**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

№ 12 (грудень)

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.– №12 (грудень) . – 234 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.

ЗМІСТ

Стан кібербезпеки в Україні 4
Боротьба з кіберзлочинністю в Україні 5
Міжнародне співробітництво у галузі кібербезпеки 10
Коронавірус COVID-19 та питання кібербезпеки 11
Світові тенденції в галузі кібербезпеки 14
Сполучені Штати Америки 65
Країни ЄС та Великобританія 78
Російська Федерація та країни ЄАЕС 87
Японія та Австралія 92
Інші країни 94
Кібервійни та протидія зовнішній кібернетичній агресії 97
Створення та функціонування кібервійськ 97
Захист персональних даних 98
Кіберзлочинність та кібертерроризм 109
Вірусне та інше шкідливе програмне забезпечення 148
Програми-вимагачі 158
Програми-трояни 195
Операції правоохоронних органів та судові справи проти кіберзлочинців .197
Технічні аспекти кібербезпеки 202
Виявлені вразливості технічних засобів та програмного забезпечення 208
Технічні та програмні рішення для протидії кібернетичним загрозам 232

«Украинская ядерная энергетика сегодня обеспечивает 55% потребности страны в электричестве, и поэтому также является потенциальной мишенью для кибератак.

Мы поинтересовались у американского эксперта Тима Конвея, технического директора программ ICS и SCADA в SANS, как защищена данная критическая инфраструктура и есть ли обращения за консультациями с украинской стороны.

Напомним, что в начале декабря в Украине состоялись учения по киберзащите объектов критической инфраструктуры Grid NetWars, сценарии для которых созданы SANS Institute – ведущей мировой организацией, которая обучает, развивает и сертифицирует специалистов по кибербезопасности.

«В ядерном секторе внимание фокусируется в первую очередь на физической защите и изолированности объекта. В то же время системы генерации и передачи электроэнергии в основном сосредоточены на кибербезопасности. Есть немало международных стандартов и законодательных актов, которые применяются к ядерной отрасли, - отметил Тим Конвей. - При проведении учений по кибербезопасности в США, Польше и Украине мы приглашаем и представителей ядерной отрасли. Но настройки внутренних сетей атомных электростанций уникальны. Операторы транспортной инфраструктуры должны присоединяться к общей сети, чтобы иметь возможность работать. В ядерной энергетике это необязательно. Сеть АЭС может быть изолирована и работать сама по себе». ***(Герман Богапов. Тим Конвей: украинским АЭС кибератаки не угрожают // Internetua (http://internetua.com/tim-konvei-ukrainskim-aes-kiberataki-ne-ugrojauat). 09.12.2021).***

***

«Сегодня Национальный координационный центр кибербезопасности при СНБО Украины и проект USAID «Кибербезопасность критически важной инфраструктуры Украины» при поддержке Государственной службы специальной связи и защиты информации проводят обучающий турнир по киберзащите объектов критической инфраструктуры Grid NetWars.

Кроме того, состоялись командно-штабные учения стратегического уровня, в которых отрабатывались киберугрозы на уровне руководства страны, принятие решений, поиск проблемных вопросов.

Сценарии учений Grid NetWars созданы SANS Institute – ведущей мировой организацией, которая обучает, развивает и сертифицирует специалистов по кибербезопасности от начального до высших уровней.

Формат Grid NetWars предусматривает командную работу по отражению имитированных кибератак: в ходе учений представители государственных органов и частных компаний отработают на практике умение защищать объекты критической инфраструктуры от хакеров.

При этом украинские специалисты в первый раз получат престижную сертификацию от SANS Institute.

SANS обеспечивают учения одновременно 250 человек. Мы стремимся привлекать именно украинские компании к учениям, потому что имеется опыт, но к сожалению ни одна из них не смогла обеспечить более 50 одновременных участников. Поэтому американская SANS даст достаточно высокий уровень знаний.

Сегодня данные учения и учения стратегического уровня проходят параллельно. То есть, не пересекаются. Но мы изучаем опыт США и НАТО, с которыми плотно сотрудничаем. У них подобные состязания проходят снизу доверху. И информация по цепочке передается обменом наверх, и там принимаются соответствующие решения, которые опять же спускаются вниз.

Но на самом деле это первое учение уровня SANS. И мы хотим понять, как идти сверху вниз и снизу вверх. И я надеюсь, что уже со следующего года мы сможем задавать более сложные сценарии, они будут пересекаться и идти вместе.

Сегодня 75 участников соревнуются в Парковом, остальные 175 соревнуются онлайн. Это команды со всей Украины. Было тяжело отобрать участников, потому что количество желающих было более двух человек на одно место. Мы старались отобрать три категории: государственные органы, предприятия, которые являются частью критической инфраструктуры, в частности из сферы энергетики, коммерческие компании, которые пребывают в состоянии частно-государственного партнерства, а также университеты.

Возможно в следующем году мы сможем провести что-то объединяющее тематически. Сначала - взаимодействие технических специалистов в рамках состязания, похожего на Grid NetWars, а затем - командно-штабные учения, так называемый Table Top Excercise - упражнение для лиц, принимающих стратегические решения касательно синхронного реагирования на киберинциденты, по взаимодействию, коммуникации, по использованию регуляторных документов, которые позволяют общаться разным организациям на одном языке и как можно скорее обмениваться информацией, потому что безопасность - это коллективная работа и коллективные усилия». ***(Герман Богапов. В Украине проходят учения по отражению кибератак // Internetua (http://internetua.com/v-ukraine-prohodyat-ucseniya-po-otrajeniua-kiberatak). 02.12.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Правоохранители Харькова установили, что на территории их юрсидикции действует неизвестный, имеющий отношение к организации популярной схемы кибермошенничества. Речь идет о создании фишинговых веб-страничек, имитирующих сервис безопасных сделок «ОЛХ Доставка», в результате посещения которых, жертвы неосмотрительно передают мошенникам данные своих банковских карт, с которых преступники крадут деньги.

В ходе расследования, правоохранители обнаружили, что в настоящее время в кроссплатформенном мессенджере Telegram функционирует 76 активно действующих закрытых преступных telegram-сообществ, где администраторы

предоставляют возможность заинтересованным лицам принять участие в данной преступной схеме, с целью завладения денежными средствами граждан с помощью фишинговых ссылок.

Установлено, что участники преступных сообществ имеют четкую иерархию и распределение ролей, направленных на создание Telegram-каналов и Telegram-ботов, с помощью которых фигуранты генерируют фишинговые ссылки.

В состав преступных сообществ входят:

Учредитель проекта (так называемый «ТС»), организатор преступной схемы, лицо, создавшее сообщество и установившее определенные правила, которые должны соблюдать все остальные члены преступной группировки. Он также отвечает за своевременные выплаты денежных средств участникам преступной схемы и контролирует их деятельность;

«КОДЕР» - лицо, обладающее техническими знаниями и навыками, отвечает за функционирование «Telegram»-бота, с помощью которого участники преступной схемы создают необходимые «фишинговые» ссылки;

«УБИВЕР» - лицо, отвечающее за использование полученных, в результате фишинга, платежных реквизитов, получения доступа к личным кабинетам онлайн-банкингов и осуществления вывода средств на подконтрольные банковские карты;

Операторы - лица, в обязанности которых входит поиск потенциальных жертв на торговой площадке «OLX», введение их в заблуждение, под предлогом осуществления платежа за покупку или продажу товара и предоставление им фишинговой ссылки, используя которую, потерпевший передает данные своей банковской карты мошенникам.

По поручению следователя, сотрудники Департаментка киберполиции НПУ в Харьковской области провели мониторинг Telegram-сообществ и Telegram-каналов, в ходе которого были установлены учетные записи ряда пользователей Telegram, являющихся участниками преступной схемы, выполняющих отведенные им роли операторов в указанной схеме.

Киберполицейским удалось установить уникальные идентификаторы 37 человек и запросить через суд их персональные данные в одном из украинских банков, с поддержкой которого в Telegram эти лица общались при помощи тех же идентификаторов.

В перечень таких данных входят анкетные данные, копии паспортов и идентификационных кодов, платежные реквизиты и выписки по счетам, IP-адреса, с которых производилась авторизация в системах интернет-банкинга, а также фотоснимки с камер наблюдения банкоматов.

В результате обработки этих данных, правоохранители смогут установить большой круг подозреваемых лиц, причастных к мошеннической схеме, чтобы вручить им обоснованное подозрение». ***(Андрей Майданик. Киберполиция установила 76 активных преступных телеграм-сообществ // Internetua (http://internetua.com/kiberpoliciya-ustanovila-76-aktivnyh-prestupnyh-telegram-soobsxestv). 23.12.2021).***

***

«В течение ноября-декабря 2021 года киберполицейские провели профилактическую операцию под условным названием «ДАТА» для противодействия незаконному распространению персональных данных граждан, баз данных, а также установке предприятий и организаций, которые могут быть причастны к нарушению законодательства Украины в сфере обращения персональных данных.

Установлен 51 человек, причастный к противоправной деятельности. Действия фигурантов были направлены на незаконное завладение персональными данными граждан, закрытыми сведениями о ведении финансово-хозяйственной деятельности физических и юридических лиц, информацией о клиентах банковских и коммерческих учреждений, данными для авторизации на электронных почтовых ящиках, соцсетях, интернет-магазинах и т.д.

По результатам операции изъято около 100 баз персональных данных, актуальных на 2020-2021 годы. В изъятых базах содержались сведения более чем на 300 миллионов граждан Украины, Европы и США.

Также правоохранители прекратили деятельность одного из крупнейших сайтов, где распространялись персональные данные как украинцев, так и иностранцев. На сайте содержались сведения о номере телефона, фамилии, имени и отчестве граждан, их месте регистрации, а в отдельных случаях - информация о предоставленных админуслугах, связанных с использованием транспортных средств.

В ходе проведения следственных действий заблокировано более 30 каналов незаконного распространения информации.

Кроме этого, киберполицейские Днепропетровщины разоблачили бывшего сотрудника сети супермаркетов по сбыту конфиденциальных данных. Мужчина незаконно собирал и продавал компаниям-конкурентам информацию, содержащую коммерческую тайну. Таким образом сеть понесла более миллиона гривен убытков.

Начальник отдела противодействия преступлениям в сфере компьютерных систем Сергей Липка отметил:

«Стоимость баз колебалась от 500 до 50 тысяч гривен – в зависимости от ее содержания и коммерческой ценности. Злоумышленники сбывали информацию на закрытых хакерских форумах, а также в соцсетях и мессенджерах. Всего проведено 117 обысков в разных регионах Украины. По результатам изъято более 90 тысяч гигабайтов информации».

Мероприятия проводились совместно с представителями Уполномоченного Верховной Рады Украины по правам человека и при поддержке международных партнеров, Главного следственного управления и Офиса генерального прокурора Украины.

«Государственный курс на диджитализацию заставил все государственные органы значительно усилить меры киберзащиты собственных систем и сохранение персональных данных, что качественно повлияло на их защищенность. Однако, существенное увеличение владельцев и распорядителей персональных данных в частном секторе ставит перед нами новые вызовы, поскольку в данном секторе наблюдается увеличение случаев утечки чувствительной информации», - подчеркнул Сергей Липка.

Уголовные производства расследуются по ст. 361 (Несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи), ст. 361-2 (Несанкционированный сбыт или распространение информации с ограниченным доступом, хранящейся в компьютерах, автоматизированных системах, компьютерных сетях или на носителях такой информации), ст. 362 (Несанкционированные действия с информацией, обрабатываемой в компьютерах, автоматизированных системах, совершенные лицом, обладающим правом доступа к ней) и ст. 182 (Нарушение неприкосновенности частной жизни) Уголовного кодекса Украины. Девятнадцати фигурантам уже объявлено подозрение. Следственные действия продолжаются». ***(Дмитрий Сизов. Киберполиция провела масштабную облаву на торговцев персональными данными // (http://internetua.com/kiberpoliciya-provela-masshtabnuua-oblavu-na-torgovcev-personalnymi-dannymi). 13.12.2021).***

***

«Житель Хмельницкой области хотел установить мобильное приложение Приват24, но посчитал, что не сможет разобраться с этим самостоятельно и пригласил к себе домой «специалиста», который пообещал помочь.

