoff 365, перенесенная специалистами Positive Technologies с одноименного киберполигона.

«На The Standoff 365 не предусмотрено никаких ограничений по сценариям, поскольку объекты на полигоне атакуют реальные исследователи безопасности — каждый со своим бэкграундом, навыками и набором инструментов. А это значит, что даже мы не знаем, как будут разворачиваться события. Благодаря этому сценарии атак на онлайн-полигоне каждый раз могут быть новыми, что дает возможность практиковать различные способы защиты в непредсказуемых условиях», — отметил Ярослав Бабин, руководитель отдела анализа защищенности приложений Positive Technologies». ***(Positive Technologies представила онлайн-платформу The Standoff 365 для киберучений // CNews (https://www.cnews.ru/news/line/2021-11-15_positive_technologies_predstavila). 15.11.2021).***

***

«Холдинг «Технодинамика» Госкорпорации Ростех разработал флеш-накопитель, ликвидирующий информацию нажатием кнопки. В отличие от имеющихся аналогов устройство безопасно для пользователя, поскольку при срабатывании электродетонатора целость его корпуса не нарушается, а хранящиеся на флешке данные уничтожаются без возможности восстановления.

В новой разработке чип памяти, элементы питания и управления расположены в едином корпусе. При необходимости уничтожить информацию с флеш-накопителя пользователь нажимает кнопку на торце устройства. Встроенный источник питания

активирует электродетонатор, который прожигает печатную плату кумулятивной струей. Целостность корпуса при этом не нарушается, что гарантирует безопасность пользователя.

«В современном цифровом мире безопасность данных требует особого внимания. Мы создали новое устройство, которое способно надежно обезопасить информацию от несанкционированного доступа: невозможность восстановления данных подтверждена экспертизой. В дальнейшем предстоит провести испытания устройства на безопасность при длительном хранении, на стойкость к механическим и климатическим факторам, а также проработать различные варианты дизайна корпуса», – рассказал генеральный директор холдинга «Технодинамика» Игорь Насенков.

Самоуничтожающееся устройство хранения информации разработано в инициативном порядке АО «НПП «Краснознаменец». Объем памяти, как и внешний вид флешки, может быть любым – в зависимости от предпочтений заказчика.

Потенциальными потребителями устройства могут стать госведомства, а также компании, работающие с конфиденциальной информацией». ***(Ростех разработал самоуничтожающуюся флешку // SecurityLab.ru (https://www.securitylab.ru/news/526893.php). 25.11.2021).***

***