Приглашенный действительно установил программу на смартфон, однако при этом, у него внезапно возникло непреодолимое желание завладеть банковской картой хозяина квартиры.

Воспользовавшись моментом, когда хозяин вышел из комнаты, «специалист» прихватил с собой карточку и телефон с установленным приложением, пароль от которого он знал, поскольку сам же и помогал с установкой.

После этого он покинул квартиру, и, воспользовавшись украденным телефоном, сменил через Приват24 пин-код от похищенной карты. Это позволило ему беспрепятственно снимать деньги через банкомат, что он незамедлительно и сделал, обналичив 6,5 тысяч гривен в два приема.

Однако этого ему показалось мало, и в течение следующих трех дней мошенник активно обналичивал деньги с карты, а также тратил их на онлайн-игры. Когда деньги на карте закончились, злоумышленник вошел в приложение Приват24 и опустошил сбережения, накопленные в сервисе «Скарбничка». Тем самым «мастер» нанес общий ущерб доверчивому потерпевшему, в размере более 48 тысяч гривен.

Убедившись, что по истечении трех дней потерпевший так и не принял мер по предотвращению этой ситуации (не заблокировал телефон и карту), мошенник решил выжать из этой ситуации возможный максимум. Используя смартфон потерпевшего, он принялся оформлять на него онлайн-кредиты. Всего, через сервисы Moneyveo, MiLoan, InstaFinance и другие, он сумел заполучить в свое распоряжение еще более 31 тысячи гривен, после чего выкинул краденый телефон, испугавшись, что его смогут найти.

Когда мошенника действительно нашли правоохранители, он полностью признал свою вину, вернул потерпевшему часть денег и пообещал со временем полностью возместить нанесенный ущерб.

В суде его действия были квалифицированы сразу по трем статьям Уголовного Кодекса: воровство, мошенничество и взлом электронно-вычислительных систем, приведший к утечке данных. Все это вместе потянуло на 4 года лишения свободы.

Однако, учитывая отсутствие прежних судимостей, двух маленьких детей на попечении и частичное возмещение ущерба, судья принял решение, что исправление подсудимого возможно без заключения его за решетку - приговор был заменен на 3 года испытательного срока». ***(Андрей Майданик. Мужчина попросил «мастера» установить ему Приват24 и лишился 82 тысяч гривен // Internetua (http://internetua.com/mujcsina-poprosil-mastera-ustanovit-emu-privat24-i-lishilsya-82-tysyacs-griven-). 16.12.2021***

***

«Правопорушники в Інтернеті продавали технічні засоби для лічильників, які дозволяли споживачам «зменшити» плату за послуги. Фігурантам може загрожувати до шести років ув'язнення.

Протиправну діяльність п'ятьох жителів Дніпра викрили співробітники управління протидії кіберзлочинам у Дніпропетровській області спільно зі слідчими обласної поліції.

Фігуранти використовували вебсайти, на яких продавали прилади та програмно-апаратні комплекси для втручання в роботу програмного забезпечення електролічильників. Клієнтам пропонували виготовлення та встановлення різних саморобних технічних засобів для зменшення реальних показників споживання електроенергії.

Спільно зі спецпідрозділами поліції проведено 11 обшуків за адресами проживання фігурантів, в офісах, складських приміщеннях та в їхніх автівках. За результатами вилучено комп'ютерну техніку, банківські та SIM-картки, а також близько 1000 різних приладів для втручання у роботу лічильників.

Відкрито кримінальне 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. Фігурантам може загрожувати до шести років позбавлення волі. Слідчі дії тривають. Процесуальне керівництво здійснює Дніпропетровська обласна прокуратура». ***(Кіберполіція Дніпропетровщини викрила зловмисників у втручанні в програмне забезпечення електролічильників // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-dnipropetrovshhini-vikrila-zlovmisnikiv-u-vtruchanni-v-programne-zabezpechennya-elektrolichilnikiv/). 21.12.2021).***

***

«Рік тому Агентство національної безпеки (АНБ) створило Центр співпраці з кібербезпеки у відкритому бізнес-парку за межами огорожі АНБ, знищивши бар'єри між Агентством і зовнішнім світом.

Протягом минулого року завдяки обміну актуальною, контекстуалізованою розвідкою про загрози, отриманою в результаті місії розвідки іноземних сигналів АНБ, тисячі аналітичних обмінів між Центром співпраці та галузевими партнерами щодо відомих іноземних акторів допомогли визначити та визначити пріоритети критичних загроз. Уявлення, якими ділиться NSA, дають змогу партнерам виявляти зловмисників, які націлені на їхню інфраструктуру, і пом'якшувати дії, щоб захистити свої мережі та клієнтів.

«Ми бачимо лише частину картини. Ми бачимо щось у SIGINT, наші партнери бачать активність у своїх мережах. Єдиний спосіб пом'якшити загрозу – це спілкуватися та співпрацювати в режимі реального часу для досягнення результатів», – сказав Морган Адамскі, керівник Центру співпраці АНБ.

Центр співпраці з кібербезпеки представляє компанії оборонної промислової бази (DIB), які підтримують програми Міністерства оборони (DoD) для криптографії, зброї та космосу, ядерного командування та контролю, а також їхніх основних постачальників послуг. Робота, виконана за перший рік, була значною, і найкраще те, що вони тільки починаються.

Центр співпраці з кібербезпеки перший рік у цифрах:

Лише за один рік Центр збільшив свою партнерську базу з менш ніж 10 до понад 100.

Дослідження вразливості АНБ є ключовим аспектом нашої місії з кібербезпеки, оскільки ми покладаємося на багато комерційних продуктів у сфері національної безпеки та оборони. У 2021 році Центр виявив низку вразливостей, включаючи серію з п'яти критичних вразливостей у Microsoft Exchange, які постачальник має виправити.

Завдяки платформі Enduring Security Framework АНБ і CISA працювали в різних секторах, щоб досліджувати загрози безпеці 5G, опублікувавши серію з п'яти статей про загрози. Ця серія тепер доступна для всіх на NSA.gov.

За допомогою пілотної програми Protective Domain Name System (PDNS) Центр обробив понад 3,8 млрд запитів і заблокував понад 6,5 млн шкідливих доменів, включаючи відомий російський фішинг, ботнети та шкідливе програмне забезпечення. На сьогоднішній день Центр надав послуги PDNS 40 підрядникам DIB і очікує, що в наступному році буде розширено ще на сотні. Детальніше від кібербезпеки Інформаційного листа Анбал, «Вибір Protective служби DNS» або чути про проект у співпраці першого епізод Центру по співробітництву Центральної АС серії.

NSA брала участь у роботі технічних комітетів, які розробили 12 міжнародних стандартів із захищених протоколів Інтернету, безпеки 5G та IT-безпеки підприємства. Ці зусилля є надзвичайно важливими, оскільки іноземні супротивники намагаються використовувати органи стандартизації як форуми для

просування стандартів, ворожих вільному та відкритому Інтернету та цифровій демократії.

Оскільки комерційні продукти все більше покладаються на захист національних систем безпеки (NSS), через Національну програму забезпечення інформації (NIAP) Центр співпраці з кібербезпекою сертифікував 91 комерційний компонент для захисту NSS і опублікував 14 профілів захисту для підвищення безпеки цих продуктів. Профілі захисту — це інструкції, що не залежать від постачальників, які підвищують безпеку комерційних продуктів шляхом визначення належних конфігурацій…» ***(NSA's Cybersecurity Collaboration Center Celebrates First Year // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/nsas-cybersecurity-collaboration-center-celebrates-first-year/). 27.12.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Вигорання робочої сили, викликане пандемією, завдало шкоди психічному та фізичному здоров'ю працівників усіх галузей, але новий звіт від 1Password показав, що вигорання також може призвести до підвищення ризиків кібербезпеки.

1Password опитав 2500 дорослих, чия робота в основному проводиться за комп'ютером. Результати показали, що співробітники, які відчувають вигорання, втричі частіше вважають, що правила та політика безпеки «не варті клопоту», порівняно з респондентами, які не відчували вигорання.

Тривожно, що фахівці з кібербезпеки відзначилися тим, що повідомили про непропорційно високий рівень вигорання. Фахівці з кібербезпеки вдвічі частіше, ніж інші респонденти, сказали, що вони «повністю виписані» або «роблють максимум» через вигорання.

«Незважаючи на високий рівень автоматизації в сучасному діловому світі, робочі місця все ще в значній мірі залежать від людей — і, зокрема, фахівців із технологічної безпеки — для впровадження протоколів, які захищають їхні активи, дані, інформацію та, зрештою, репутацію», — зазначається у звіті.

«Коли навіть невелика кількість людей послаблює свою пильність, організації піддаються серйозному ризику. Поширене вигорання серед професіоналів у сфері безпеки та інших співробітників становить значну загрозу кібербезпеці».

Майже половина вигорілих респондентів повідомили, що створюють, завантажують або використовують програмне забезпечення та програми на своєму робочому місці без дозволу IT. Крім того, 59 відсотків співробітників, які вигоріли, повідомили, що вибирають прості паролі та використовують однакові паролі для всього, порівняно з 43 відсотками працівників, які не відчували вигорання.

На додаток до слабких заходів безпеки, дослідники виявили, що понад 64% респондентів активно шукали нову роботу або були на межі звільнення. Майже на

50 відсотків більше професіоналів у сфері безпеки повідомили, що активно шукають нову роботу, ніж інші працівники.

Недавній аналіз (ISC)I показав, що розрив кадрів у сфері кібербезпеки скорочується другий рік поспіль, але глобальна робоча сила все ще має зрости на 65 відсотків, щоб ефективно захищати важливі активи та дані.

Дефіцит робочої сили в поєднанні з вигоранням співробітників і тривала глобальна пандемія створює вразливі IT-мережі, залишаючи організації відкритими для кібератак. Для охорони здоров'я кібератаки можуть завдати шкоди безпеці пацієнтів.

Більшість опитаних співробітників, які залишили роботу в період «Великої відставки» пандемії, повідомили, що могли отримати доступ до колишніх робочих облікових записів після того, як вони залишили компанію, що вказує на ще один серйозний ризик для безпеки.

Опитування також показало, що багато співробітників, як правило, не впевнені у виникненні загроз безпеці. Більше половини опитаних співробітників сказали, що нещодавно отримали електронний лист, який міг бути фішинговим, але вони не змогли його ідентифікувати.

Оскільки все більше галузей переходять на гібридні або віддалені моделі роботи, включаючи сектор охорони здоров'я, погані суб'єкти неодмінно будуть використовувати нові ризики безпеки. Тим часом вигорання робочої сили продовжує створювати ризики для безпеки та здоров'я працівників у всіх секторах.

«Поширене вигоряння серед співробітників, зокрема фахівців з безпеки, робить організації небезпечно вразливими до атак кібербезпеки», — підсумовується у звіті.

«Хоча технології та методи, що швидко розвиваються, дозволили організаціям вижити та процвітати протягом пандемії Covid-19, їх швидка ескалація — у поєднанні з величезними збитками, які пандемія завдала життя та добробуту працівників — створила нові можливості для поганого. актори». ***(Jill McKeon. Workforce Burnout Presents Cybersecurity Risks, Report Finds // TechTarget, Inc. (https://healthitsecurity.com/news/workforce-burnout-presents-cybersecurity-risks-report-finds). 09.12.2021).***

***

«COVID-19 послужив каталізатором кібератак, коли хакери скористалися перевагами віддалених працівників у складні часи. Оскільки кількість кібератак продовжує зростати, можна стверджувати, що кібербезпека стала найбільш швидкозростаючою формою злочинної діяльності у світі.

Однією з основних причин втрати даних є помилки внутрішнього персоналу, оскільки 88% порушень даних спричинені людськими помилками. Компанії дедалі більше стурбовані ризиком ненавмисної втрати даних, оскільки важлива така конфіденційна інформація, як-от відповідність нормативним вимогам щодо захисту інтелектуальної власності (ІВ). Але як можна пом'якшити цю загрозу? Запровадження важливої подвійної перевірки має вирішальне значення для покращення культури безпеки.

Внутрішня вина

Залежність від електронної пошти значно збільшує ризик кібератаки для всіх компаній. Оскільки протягом 2020 року щодня надсилається й отримується понад 300 мільярдів електронних листів, помилки неминучі. Конфіденційна інформація та активи компанії довіряються співробітникам, і багатьом з них дозволяється здійснювати фінансові операції – часто без схвалення. Крім того, із суворими вимогами щодо захисту даних, такими як GDPR, організаціям потрібні надійні процеси, щоб зменшити загрозу того, що ці дані попадуть у чужі руки.

Фінансові штрафи, втрата довіри та переваги конкурентів – це лише деякі з потенційно руйнівних наслідків потрапляння інформації в чужі руки. Але відповідальність за захист даних працівник часто нехтує. BitMEX, одна з найбільших у світі платформ для торгівлі криптовалютою, випадково розповсюдила тисячі адрес електронної пошти приватних клієнтів, коли співробітник розповсюдив масову пошту без використання функції BCC. Але як можна було запобігти цій помилці? Співробітникам потрібна можливість позначати помилки перед натисканням кнопки «Надіслати», що надає їм покращений спосіб керування функціями електронної пошти.

Багаторівневий підхід до безпеки

Лише невелика кількість компаній має чітку стратегію, яка допоможе своїм працівникам зрозуміти, як проста помилка може поставити компанію під значний ризик; і ще менша кількість мають стратегію захисту своїх співробітників від того, щоб стати внутрішньою загрозою. Але важливіше те, що вони можуть не знати, що є доступне рішення, яке може додати рівень усвідомлення безпеки співробітників, який можна використовувати для розширення можливостей користувача під час надсилання електронних листів.

Підприємства можуть допомогти співробітникам уникнути легких помилок, таких як неправильна адреса електронної пошти або включення неправильних вкладень, забезпечуючи просту перевірку безпеки, яка сповіщає користувачів підтвердити як особу адресата, так і, якщо доречно, будь-які вкладення. Рішення можна налаштувати для роботи на основі відділу або користувача, наприклад, компанія може не хотіти, щоб HR міг помилково надсилати конфіденційну особисту інформацію комусь внутрішньо, і тому вимагатиме підтвердження для всіх електронних листів.

Використовуючи правила запобігання втраті даних, технологія також може перевірити наявність ключових слів у вмісті електронної пошти. Кожен бізнес може встановлювати власні вимоги та параметри, визначені корпоративними протоколами безпеки. Будь-які електронні листи, у тому числі вкладені файли, що містять ці ключові слова, будуть позначені прапорцем, що вимагатиме додаткового процесу підтвердження, перш ніж вони будуть надіслані без перешкод для роботи, і надасть користувачам можливість ще раз перевірити, чи слід надавати дані одержувачу(ам).

З гібридною роботою, що означає, що співробітники більш розсіяні, це як ніколи раніше важливо. Цей тип інструментів зміцнює культуру безпеки, спираючись на освіту та навчання, з цінним рішенням, яке допомагає користувачам уникнути поширених помилок електронної пошти, які неминучі, коли люди

відволікаються, втомлені або напружені. Це забезпечує важливий момент «паузи», дозволяючи людям бути впевненими, що електронні листи були надіслані потрібним людям і з потрібними вкладеннями.

Висновок

У більшості сучасних робочих середовищ електронну пошту можна вважати ключовим інструментом підвищення продуктивності, покладаючи велику частину відповідальності за безпечне використання цього інструменту на співробітників. Але допоміжний персонал із додатковим сповіщенням про те, що вони не передають конфіденційні дані помилково, допомагає підвищити обізнаність і забезпечує необхідну перевірку безпеки – поки не пізно. Ідея полягає в тому, щоб сприяти обізнаності та турботі в області, де легко допускаються помилки, не додаючи затримок у щоденному управлінні електронною поштою.

Це пов'язано з підвищенням обізнаності та покращенням культури електронної пошти, одночасно зміцнюючи облікові дані щодо відповідності. Жодна організація не застрахована від людських помилок, але наявність чіткої стратегії для вирішення проблеми неправильної адреси електронної пошти та втрати даних через електронні листи, а також зменшення пов'язаних з цим ризиків допомагає підприємствам залишатися відповідальними та безпечними». ***(Andrea Babbs. Double-Checking Your Cybersecurity // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/double-checking-your-cybersecurity/). 14.12.2021).***

***

Світові тенденції в галузі кібербезпеки

«Ми є свідками зорі нової ери цифрових досліджень. Хоча метавсесвіт зараз може бути просто модним словом, це концепція, яка набуває великої популярності. Припускаючи широке поширення, це суттєво змінить те, як люди взаємодіють один з одним. Однак цей новий засіб, за допомогою якого люди можуть підключатися в Інтернеті розширеними способами, може відкрити нові поверхні для атаки для кіберзлочинців.

У цій статті ми обговоримо проблеми захисту метавсесвіту та порівняємо вразливості кібербезпеки в метавсесвіті з тими, з якими стикаються поточні користувачі Інтернету. Ми розглянемо важливість індивідуальної відповідальності щодо кібербезпеки та кіберстійкості, а також того, як освіта та профілактика можуть запобігти тому, щоб стати жертвою хакерів.

Що таке метавсесвіт?

Термін «метавсесвіт» був введений у середині 1990-х років автором наукової фантастики Нілом Стівенсоном. Однак слово «метавсесвіт» отримало своє нинішнє популярне визначення у Facebook. Нещодавно компанія оголосила, що її міжнародно визнану назву компанії буде змінено на Meta. Це рішення було прийнято для того, щоб відобразити їхню спрямованість на те, щоб стати ключовим гравцем у метавсесвіті.

Facebook відіграє велику роль у об'єднанні людей в Інтернеті, але концепція метавсесвіту виходить далеко за межі групи у Facebook або дзвінків у Facetime. Метавсесвіт дозволяє компаніям створювати «цифрових близнюків», які можуть використовувати дані та алгоритми, щоб впливати на рішення, які приймаються керівниками в реальному житті.

Метавсесвіт визначається як цифровий світ, який поєднує віртуальну та доповнену реальність. Особи будуть орієнтуватися в цьому онлайновому світі, який може бути ідентичним справжньому або заснованим на уяві, або на певній комбінації того і іншого, використовуючи цифрові аватарки. Цифрові аватари та гарнітури віртуальної реальності дають більш глибоке уявлення про реальне життя користувачів, ніж все, що можна було б висловити в соціальних мережах. Інтимна природа метавсесвіту та дані, які він створює, нададуть широкі можливості для кіберзлочинців.

Мантія метавсесвіту

З рішеннями кібербезпеки, які пропонуються заднім числом, часто вводяться нові та захоплюючі технології. У майбутньому розробники повинні не тільки навчитися кодувати, але й повинні усвідомлювати важливість заходів кібербезпеки під час створення нових програм. Проте, як зараз, нові технології часто приходять із безпекою як позаду.

Деякі проблеми кібербезпеки з цією новою технологією будуть подібними до тих, з якими ми вже знайомі в Інтернеті. Постійне зростання кіберзлочинності протягом останніх 18 місяців показало, наскільки прибутковим може бути злам компанії або особистих онлайн-рахунків.

Однак, поряд зі звичайним фішингом, шкідливим програмним забезпеченням і хакерством, з якими ми знайомі, метавсесвіт, ймовірно, принесе абсолютно нові кіберзлочини через свою інфраструктуру. Метавсесвіт значною мірою зосереджений на використанні криптовалют і незмінних токенів (NFTS), які можуть бути привабливою мішенню для кіберзлочинців з різних причин.

Наприклад, відомий арт-дилер Sotheby's нещодавно представив Sotheby's Metaverse, який виставляє на аукціони вибрані NFTS, які перевіряються за допомогою процесу, який називається карбуванням. Витвори мистецтва перевіряються та відстежуються в цифровому вигляді шляхом розміщення в загальнодоступній книзі блокчейну через Ethereum. Однак, як і в реальному світі мистецтва, колекціонерів можна легко обдурити копіями, які виробляють кіберзлочинці, які вважаються законними аутентифікаторами.

Крім того, трансакції Ethereum можуть бути вразливими до шахраїв, які сквотують на веб-сайтах.eth під назвою іншої компанії. Як і підробка домену, кіберзлочинці можуть покладатися на впізнаваність усталеного бізнесу, щоб створити підроблені доменні імена та смарт-контракти Ethereum. Транзакції настільки безпечні, як і організація, яка їх виконує, а в Інтернеті може бути важко визначити, з ким саме ви маєте справу.

У метавсесвіті завдати шкоди компанії не так просто, як залишити негативний відгук в Інтернеті або розбити скло за прилавком, щоб вкрасти предмет. Оскільки кілька шарів доповненої або віртуальної реальності приховують

справжню особу зловмисників, потерпілим від крадіжки чи переслідування важко або неможливо звернутися до суду.

Проблеми забезпечення метавсесвіту

Ще одна проблема з метавсесвітом — це його залежність від апаратного забезпечення, щоб випробувати платформу. Метавсесвіт зосереджений на зовнішніх цифрових пристроях, таких як гарнітури віртуальної реальності, які можуть легко стати жертвою хакерів, якщо їх залишити без захисту.

Дані, отримані через ці гарнітури або будь-які інші носії, які, безсумнівно, будуть представлені в майбутньому, можуть бути дуже чутливими за своєю природою. Дані, які потрапляють у чужі руки, можна легко перетворити на погрози шантажу або на паливо для змови з соціальної інженерії від кіберзлочинця. Крім того, інтелектуальну власність може бути важче захистити, коли люди та компанії живуть не лише в реальному світі, а й у метавсесвіті.

На жаль, політики іноді відстають у вирішенні технологічних проблем. Закони рідко відображають швидко мінливі способи взаємодії людей один з одним онлайн. Врахуйте той факт, що середній вік сенатора США становить 64 роки. Велика частина технологій, які формують світ навколо нас сьогодні, дуже чужа поколінню людей, які ухвалюють закони для країни. Це частково пояснює, чому кіберзлочинність залишається такою привабливою сьогодні.

На жаль, нові технології часто розробляються та вводяться на ринок задовго до вирішення проблем кібербезпеки. Коли споживачі почали розуміти, що передові пристрої Інтернету речей, такі як розумні помічники, системи безпеки розумного дому, фітнес-трекери тощо, мають мінімальні вбудовані засоби кібербезпеки, закони повинні були змінитися, щоб захистити цих споживачів. Однак лише у 2021 році Конгрес представив законопроект про безпеку, який вводить стандарти кібербезпеки для пристроїв IoT, що продаються на ринку.

Як утримати злочинність від метавсесвіту?

Немає однозначної відповіді на питання, як зробити метавсесвіт безпечнішим місцем. Як і в Інтернеті, ймовірно, завжди буде певний рівень анонімності, який захистить злочинців. Це може дозволити їм безкарно позбутися такої поведінки, як крадіжка, кіберпереслідування, доксінг та переслідування в Інтернеті.

Можливе посилення регулювання Інтернету. Однак Інтернет залишається одним із останніх кордонів свободи слова та інформації. Поширений контроль над Інтернетом з боку державних органів у майбутньому настільки ж малоймовірний, як і неетичний.

Освіта та профілактика залишаються найкращим способом для людей і бізнесу залишатися в безпеці в Інтернеті, а в майбутньому і в метавсесвіті. Розуміння ризиків, притаманних онлайн-діяльності, і використання правильних ресурсів кібербезпеки, щоб захистити себе та свою організацію, є ключем до збереження кіберстійкості в цю нову епоху». ***(Cybersecurity and the Metaverse: Pioneering Safely into a New Digital World // Security Boulevard (https://securityboulevard.com/2021/12/cybersecurity-and-the-metaverse-pioneering-safely-into-a-new-digital-world/). 10.12.2021).***

***

«Доступність Інтернету створила культуру, де все доступне кожному в будь-який час. Ми можемо ділитися думками та співпрацювати з окремими особами по всьому світу, а Інтернет є домом для найбільшої бази даних ресурсів «як робити», коли-небудь створених.

Кібербезпека не є винятком із цієї тенденції, і, на жаль, ця доступність означає, що тепер будь-хто може стати кіберзлочинцем. Образ геніальних акторів-загроз, прихованих за незліченною кількістю комп'ютерів, які розробляють складну атаку, більше не відображає сучасних сучасних злочинців. Завдяки розробці фішингових наборів наступною людиною, яка націлена на ваш бізнес, може бути будь-хто, кого ви пройдете на вулиці.

Враховуючи їх адаптивність і відносно просту природу, фішингові атаки залишаються популярним прийомом, який використовується суб'єктами загроз, особливо протягом тривалого періоду віддаленої роботи. Однією з найбільших тенденцій, які ми помітили, є зростання кількості фішингових сайтів, націлених на користувачів рахунків у банку Chase. Дослідження показали збільшення кількості фішингових URL-адрес за допомогою бренду Chase на 300 відсотків.

Кіберіндустрія стала свідком кількох подій у секторі фішингу, всі такі ж загрозливі, як і останні.

Тенденції зростання фішингових атак

Фішинг завжди був найкращим другом актора: він простий, адаптований і недорогий. Незалежно від того, як розвивався ширший ландшафт загроз електронної пошти та шкідливого програмного забезпечення, фішинг залишається в центрі.

Основною мотивацією кожного фішера є отримання облікових даних, які відкривають сховище даних або фінансів бізнесу. Однак останнім часом зросла кількість зловмисників, які безпосередньо переслідують цінну інформацію, таку як банківські реквізити або номери соціального страхування, замість того, щоб шукати легких цілей, як-от імена користувачів та паролі. Так, цю інформацію важче отримати, але вигідні винагороди варті деяких додаткових зусиль.

Хоча фішинг часто використовується як одноетапна атака, він також використовується в більших багатоетапних кампаніях. Фішинг, як правило, є першим кроком – як техніка, яка використовується для отримання початкового доступу до мережі – але потім слідує другий етап з іншою метою, наприклад, програмним забезпеченням-вимагачем. Ці багатоетапні атаки можуть бути надзвичайно шкідливими для бізнесу, але все починається з простого фішингового електронного листа.

Однак тенденція номер один, за якою ми стежимо, — це розробка комплектів для фішингу. Регулярно випускаються нові набори, останні зосереджені на використанні мобільних пристроїв для обману жертв. Завдяки безперервній змішаній роботі, IT-командам та командам безпеки не вистачає повної видимості, якими пристроями користуються працівники вдома, чи дотримуються правильні процедури та методи всіма працівниками. Один наївний і вразливий співробітник може бути все, що потрібно, щоб зруйнувати захист компанії.

Перехід до фішингових комплектів

Фішингові набори стають набагато доступнішими в Інтернеті і, по суті, є пакетом «зроби сам» для фішингових атак. Набори містять код для налаштування фішингового сайту, який легко розгортається, коли особа купує необхідний домен. На цьому етапі користувач повинен просто отримати свої цілі електронної пошти, які можна легко знайти в Інтернеті, і почати. Для тих, хто бажає зробити атаки більш ефективними, існують технології, які можуть автоматизувати процес і їх можна залишити без нагляду.

Наше дослідження фішингових комплектів показало, що ці «початкові набори» швидко стають все більш досконалими і тепер створені для збору цінних даних, включаючи інформацію про банківські та кредитні картки, домашні адреси та номери соціального страхування. Ми знайшли на ринку популярний комплект під назвою Chase XBALTI, який спеціально націлений на власників акаунтів Chase і Amazon. Особи, яка розгортає набір, більше не потрібно бути вправним хакером, оскільки технологія робить все за них. Насправді ми бачили набори, які були створені для захоплення одноразових кодів, які використовуються для багатофакторної аутентифікації (MFA), що робить їх ще більш загрозливими.

Без сумніву, ці комплекти революціонізують обличчя фішингу.

Як боротися з фішингом

Як правило, всі організації повинні дотримуватися основних кібергігієнічних правил. Це включає використання MFA в якомога більшій кількості процесів, уникнення повторного використання паролів і довіру до свого інтуїції. У більшості випадків, якщо щось здається оманливим, то, ймовірно, це так. Дуже важливо, щоб усі компанії цінували справжню цінність людської інтуїції, оскільки це один із найпотужніших інструментів у наборі інструментів команди безпеки. Навчання співробітників розпізнавати ознаки фішингової атаки за допомогою тренінгів щодо безпеки, а потім оснащення їх застосуванням цих знань на практиці буде дуже ефективним проти методів соціальної інженерії злочинців. Просто зв'язатися з банком для підтвердження електронної пошти може бути відмінністю між успішною та попередженою кібератакою.

Існує кілька інших форм захисту від фішингових атак, які підходять для будь-якого бюджету. Для початку компаніям варто розглянути можливість розгортання рішення безпеки електронної пошти, яке аналізує вміст електронної пошти, щоб визначити, чи є він справжнім. Вбудовані фільтри електронної пошти можуть забезпечити високу швидкість виявлення широкого вибору вхідних загроз, таких як зловмисне програмне забезпечення, спам та будь-які добре відомі фішингові URL-адреси. Цей захист можна посилити за допомогою спеціальних рівнів виявлення, які вивчають та ідентифікують більш розвинені загрози за допомогою машинного навчання та обробки природної мови.

Кількість вхідних фішингових атак не вказує на сповільнення, тому дуже важливо, щоб підприємства діяли швидко. Крім того, оскільки фішингові набори стають доступнішими з кожним днем, кількість потенційних зловмисників швидко зростає. Хоча не всі вони можуть бути злочинцями, які мають у своєму розпорядженні набір інструментів, повний передових навичок і методів, набори, які використовуються, мають достатньо можливостей, щоб виявити упущені слабкі місця в периметрі компанії. Якщо лише один фішинговий лист успішно обдурить

співробітника, це може бути все, що потрібно. Щоб не стати наступною жертвою, підприємства не можуть дозволити собі недооцінювати силу фішингових наборів і тих, хто бажає ними скористатися». ***(Magni Sigurpsson. Can anyone go phishing? // Future US, Inc. (https://www.techradar.com/features/can-anyone-go-phishing). 10.12.2021).***

***

«Незважаючи на нові та все більш складні кіберзагрози, що з'являються щодня, більшість організацій продовжують покладатися на власні команди безпеки, щоб захистити свої мережі та інфраструктуру в ізоляції. Однак покладатися на власні дані кібербезпеки вже недостатньо для організації, щоб ефективно захищатися від останніх кіберзагроз.

Такий ізольований підхід спричинив тривалий період, потрібний організації, щоб виявити порушення даних, у середньому 191 день, не кажучи вже про ефективний захист від цих атак. Таким чином, незважаючи на різкі витрати на кібербезпеку, сьогоднішній кіберзахист виявляється невдалим і більше неефективним.

На щастя, завдяки новим і новим технологіям є способи покращити кібербезпеку організацій, наприклад, за допомогою спільного кіберзахисту. Це означає, що організації об'єднуються для співпраці над своїми даними кібербезпеки, наприклад, даними про показники компромісу (IoC).

Маючи більший обсяг цінних даних, доступних для кожної організації, яка співпрацює, усі вони зможуть:

1. Краще передбачати та визначати майбутні кібератаки

Завдяки отриманим колективним уявленням організації можуть порівнювати себе з аналогами за історичними даними МОК та ефективності витрат на кіберзахист. Організації також можуть навчати моделі на набагато більшому наборі даних, ніж той, що доступний в одній організації, що допоможе їм краще передбачати майбутні атаки.

2. Підвищити надійність планів реагування на інциденти

Маючи більше уявлень і глибше розуміючи більшу кількість кібератак, організації можуть удосконалити та покращити свої плани реагування на інциденти, щоб краще задовольнити ширший спектр загроз. Організації також можуть співпрацювати над скоординованими відповідями на подібні загрози, з якими вони стикаються.

3. Зменшити витрати на кібербезпеку

Оскільки організації працюють з більшим набором даних і потенційно координують свої відповіді, вони можуть бути більш ефективними з витратами на кібербезпеку.

Чому організації не співпрацюють у сфері кібербезпеки?

Хоча деякі організації можуть захотіти співпрацювати над своїм кіберзахисту, дані кібербезпеки, такі як інциденти, вразливості та атаки, зазвичай є надзвичайно чутливими, конфіденційними, і тому їх використання обмежено.

Організації дуже неохоче діляться цими конфіденційними та обмеженими даними зі своїми партнерами чи іншими компаніями у своїй галузі. Організації

були б готові співпрацювати над даними кібербезпеки, лише якби вони знали, що їхні конфіденційні дані не побачать сторонні сторони, особливо інші організації в їхній галузі.

Як сьогодні організації можуть безпечно співпрацювати з кіберзахисту?

На щастя, вже існує кілька способів спільної роботи над даними кібербезпеки, не розкриваючи дані стороннім особам, у різному ступені.

Перший — використовувати довірені треті сторони, які діють як посередники, які конфіденційно керують і аналізують дані від кількох організацій, перш ніж поділитися індивідуальними думками та результатами з відповідними учасниками. Хоча організації-учасниці не можуть бачити конфіденційні дані одна одної, вони все одно зобов'язані поділитися цими даними з довіреною третьою стороною. Все ще існує ймовірність злому або розкриття їхніх даних, що не ідеально для багатьох організацій.

Нові технології можуть вирішити проблему повної конфіденційності даних. Технологія безпечного шифрування на основі анклаву, що використовується, така як конфіденційні обчислення, а також програмні методи шифрування, такі як безпечні багатосторонні обчислення (SMPC) і гомоморфне шифрування, можуть гарантувати, що конфіденційність даних ніколи не буде порушена.

SMPC і гомоморфне шифрування засновані на передовій криптографії, яка гарантує, що дані завжди залишаються зашифрованими, і що жодна третя сторона не зможе побачити дані навіть під час виконання обчислень. Конфіденційні обчислення гарантують, що дані також шифруються під час обчислень та аналізу, а генеруються лише агреговані результати.

Таким чином, організації, що співпрацюють, не зможуть бачити дані про кібербезпеку одна одної, навіть якщо загальний обсяг даних збільшується і веде до більш глибокого розуміння.

Конфіденційні обчислення також гарантують, що постачальник інфраструктури та хмари не зможе переглядати або отримати доступ до даних організацій, які співпрацюють. Наприклад, якщо організації співпрацювали над своїми даними кібербезпеки на платформі, заснованій на конфіденційних обчисленнях, ні постачальник платформи, ні постачальник хмари не могли бачити їхні конфіденційні дані. Це ще більше підвищить конфіденційність і конфіденційність даних кібербезпеки.

Настав час співпрацювати над даними кібербезпеки та зміцнювати свій кіберзахист

Наявність технологій, які гарантують конфіденційність конфіденційних даних навіть під час обчислень, означає, що організації можуть легше та безпечніше співпрацювати над своїми даними кібербезпеки, не боячись розкрити свої конфіденційні дані стороннім особам. У зв'язку з загрозою кібератак, що розвиваються, організації та їхні найбільш чутливі й цінні дані стають все більш уразливими до злому. Зараз настав час для організацій об'єднатися, щоб протистояти загрозі кібератак, що постійно розвивається та зростає». ***(Maximilian Groth. Now is the optimal time for orgs to collaborate on cybersecurity // VentureBeat. (https://venturebeat.com/2021/12/09/now-is-the-optimal-time-for-orgs-to-collaborate-on-cybersecurity/). 09.12.2021).***

***

«Як правило, фінансові консультанти хочуть отримати чітке уявлення про кібербезпеку. Пріоритетним є захист даних клієнта. Кібератаки дуже критичні. Це може вплинути на інвестиції від імені своїх клієнтів. CNBC повідомляє, що кілька компаній схильні до дорогих кібератак порівняно з іншими. Слідкуйте за статтею, оскільки ми збираємося обговорити кілька речей. Основним ризиком є охорона здоров'я, енергетика та виробництво. Історично ці сектори не інвестували багато в інші цінні папери, такі як фінансові послуги або технології.

Fi фінансові консультанти повинні приймати кібербезпека серйозно

Головний технологічний директор Mandiant пан Чарльз Кармакал сказав, що частина способу оцінки кіберзагроз компанії полягає в тому, щоб знати реальні загрози. Кармакал додав, що не всі організації стикаються з подібними загрозами. Для охорони здоров'я існують різні види загроз; це різні. Спільне те, що всі небезпечні.

Ми можемо дізнатися, що існує кілька типів пов'язаних проблем. Чарльз Кармакал запропонував кілька речей. Дивлячись на зрілість безпеки компанії, він сказав, що багато компаній мають серйозні інциденти з кібербезпекою. Вона, як правило, стає більш безпечною після того, як організація, можливо, не живе.

Кармакал також додав, що серйозно займається цим питанням. І Carmakal, і Equifax стикалися з подібними ситуаціями кібербезпеки. Обидва вони є найгіршими жертвами кібербезпеки.

Люди часто стають жертвами кібератак

Є одна гарна новина для всіх інвесторів. Корпоративні зали засідань, здається, більш зосереджені, ніж інші. Він також сказав, що всі люди ставляться до цього серйозніше. Таким чином, це є результатом збільшення кількості людей, які володіють технологіями та безпекою, у залі засідань. Це думки Кармакала і Фарщі. Усе «якщо-то» підійшло до висновку і серйозно поставилося до питання кібербезпеки. Головне, щоб споживачі були обережні. Нині це серйозна загроза. Багато людей втрачають свої цінні заробітки. Особи повинні проаналізувати та оцінити пов'язані з цим ризики, перш ніж приймати рішення щодо фінансового плану». ***(David Crabtree. Cybersecurity: A Dilemma For Financial Advisors // Chronicle News (https://chronicle99.com/2021/12/09/cybersecurity-a-dilemma-for-financial-advisors/). 09.12.2021).***

***

«Зазирніть на соціальні мережі в будь-який день, і ми почуємо від коментаторів, які стверджують, що існує нестача (кібер) навичок і що її необхідно усунути, якщо ми хочемо вирішувати проблеми, з якими ми все частіше стикаємося.

Давайте прояснимо щось, перш ніж продовжити. Якщо ми говоримо про дефіцит навичок, то є організації, які вже зараз готові наймати фахівців з кібербезпеки. Припускається, що ці фахівці не мають належних навичок, які шукають організації.

Але наскільки це правда?

Життя та часи професіоналів з кібербезпеки

Міжнародна асоціація безпеки інформаційних систем (ISSA) опитала 489 спеціалістів із кібербезпеки, щоб дізнатися їхню думку щодо проблем, пов'язаних із дефіцитом кібернавичок. Потім ISSA опублікувала свої відповіді в The Life and Times of Cybersecurity Professionals 2021.

Підсумовуючи, результати звіту полягають у тому, що для подолання дефіциту навичок необхідний більш цілісний підхід до безперервної освіти з кібербезпеки. Це повинно розпочатися з публічної освіти і поширитися на всебічний розвиток кар'єри, складання карт і стратегію планування, функції, які підтримуватимуться та інтегруються в бізнес.

Звичайно, це не станеться за одну ніч, якщо це взагалі можливо. Однак дослідження продовжує стверджувати, що одна, здавалося б, проста зміна, яку можуть зробити організації, — це підвищити заробітну плату та компенсації для фахівців з кібербезпеки.

Але чи може це статися без змін у самому секторі кібербезпеки?

Правда в тому, що я вважаю, що є дві проблеми, які ми повинні вирішити, перш ніж ми зможемо закрити цей усвідомлений розрив у навичках. Справді, я взагалі не відчуваю, що в навичках кібербезпеки немає. Принаймні не такий, про який думає більшість людей. Я вважаю, що існують фундаментальні непорозуміння та розуміння того, що таке кібербезпека. Існує нестача комунікацій, а не навичок кібербезпеки.

Кібербезпека: бізнес-перспектива

Почнемо з тих, хто не є нашою галуззю. Коли організації наймають фахівців з кібербезпеки, вони повинні чітко уявляти, яку проблему вони намагаються вирішити, а потім наймати відповідним чином. Якщо відповідь полягає в тому, щоб збільшити винагороду, запропоновану професіоналам з кібербезпеки, як свідчить звіт ISSA, то організація повинна знати, яку цінність вони отримають. Рекрутерам також потрібно більше працювати, щоб зрозуміти професію кібербезпеки, оскільки, виходячи з особистого досвіду, вони цього не роблять. Я пригадую, як у 2018 році розмовляв із рекрутером, який шукав спеціалістів із захисту даних з «п'ятирічним досвідом роботи в GDPR.». Як можна отримати п'ятирічний досвід роботи в законодавстві, яке було введено лише за два роки до цього, можна тільки здогадуватися!

Ми знаємо, що підтримка кібербезпеки за столом Ради була боротьбою протягом багатьох років. Ця проблема отримання підтримки зверху поширюється на найм людей на ролі, де не спостерігається негайної вигоди. Компанії повинні визнати, що (залежно від назви посади) роль спеціаліста з кібербезпеки є переважно профілактичною. На жаль, бізнес вважає, що кібербезпека є центром витрат, а також витратою, яку можна відкладати на невизначений термін.

З цим пов'язані витрати, пов'язані з постійним удосконаленням і підвищенням кваліфікації спеціаліста з кібербезпеки. Навчання та професійна освіта для фахівців з кібербезпеки часто значно дорожчі, ніж інші форми навчання. Це також ніколи не припиняється. Які навички, інструменти та методи, які ви використовуєте зараз, можуть бути застарілими через два роки (або менше).

Одним із рішень цієї проблеми є інвестування в аутсорсинг потреб у кібербезпеці організаціям, які пропонують повністю керовані послуги. Це покладає тягар найму, навчання та утримання професіоналів з кібербезпеки на організації, які краще оснащені для надання цих послуг.

З точки зору бізнесу, немає пробілу в навичках кібербезпеки. Існує лише різниця між очікуваннями (бізнесу) та сприйнятою цінністю, яку вони отримують. Як професіонали з кібербезпеки, я вважаю, що наша роль полягає в тому, щоб стати кращими комунікаторами, навчити бізнес цінності, яку вони отримають від кібербезпеки, і допомогти їм зрозуміти, які ресурси (людські чи технічні) допоможуть їм найбільше.

Кібербезпека: професія

Я вже давно стверджував, що кібербезпека — це професія, і її слід поважати як таку. Якщо ми (як професіонали) почнемо бачити себе такими, як лікарі та юристи, то я думаю, що ми почнемо бачити деяку плутанину у відношенні розриву в навичках.

Кібербезпека багатогранна, і кожен аспект вимагає різного набору навичок та знань, якщо ми хочемо бути ефективними в цій сфері. Щоб досягти успіху в цій сфері, я вважаю, що існують основні навички та знання, які люди повинні розвивати шляхом формального навчання або саморозвитку.

Зараз багато університетів пропонують офіційні дипломи з кібербезпеки. Це не означає, що вони не мають цінності, але в житті є більше, ніж університет. Наприклад, я знаю багатьох випускників університетів, які ніколи не стикалися з Книгою знань з кібербезпеки (CyBok). CyBok — це посібник, який кодифікує інформацію, яка вже існує в літературі, таку як підручники, академічні науково-дослідні статті, технічні звіти, технічні документи та стандарти, що об’єднує єдиний ресурс для практиків для перегляду та розвитку своїх знань.

Натисніть тут, щоб отримати більше інформації про CyBok.

CyBok, звичайно, не єдиний шлях, яким ми можемо розвиватися в цій сфері. Професіонал може отримати широкий спектр сертифікатів та значків, якщо у нього є час і (великий) бюджет для проходження курсів та іспитів.

Серед багатьох на вибір є кілька видатних сертифікатів, які шукають багато організацій. Серед них:

Сертифікований спеціаліст з безпеки інформаційних систем (CISSP)

Сертифікований менеджмент інформаційної безпеки (CISM)

Сертифікований аудитор інформаційної безпеки (CISA)

Сертифікований етичний хакер (CEH)

Існує безліч інших, на які варто звернути увагу, коли ви познайомитеся з специфічними для постачальників технологіями, такими як Amazon Web Services, Microsoft Azure, і навіть більше, коли розглядаєте управління та захист даних.

Це знову змушує професіоналів (особливо «нубів») замислюватися, яким шляхом піти, і, зрештою, це залишає у них прогалини в знаннях. З цієї причини я більше не гнаюся за цими значками, а вважаю за краще розширювати свою мережу та навчатися у тих, хто мене оточує. Натомість я вважаю за краще здобувати практичний досвід у однолітків та наставників.

Це одна з причин, чому я приєднався до Chartered Institute of Information Security (CIISec). Інститут був започаткований у 2006 році з метою підвищення рівня професіоналізму в галузі інформаційної та кібербезпеки. Як незалежний некомерційний орган, яким керують його члени, CIISec є координаційним центром для професії інформаційної кібербезпеки. Метою є розробка стандартів професіоналізму для навчання, кваліфікації, операційної практики та окремих осіб.

CIISec має дедалі більше членів, які представляють понад 10 000 осіб у галузі інформаційної та кібербезпеки. Він має структурований план навчання та розвитку від початкового рівня до членства «Спільники».

Щоб розвиватися в рамках цієї професії, ми повинні визнати, що ми повинні вийти за рамки «збирання значків», а також розвивати наші мережі та асоціації з професіоналами-однодумцями, щоб ми могли вчитися один у одного. У звіті ISSA, на який посилалися раніше, підкреслюється необхідність для фахівців з кібербезпеки розробити поєднання практичного досвіду, базових сертифікатів і мереж. Мережа стосується не технічних знань, а того факту, що професіонали повинні об'єднуватися всередині та поза власними галузями та сектором.

Недолік навичок кібербезпеки для професіоналів полягає в тому, що нам потрібно вийти із зони комфорту та зайнятися більш широкою темою кібербезпеки. Як професіонали, ми повинні зрозуміти, чого хоче і чого потребує бізнес, і навчитися деяким з тих «м'яких» навичок, які, здається, так важко розвинути. А саме, нам потрібно закрити комунікаційний розрив і працювати над власною маркетинговою стратегією.

Висновок

У 2020 році уряд Великої Британії піддався жорсткій критиці за рекламну кампанію, в якій була зображена балерина (на ім'я Фатіма), яка стверджувала, що «Наступна робота Фатіми може бути в кіберпрограмі. Просто вона цього ще не знає».

Звісно, реклама впала, як і можна було очікувати – погано! Але що це говорить нам про ставлення до індустрії кібербезпеки? Я вважаю, що це говорить нам про багато, і ми повинні почати звертати увагу.

Компанії повинні цінувати цінність, яку приносить кібербезпека, навіть якщо вони не відразу бачать і не відчувають її. Якщо вони не хочуть наймати свої власні команди, передайте це керованому постачальнику послуг, який може взяти на себе відповідальність за вас. Фахівці з кібербезпеки також повинні розуміти, що підприємства не відразу сприйматимуть їх як цінний актив. Нам потрібно змінити наш підхід до повідомлення про необхідність того, що ми робимо, не налякаючи їх історіями та статистикою, а ставши кращими комунікаторами цінності, яку ми приносимо.

Простіше кажучи, немає пробілу в навичках кібербезпеки. Просто розрив у спілкуванні». ***(Gary Hibberd. The Cybersecurity Skills Gap: Myth or Reality? // Tripwire, Inc. (https://www.tripwire.com/state-of-security/security-data-protection/cybersecurity-skills-gap-myth-or-reality/). 08.12.2021).***

***

«Оглядаючи ретроспективу, 2021 рік пройшов як вихор для тих із нас, хто займається кібербезпекою. Ми відчули прискорений зсув до світу, в якому його відмінності, визначення та категоріальні ідентичності ставали все більш пористими.

Фізичний і цифровий світ продовжували зливатися, настільки, що будь-який бар'єр, який існував між ними, тепер майже зник. Зростання цієї пористості та пов'язане з нею збільшення векторів атаки посилювалося розширенням Інтернету речей (IoT) та більш взаємопов'язаним і пов'язаним середовищем, яке воно створює.

Це підводить нас до того, що ми можемо вважати основними проблем цього року, що відображено в компромісах SolarWinds і Colonial Pipeline: постійне зростання успішних атак програм-вимагачів і оприлюднення наказу щодо програмного забезпечення (SBOM). Ці події виділяються як відображення того, що я вважаю найбільш значущим, коли мова йде про те, що ми побачили у 2021 році, і є основою того, що ми можемо очікувати побачити в наступному році.

SolarWinds

Додатковою складністю цього компромісу стало зростання та прийняття безперервного впровадження/безперервної доставки (CI/CD) протягом багатьох років як основи сучасних операцій DevOps. CI/CD являє собою підхід до розробки програмного забезпечення, який прагне використовувати коротші цикли розробки для забезпечення постійного потоку потенційно руйнівних інновацій для клієнтів, які невпинно вимагають «більше, швидше».

SolarWinds змусив нас тривожно усвідомити наслідки фундаментальної системи, оновлення якої були скомпрометовані та розповсюджувалися таким чином, як було виявлено. Контекстний бойовий простір, у якому відбувалося це поширення, ще більше посилювався зростаючою пористістю, згаданою вище, що складає сучасний ланцюжок поставок, надаючи противнику майже необмежену кількість «найслабших витоків», за допомогою яких можна досліджувати варіанти та усвідомлювати плоди своїх зусиль.

Колоніальний трубопровід

Уроки, проголошені компромісом колоніального трубопроводу в травні минулого року, були нещодавно перемежовані справою з іранськими газовими насосами. Ці зрозумілі аспекти повсякденного життя не повинні бути відмовлятися нам дуже довго, перш ніж неприйнятний біль поселиться. Колоніальний трубопровід, який забезпечує 45% постачання різноманітного палива на Східне узбережжя, був вимкнений після нього постраждала від атаки програмного забезпечення-вимагача. Тепер, на іншому кінці світу, чергова кібератака залишила водіїв в Ірані практично без палива. Повідомляється, що онлайн-атака пошкодила практично кожну заправку в Ірані — іронія, оскільки ця країна є провідним експортером нафти.

Програми-вимагачі на підйомі

Справа Colonial Pipeline була лише одним із прикладів того, як у 2021 році атаки програм-вимагачів захопили заголовки газет — незважаючи на існування перевірених математичних моделей, що підтримуються штучним інтелектом, чия майстерність проти таких атак досі добре задокументована. Те, що інерція, схоже,

все ще тримає великі компанії та інфраструктури країн зі списку Fortune 500 у в'язнях і наполегливо відданих застарілим моделям оборони вражає раціональне розуміння. Те, що сучасні атаки програм-вимагачів, здається, легко обходять усталені стовпи традиційного кіберзахисту, підкреслює необхідність пошуку нових шляхів вирішення цієї проблеми. Просування тих самих старих рішень, очікування різних результатів — це класичне визначення «божевілля».

Виконавчий наказ

Доводячи, що наслідки цих видатних подій для ланцюга поставок не залишилися без уваги, адміністрація президента США видала виконавчий указ, суть якого вимагає від тих, хто виробляє та розповсюджує програмне забезпечення, по-новому знати про свій ланцюжок поставок, щоб деталізувати, що насправді є в їхніх продуктах. — зокрема програмне забезпечення з відкритим кодом — і здатність відображати це усвідомлення в точному SBOM. Оскільки оголошені вразливості стають все більш поширеними, ці SBOM нададуть покупцям спосіб визначити, наскільки будь-яке оголошення може відповідати їхнім інтересам.

Куди йти звідси

Хоча прогнозування майбутнього є складною справою за найкращих обставин, це, можливо, полегшується тим фактом, що ми, як люди, так часто відмовляємося вчитися з минулого і, отже, приречені повторювати його, як Джордж Сантаяна часто цитується. Таким чином, передбачення майбутнього частково стає практикою виокремлення тих уроків, які ми повинні були засвоїти, але цього не зробили, і перетворення їх у те, що ми, ймовірно, знову випробуємо. Геракліт Ефеський висловив думку, що ви не можете увійти в одну і ту ж річку двічі, але ці повторювані переживання повинні бути достатньо подібними, щоб дозволити зрозуміти, які пом'якшувальні дії можуть бути відкритими для нас.

Ми дізналися, що, мабуть, наші математичні моделі можуть передбачати і продовжують робити це принаймні в обмеженій сфері шкідливих програм. Насправді вони знають, яка атака буде наступною — часто роками наперед. В інших сферах нам не так пощастило. Однак ми можемо використовувати наявну інформацію, щоб якнайкраще підготуватися до будь-якого можливого сценарію. Ми знаємо, яка технологія розробляється, і ми знаємо потенційні ризики, які з нею пов'язані. Ми бачили, як противники можуть використовувати силу добра, щоб завдати шкоди. Кожен у спільноті кібербезпеки повинен забезпечити наявність розумних і потужних засобів захисту в наступному році для захисту від цих загроз…». ***(John McClurg. A cybersecurity year in review // BNP Media (https://www.securitymagazine.com/articles/96655-a-cybersecurity-year-in-review). 08.12.2021).***

***

«Исследование, проведенное Mastercard для Kantar, показало, что кибербезопасность становится все более важной для потребителей, поскольку они все больше входят в цифровую экономику. Согласно данным «Барометра цифровой безопасности», 87% потребителей осведомлены о кибератаках, 75% сообщили, что так или иначе были жертвами киберпреступников, а 20% заявили, что компания утекла их личную информацию.

Менее чем за десять лет кибербезопасность стала одной из важнейших системных проблем мировой экономики. Кибератаки становятся все более изощренными и дорогостоящими, создавая проблему в размере 350 миллиардов долларов во всем мире и ежегодно принося убытки в размере 5,2 триллиона долларов. Поскольку использование цифровых услуг увеличивалось во время пандемии COVID-19, также быстро росло мошенничество, мошенничество и кибератаки против частных лиц и предприятий.

Другие данные исследования Mastercard Digital Security Barometer показывают следующее:

Защита личных данных также важна: с ростом оцифровки возникает опасение, что личные данные будут раскрыты. Согласно опросу, защита персональных данных является деликатным вопросом в регионе. Потребители осведомлены о последствиях, которые может иметь нарушение безопасности их личной информации. Для 92% потребителей раскрытие их номера социального страхования, номера мобильного телефона и результатов медицинского осмотра может нанести «наибольший вред».

Потребители проявляют все большую активность в поисках защиты: когда их спросили, «насколько безопасно, по вашему мнению, компании хранят вашу информацию», средний балл составил 3 балла по шкале от 0 до 10, где 0 означает «Не уверен», а 10 - «Очень безопасно». В результате такого восприятия 70% опрошенных заявили, что они приняли биометрический идентификатор.

Потребители требуют большей ясности: почти каждый испытывал разочарование от попыток расшифровать очень короткие или неузнаваемые описания покупок, просматривая выписки по своим картам в Интернете. В Латинской Америке 77% потребителей не могут определить, чему соответствуют некоторые транзакции, отображаемые в их цифровых аккаунтах…» ***(Cybersecurity is a priority for Latin American consumers: report // Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/401030). 06.12.2021).***

***

«Існує багато бар'єрів на шляху до кар'єри в галузі кібербезпеки — принаймні так вважає сьогоднішня робоча сила. На заході (ISC)I Security Congress 2021 учасники дискусії відзначили, що людей відкладають, тому що вони вважають, що їм потрібно мати передові технічні здібності, отримані в подальшій освіті.

Такі перешкоди не тільки заважають рівності, але й можуть перешкодити здатності організації захищатися від нападу.

Існує величезна кількість складних проблем, які можуть зловживати зловмисниками. Їм байдуже, як вони отримають доступ до організації — тільки так. Це ультрапрагматичне мислення звільняє їх і надає чистоту фокусу, яка виходить за межі всього. Не обмежені такими факторами, як групова політика, стать, зовнішній вигляд, правила, географія та соціальний статус, вони не хочуть, щоб конкретна людина на цю роботу — вони просто хочуть мати найкращі навички.

Візьмемо, наприклад, темні ринки, де зловмисники шукають членів команди. Вибираючи з анонімного та глобально розподіленого кадрового резерву, людей

оцінюють виключно за здібностями. Якщо хтось із репутацією каже, що ви найкращий розповсюджувач шкідливих програм, фішер або хакер веб-програм, ви отримуєте роботу. Ніяких сертифікатів, жодних чотириетапних співбесід, щоб переконатися, що у вас такий світогляд, як у ваших колег, — лише робота.

Це усуває підсвідоме упередження щодо найму, яке обумовлено колегами на оборонній стороні кібер. Освіта, сертифікати, роки роботи на посаді, спільний досвід: це головоломка, що складається з величезної кількості частин, багато з яких в основному не мають відношення та обмежують талант, який надходить в організації, лише людьми, які відповідають певному «типу».

Спосіб роботи зловмисників, природно, вдихає в їхні ряди більше різноманітності. Якщо єдина необхідна кваліфікація полягає в тому, чи можете ви виконувати цю роботу, географія, економічне походження, стать, раса та нейрорізноманіття не будуть проблемними.

Це забезпечує перевагу. У сфері кібербезпеки, де успіх часто залежить від несподіваних дій, різноманітність думок є цінною зброєю. Якщо захисна команда стандартизована, але група атаки різноманітна, вона має більший пул перспектив, з яких можна опиратися.

Різноманітність як захисна зброя

З цієї причини необхідність залучення нових та різних типів талантів у сфері кібербезпеки є надзвичайно важливою. Він відкриває нові типи мислення, що, у свою чергу, забезпечує навички вирішення проблем, які можуть допомогти відновити конкурентну перевагу.

Різноманітність у захисті — це об’єднання різноманітних точок зору, рішень, досвіду та ідей, які є абсолютно важливими для попередження загроз. Зрештою, для кібербезпеки потрібен такий самий прагматичний підхід, як і зловмисники, який зосереджується на широті навичок і позбавляється довгих списків дорогих сертифікатів та кваліфікацій.

Ми всі по-різному дивимося на речі, що суттєво впливає на те, як ми реагуємо під час кризи. Простіше кажучи, одна людина може не побачити рішення, яке є вражаюче очевидним для іншого. Дослідження показали, що різноманітність має величезне практичне застосування у вирішенні проблем на робочому місці, оскільки приносить до столу безліч різноманітних знань, навичок і суджень. Коли організації мають таку широту знань і мислення в кризових сценаріях, це дає їм перевагу, щоб відбиватися від витончених зловмисників, які складають сучасне середовище загроз.

Пріоритетність навичок під час найму та утримання талантів

Нам потрібно усунути міф про кібербезпеку про те, що кандидати повинні відзначити цілу низку кваліфікацій та сертифікатів, якщо вони сподіваються увійти в галузь або просунутися кар’єрно.

Крім того факту, що сертифікати дуже швидко застарівають через темпи загроз, вони також недоступні для багатьох людей. Це створює штучний бар’єр для входу, який підриває різноманітність у сфері кібербезпеки.

Натомість, чому б не скопіювати хакерів? Наймати на основі вміння виконувати роботу. Поставте кандидатів на тест, щоб розкрити унікальні якості та

можливості вирішення проблем. Те, чи є у них аркуш паперу, не впливає на те, чи зможуть вони помітити вразливу програму на 50 кроках.

Дослідження HBR показують, що підсвідомі упередження лежать в основі багатьох процесів найму, затягуючи неправильних кандидатів у воронки рекрутингу організацій. Це має змінитися, оскільки воно стримує захисні команди, вводячи такий плоский підхід до вирішення проблем, який несе ризик.

Заохочення нових та різноманітних талантів приєднатися та залишитися в цій сфері

Як і для багатьох речей у технологіях, для вирішення проблеми потрібні нові підривні способи мислення. Існує потреба впровадити платформи, фінансування, політику та процеси, які диверсифікують кадровий потенціал у сфері кібербезпеки, відкриваючи його для якомога ширшого кола досвіду.

Розвідка та правоохоронні органи лідирують, прагнучи повернути перевагу від нападників. Те, що почалося з того, що ФБР боролося з питанням, чи наймати хакерів, які курять канабіс у 2014 році, перетворилося на більш формалізовані програми з відкритими обіймами для різноманітності.

Такі організації, як GCHQ, агентство сигнальної розвідки Великобританії, лідирують, активно наймаючи людей із нейрорізноманітністю за їх унікальну здатність виявляти закономірності в даних. Як і в будь-якому випадку в кіберпространстві, те, що починається з розвідувальних служб, має властивість досягти поширення серед тих, хто захищає великі корпорації.

Ті, хто займається кібербезпекою, повинні визнати, що різноманітність – це більше, ніж просто рівність. Йдеться про оптимізацію оборонних можливостей, маючи доступ до якомога ширшого діапазону можливостей вирішення проблем. У просторі, визначеному прагматизмом, це означає отримати фору в ініціативах, які оцінюють і наймають на основі знань, навичок і суджень, а не шматочків паперу». ***(James Hadley. The defensive power of diversity in cybersecurity // Yahoo. (https://techcrunch.com/2021/12/06/the-defensive-power-of-diversity-in-cybersecurity/). 06.12.2021).***

***

«Оскільки 2021 рік наближається до кінця, щорічні прогнози технологічної дослідницької компанії Gartner для професіоналів з кібербезпеки дають деяке уявлення про теми, які можуть почати з'являтися в наступному році. Цьогорічний набір прогнозів щодо кібербезпеки стосується очікуваного зростання законів про конфіденційність та правил щодо програм-вимагачів у всьому світі, змін у структурі корпоративної безпеки та навіть попередження про перше використання операційних технологій, що призводять до людських жертв.

Річні прогнози консалтингової компанії не завжди відповідають 100%, наприклад, применшують поширеність атак нульового дня в наборі прогнозів на сьогоднішній день, які були опубліковані ще в 2017 році. Однак фірма, як правило, має тенденцію бути в курсі загальних тенденцій, передбачаючи збільшення інтересу до таких речей, як автоматизований захист від штучного інтелекту та

інструменти для хмарної видимості (разом із правильною назвою року, коли сталася перша смерть, безпосередньо пов'язана з збоєм у кібербезпеці).

Прогнози щодо кібербезпеки передбачають серйозні зміни в організаційній структурі кібербезпеки

Більшість цьогорічних прогнозів щодо кібербезпеки стосуються того, як будуть виглядати організації в майбутньому, враховуючи нинішні тенденції в ландшафті загроз.

На додаток до тенденцій загроз, ці зміни будуть спричинені дедалі більшим прийняттям правил щодо конфіденційності та безпеки даних у всьому світі. За прогнозами Gartner щодо кібербезпеки, лише за два роки 75% населення світу охоплюються законами про конфіденційність (на національному або державному/місцевому рівні). Gartner фактично збільшує свою довіру до цього прогнозу; минулого року компанія сказала те саме про 2023 рік, але закликала охопити лише 65% світу. На даний момент близько 130 юрисдикцій у всьому світі мають закони про конфіденційність даних. Закон на національному рівні в Сполучених Штатах – це єдина велика проблема, яка залишається, але окремі штати все більше заповнюють цю прогалину, ухвалюючи власні закони; Вірджинія і Колорадо нещодавно ухвалили законопроекти, які набудуть чинності на початку 2023 року.

Ще одна проблема, яка виникла порівняно недавно, яка матиме великий вплив на організаційну IT-структуру в майбутньому, — це зростання віддаленої роботи. Прогнози Gartner щодо кібербезпеки показують, що підприємства та інші організації значною мірою звертаються до сітчастих архітектур, при цьому ці системи зменшують фінансовий вплив атак у середньому на 90%. Ці системи зосереджені на безпеці на рівні пристроїв, надаючи кожній власний стандартизований набір засобів захисту для швидкого та надійного захисту пристроїв співробітників, які в іншому випадку непередбачувані, що використовуються за межами офісу. Вони також є ключовим елементом тенденції «архітектури нульової довіри», що навіть уряд США прийняв і очікує запровадити для федеральних агенцій до 2024 року.

Прогнози щодо кібербезпеки також показують, що організації мають тенденцію до «безпеки як послуги», але шукають, щоб усі ці різноманітні послуги надавалися одним постачальником. Gartner вважає, що до 2024 року 30% підприємств приймуть підхід безпеки, орієнтований на хмару, шукаючи надійних постачальників, які зможуть об'єднати купу різних інструментів в один спрощений пакет: Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Серед основних цікавих можливостей доступ до мережі з нульовою довірою (ZTNA) і брандмауер як послуга (FWaaS).

Ризик кібербезпеки також стане вирішальним фактором у тому, з ким організації вирішать вести бізнес, принаймні, згідно з Gartner. У прогнозах щодо кібербезпеки вирішальним фактором у цій сфері для 60% компаній є положення безпеки потенційного партнера (або цілі придбання).

Директори та ради директорів також будуть робити речі трохи інакше. До 2025 року Gartner бачить, що 40% рад матиме спеціальний комітет з кібербезпеки, який контролює кваліфікований член правління. Крім того, 70% керівників

зобов'язуватимуть культуру організаційної стійкості для подолання випадкових загроз кіберзлочинності, а також інших серйозних ризиків шкоди (наприклад, стихійних лих і громадянських заворушень).

Посилені заходи щодо платежів із програмним забезпеченням-вимагачем

Хоча на даний момент позиція більшості світових урядів полягає в тому, щоб дозволити компаніям здійснювати платежі з програмним забезпеченням-вимагачем, якщо вони визнають, що це відповідає їхнім інтересам, це може швидко змінитися протягом наступних чотирьох років. Згідно з прогнозами Gartner щодо кібербезпеки, до кінця 2025 року 30% країн приймуть закони, які жорстко регулюють виплати програм-вимагачів; це буде менше ніж на 1% на даний момент. Частково це може бути викликано очікуваною нездатністю регулювати криптовалюту, оскільки вона залишається життєздатним способом для злочинців отримувати платежі від жертв.

Оперативна техніка з використанням зброї може призвести до людських жертв

Найбільш похмурий запис у прогнозах кібербезпеки на 2021 рік полягає в тому, що перші людські жертви від злому операційних технологічних систем будуть помітні до 2025 року. Gartner був точний у своєму попередньому прогнозі такого характеру, який сказав, що перший збій кібербезпеки закінчився смертельним результатом відбудеться до 2020 року; саме це сталося в Німеччині того року, коли компрометація систем лікарні призвела до смерті пацієнта невідкладної допомоги, якого довелося перенаправити до іншого закладу.

Це слідує за прогнозом міністра внутрішньої безпеки США про те, що «програмне забезпечення» незабаром стане головною загрозою кібербезпеці. Це шкідливе програмне забезпечення буде зосереджено на проникненні в промислові підприємства, медичні установи та комунальні підприємства. Якщо це стане тенденцією хакерства, Gartner бачить, що генеральні директори та керівники несуть персональну відповідальність і відповідальність за шкоду». ***(SCOTT IKEDA. Cybersecurity Predictions for 2025: Mesh Architectures, Ransomware Regulations and the Specter of Human Casualties // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cybersecurity-predictions-for-2025-mesh-architectures-ransomware-regulations-and-the-specter-of-human-casualties/). 24.12.2021).***

***

«Незважаючи на зростання обізнаності про кібербезпеку, багато міфів про неї поширені. Ці хибні уявлення можуть стати перешкодою для ефективної безпеки.

Перший крок до забезпечення безпеки вашого бізнесу — відокремити неправдиву інформацію, міфи та чутки від правди.

Тут ми розбиваємо деякі поширені міфи про кібербезпеку. Прочитайте далі, щоб дізнатися, що з наведеного нижче, на вашу думку, є правдою.

Міфи кібербезпеки проти правди

Міф №1 — Занадто велика безпека знижує продуктивність

Існує поширена думка, що підвищена безпека ускладнює доступ до того, що їм потрібно, навіть для співробітників, а не тільки для хакерів. Вважається, що суворі політики безпеки, такі як регулярний моніторинг і контроль доступу, заважають продуктивності на роботі. Однак відмова від безпеки може мати далекосяжні наслідки для вашого бізнесу. Успішна атака, як-от DDoS-атака або програмне забезпечення-вимагач, може зупинити ваш бізнес. Співробітники можуть не мати доступу до важливих файлів, мереж та інформації після атаки. Відновлення займає дні, а іноді навіть тижні.

Правда: Посилена кібербезпека може підвищити продуктивність.

Сучасний підхід до кібербезпеки використовує засоби безпеки, які мають вбудовану функцію безпеки, яка легко інтегрується у вашу систему. Він також використовує передові технологічні розвідки та аналітику для виявлення в реальному часі та пом'якшення загроз. Це дозволяє розробникам зосередитися на підвищенні продуктивності, оскільки їм більше не потрібно турбуватися про проблеми безпеки.

Міф №2. Кібератаки спричиняються лише зовнішніми загрозами

Внутрішні загрози зростають і швидко стають причиною занепокоєння бізнесу. Внутрішні загрози можуть включати співробітників, постачальників, підрядників, ділових партнерів або зовнішнього зловмисника, який намагається видати себе за співробітника. Недавнє дослідження показало, що інсайдерські загрози несуть відповідальність за 60% від даних порушень.

Крім того, ви ніколи не можете повністю знати, звідки можуть виникнути ці атаки, а традиційні рішення безпеки є значною мірою неефективними, коли справа доходить до цих загроз. Це робить їх набагато важче виявити та стримати, ніж зовнішні загрози.

Правда: Тому кібератаки цілком можуть початися з когось, кого ви знаєте.

Використовуйте комбінацію поведінкової аналітики та керування привілеями та доступом, щоб мінімізувати внутрішні загрози. Крім того, проводьте тренінги з підвищення обізнаності з безпеки, щоб розповісти співробітникам про небезпеку внутрішніх загроз і способи їх виявлення.

Міф №3 — кіберзлочинці атакують лише великий бізнес

У малого та середнього бізнесу часто складається помилкове враження, що їхні дані не є цінними для хакерів. Проте малий і середній бізнес є однією з головних мішеней для хакерів.

Недавнє дослідження показало, що хакери цільових малого бізнесу майже половину часу. Але лише 14% цих підприємств були готові захищатися в такій ситуації.

Правда: жоден бізнес, який би великий чи малий, не застрахований від спроб злому та зловмисних атак.

Хакери не дискримінують, коли йдеться про їхніх жертв. Тому не дозволяйте розміру вашого бізнесу визначати, наскільки цінними є ваші дані або наскільки безпечними є ваші активи.

Міф №4. Антивірусного або антивірусного програмного забезпечення достатньо, щоб захистити мій бізнес

Антивірусне програмне забезпечення є важливою частиною вашого плану кібербезпеки. Однак це забезпечує лише одну точку входу у вашу систему. Хакери мають багато способів обійти антивірусне програмне забезпечення та проникнути в мережі за допомогою таких атак, як цілеспрямовані фішингові атаки та програми-вимагачі.

Таким чином, навіть за наявності програмного забезпечення для захисту від шкідливих програм у хакерів буде достатньо місця для атаки.

Правда: антивірусне програмне забезпечення може захистити вас лише від унікального набору визнаних кіберзагроз, а не від інших нових кіберзагроз.

Як бізнесу, вам потрібно зробити набагато більше, щоб захистити свої дані від хакерів. Розгорніть всеосяжне рішення безпеки, як-от брандмауер веб-додатків, який безперервно відстежує загрози та забезпечує цілодобовий захист від кіберризиків.

Міф № 5 — Кібербезпека надто дорога

Незважаючи на те, що зловмисні кібератаки продовжують потрапляти в заголовки газет і коштують бізнесу мільйони, компанії все ще задаються питанням, чи варті інвестиції в кібербезпеку. Безпека даних часто ігнорується, і для багатьох підприємств це лише позачергова думка. Середня вартість злому даних у 2021 році становить 4,24 мільйона доларів, що є найвищим показником за останні 17 років. І ця цифра не включає збиток, який спричиняє серйозні втрати репутації та втрати клієнтів від порушення.

Правда: вартість хорошого рішення кібербезпеки ніщо в порівнянні з вартістю успішної атаки.

Інвестуйте в сучасне рішення безпеки, як-от Indusface AppTrana, наприклад, яке може захистити вас від останніх загроз. Крім того, існує багато запобіжних заходів, які ви можете вжити абсолютно без додаткових витрат для вашого бізнесу, наприклад, надійні паролі, багатофакторна аутентифікація, керування доступом та навчання співробітників.

Міф №6 — Вам не потрібна кібербезпека, тому що на вас ніколи не нападали

Якщо ви ніколи не стикалися з кібератакою або зломом даних, велика ймовірність, що ви не знаєте, скільки шкоди вони можуть завдати. Ви також можете припустити, що ваша поточна позиція безпеки досить сильна, щоб утримати поганих акторів подалі, оскільки на вас ніколи не нападали.

Однак кіберзагрози та інструменти злому постійно розвиваються, стаючи з кожним днем все більш складними та невиявленими. І будь-які конфіденційні дані є потенційною мішенню для порушення.

Правда: ви можете легко стати наступною ціллю.

Розробіть надійну стратегію безпеки, яка допоможе вам виявити наявні слабкі місця та пом’якшити спроби атаки до того, як буде завдано будь-якої значної шкоди.

Міф №7 — Ви досягли повної кібербезпеки

Кібербезпека – це безперервний процес, який необхідно вдосконалювати разом зі змінами в ландшафті загроз. Тому ніколи не припиняйте працювати над захистом своїх ІТ-активів. Ваша організація завжди буде вразливою до існуючих і нових загроз.

Правда: не існує такого поняття, як повна чи ідеальна кібербезпека від кібератак.

Періодично переглядайте свою політику безпеки, проводьте аудит безпеки, постійно відстежуйте свої критичні активи та інвестуйте в майбутні оновлення заходів безпеки…» ***(Top 7 common Cybersecurity Myths — Busted // The Hacker News (https://thehackernews.com/2021/12/top-7-common-cybersecurity-myths-busted.html). 21.12.2021).***

***

«Після чергового важкого року в окопах кібербезпеки професіонали з безпеки заслуговують на заслужений відпочинок, а також на кілька потужних подарунків, які допоможуть їм впоратися з новорічним ландшафтом загроз і викликами безпеки, які прийдуть.

Ось наш короткий огляд того, чого бажають професіонали з кібербезпеки в цей святковий сезон.

1. Великий виклик етичного хакерського інструменту штучного інтелекту

Кібербезпека є пріоритетом національної безпеки, і лише за останній рік зловмисники атакували державні установи, комунальні підприємства, школи, лікарні та підприємства. Маючи це на увазі, професіонали з кібербезпеки хотіли б, щоб військовий Санта-Клаус — інакше відомий як DARPA (Агентство передових оборонних дослідницьких проектів) — фінансував великий доларовий конкурс Grand Challenge для компаній або університетів на розробку симуляторів «Мама всіх етичних хакерських симуляторів».

Це повинно працювати так: система створить детальну симуляцію всієї мережі організації, включаючи сторонні хмарні сервіси, пристрої користувачів — усе. Потім суперкомп'ютерна система машинного навчання-монстра кидатиметься на неї всіма відомими атаками, що призведе до списку вразливостей і політик, які потрібно виправити на основі найкращих методів кібербезпеки.

І оскільки це список бажань, доступ до цього інструменту кібербезпеки має бути безкоштовним для всіх уповноважених спеціалістів із кібербезпеки. Щось подібне було б неоціненним для всієї галузі, особливо для невеликих організацій, які не мають ресурсів для самостійного проведення моделювання або тестів на проникнення.

2. Нова правова база для припинення атак програм-вимагачів

Одним з найгірших аспектів програм-вимагачів є те, що його жертви платять за те, щоб вони продовжували працювати. Організації часто відчувають, що у них немає іншого вибору, окрім як платити зловмисникам за відновлення доступу до своєї інформації або систем, і саме ці фінансові платежі стимулюють зловмисників продовжувати свої злочини. Ефективне юридичне рішення для цільових організацій допомогло б розірвати це коло, тому не дивно, що це загальне бажання професіоналів у сфері кібербезпеки.

Одним із способів, за допомогою якого країна може зменшити атаки програм-викупів на компанії в межах своїх кордонів, є заборона сплати викупу. Проблемою цієї ідеї є катастрофічні наслідки для організацій, які не платять.

Натомість уявіть собі законодавчу базу, яка забороняє сплату викупу, водночас компенсуючи кожній організації 100% витрат, спричинених несплатою. Це могло б функціонувати подібно до кіберстрахування в національному масштабі, не вкладаючи гроші в кишені поганих акторів.

Цей удар один-два знищив би стимул до атак програм-вимагачів, тому що зловмисники знали, що їм не платять, а цільові організації не зазнають катастрофічних фінансових втрат від блокування або розкриття даних. Це була б мрія професіоналів з кібербезпеки.

3. Ноутбук, розроблений з нуля для безпеки віддаленої роботи

Виробники пристроїв повинні визнати реальність нашого часу, розробивши ноутбук для віддалених працівників, який забезпечує безпеку в першу чергу, дотримуючись найкращих практик і порад експертів з кібербезпеки. Ноутбук має бути побудований на основі концепції нульової довіри, згідно з якою співробітники не можуть отримати доступ до ресурсів компанії, за винятком захищеного ноутбука, який вимагає біометричного сканування або інших облікових даних для доступу до кожного ресурсу. Він також повинен радикально ізолювати всі процеси та мати вбудовані засоби захисту для найпоширеніших кібератак, які залучають пристрої кінцевих користувачів.

4. Радикально диверсифікований ланцюг поставок для електроніки

Причині оптимальної кібербезпеки значною мірою шкодять як кібератаки ланцюга поставок, так і уповільнення ланцюга поставок для електроніки всіх видів. Обидві ці проблеми є результатом відсутності різноманітності та розподілу ланцюгів поставок. В результаті компанії та окремі особи намагаються належним чином оновити своє обладнання, залишаючись на неоптимальних і погано працюючих пристроях довше, ніж вони повинні.

Завдяки диверсифікації кібератаки на одного постачальника можуть бути припинені, переключившись на іншого, поки атака спрямована на першого. Наскільки це можливо, електронні компоненти повинні виготовлятися та збиратися в більшій кількості місць, ніж вони є зараз, щоб зменшити критичні вразливості та збої, як ми бачили в 2021 році.

5. Повне прийняття моделі нульової довіри

Одним з найбільших подарунків, які світ міг би надати професіоналам з кібербезпеки, є повна й універсальна підтримка моделі нульової довіри. Виходьте зі старою моделлю периметра раз і назавжди, а потім з новою.

Як і у випадку з багатьма побажаннями в цьому списку, це буде серйозною зміною, але це принесе дивіденди в усьому світі кібербезпеки, зменшуючи витрати та час простою для підприємств, державних установ і фізичних осіб. Менше успішних кібератак корисно для всіх, а повне прийняття нульової довіри було б важливим кроком у правильному напрямку.

6. Масове фінансування підтримки освіти з питань кібербезпеки в університетах

Промислові, урядові та військові організації виграють від припинення розриву в навичках кібербезпеки. Настав час усім залучитися, щоб надати стипендії, гранти, програми ранньої освіти, інформаційно-пропагандистські заходи

та інші ініціативи, щоб збільшити кількість студентів, випускників і, зрештою, спеціалістів у сфері кібербезпеки.

Настав час мріяти про кращий світ. А для фахівців із кібербезпеки світ стане набагато кращим завдяки внеску всього суспільства у справу кращого ландшафту кібербезпеки, що принесе користь організаціям усіх форм і розмірів». ***(Mike Elgan. What Cybersecurity Professionals Are Wishing for This Holiday Season // IBM (https://securityintelligence.com/articles/cybersecurity-professional-2021-holiday-wishlist/). 21.12.2021).***

***

«Організаціям потрібен захист від кібербезпеки, щоб запобігти атакам і рішення швидкого відновлення

Підприємства повинні виконувати всі можливі завдання та необхідні для зміцнення цифрового захисту в кіберсвіті, що постійно змінюється. Загрози постійно розвиваються, щодня з'являються нові. Необхідно постійно переоцінювати свої підходи і налаштовуватися на злісну поведінку. Динамічна природа поточної цифрової активності ускладнює виконання ваших заходів кібербезпеки, що може дати організаціям відчуття, що вони завжди на обороні, коли справа доходить до безпеки. Більшість кіберзагроз компаній надходять від інсайдерів.

Інсайдери — це співробітники, постачальники, підрядники та постачальники, які мають доступ до внутрішніх систем компанії. Інсайдерські загрози стосуються будь-якої можливої шкоди, заподіяної інсайдерами. Ці користувачі мають доступ до конфіденційних даних та приватної інформації, оскільки вони є інсайдерами. Ці дані можуть включати важливу інтелектуальну власність, комерційну таємницю, інформацію про клієнтів і співробітників тощо. Загрози з боку інсайдерів є в кожній компанії. Згідно з опитуванням, проведеним Ernst & Young та IBM, індустрія фінансових послуг має 74 відсотки сприйманого ризику кіберзлому та зловмисних інсайдерів.

Запобігання загрозам призначене для зняття стресу від кіберзагроз, що постійно змінюються, і допомоги організаціям у підтримці кібербезпеки. Запобігання загрозам відноситься до інструментів, які виконують дії щодо виявлення загроз і запобігання, наприклад виявлення кінцевих точок і реагування на них, а також політики та плани кібербезпеки, які визначають пріоритетність запобіжних заходів.

Чому важливо запобігти загрозам, ніж одужати?

Розвитку організаційної стійкості сприяє уникнення загроз. Ці методи можуть допомогти підприємствам залишатися попереду кіберзагроз, підтримуючи свої технології, персонал і процеси в актуальному стані, щоб вони могли швидко реагувати на мінливі ситуації. «Профілактика краще, ніж лікування», – вважаємо ми. Хоча організації можуть досягти тієї ж мети – відновлення та повернення до нормальної діяльності, метод «лікування» передбачає значно більше жертв. Протягом періоду відновлення після атаки організації можуть втратити клієнтів і бізнес, що призведе до значно більших витрат з точки зору доходу, репутації та

продуктивності, не кажучи вже про негайні витрати на відновлення будь-яких даних або втрати активів.

Існує кілька доступних профілактичних рішень і послуг, зокрема захист від шкідливих програм, хмарна безпека, захист електронної пошти, безпека кінцевих точок тощо. Метою цих предметів є запобігання нападам. На жаль, усім їм важко запобігти. Немає жодного провайдера, який може гарантувати повну безпеку від кібератак. Навіть фірми, які використовують усі продукти зі списку вище, є вразливими.

Хоча ми не можемо уникнути всіх атак, ми можемо зупинити деякі з них. Ми можемо відчувати полегшення, коли напад можна уникнути за допомогою профілактичного засобу, але ми не повинні бути надмірно самовпевненими. Більшість із нас бачили попереджувальну табличку на боковому дзеркалі автомобіля, яка говорить: «Предмети в дзеркалі ближче, ніж виглядають». Охоронні товари можуть забезпечити рівень безпеки, який є недосяжним. Кібератаки постійно залишаються лише за подих, чекаючи, щоб подолати оборону.

В першу чергу, це має вирішальне значення для розгортання високої якості кібербезпеки системи і політики кібербезпеки. Splunk та інші складні рішення, запропоновані фахівцями, служать вашою найсильнішою лінією захисту від загроз, дозволяючи організаціям бути проактивними, а не реагувати. Сучасні інструменти, такі як User and Entity Behavior Analytics (UEBA), спеціально розроблені, щоб допомогти в ранньому виявленні та пом’якшенні атак із внутрішньої загрози.

Наступний крок, який може зробити будь-яка компанія, щоб удосконалити свої превентивні стратегії, — це постійний моніторинг та перегляд поточної кіберінфраструктури. Щоб уникнути утворення дір у безпеці, переконайтеся, що ваш план кібербезпеки ефективно підтримується та оновлюється.

Підприємствам слід постійно контролювати та тестувати якість своїх інструментів, процесів і налаштувань, щоб переконатися, що все працює з максимальною продуктивністю. Це не тільки дозволяє організаціям оцінити, як працюють їхні інструменти, але також дозволяє їм усунути недоліки та запобігти потенційним нападам.

Усі рішення для блокування кібербезпеки перевіряють наявність шкідливих програм. Не має значення, чи це підозріла діяльність, файл, виконуваний код чи сценарій. Вони шукають позитивну або шкідливу поведінку. Вони не можуть зупинити шкідливу поведінку, якщо не знають про це. А погані актори завжди змінюють свою діяльність, стратегію, програмне забезпечення тощо.

Розважливо мати стратегію та рішення негайного відновлення до того, як станеться порушення. Крім профілактики, важливо мати додатковий рівень захисту.

Організації можуть використовувати миттєве відновлення для активного захисту та захисту своїх даних. Коли напад проходить за межі рішень для блокування, захист важливих даних зупиняє загрозу від впливу на неї. Організації можуть відновити цифрову інформацію та пристрої до стану перед атакою зі швидким відновленням». ***(Aishwarya Banik. WHY IS PREVENTION BETTER THAN RECOVERY IN CYBERSECURITY? // Stravium Intelligence LLP***

(https://www.analyticsinsight.net/why-is-prevention-better-than-recovery-in-cybersecurity/). 06.12.2021).

***

«Деякий відчутний прогрес був досягнутий останніми роками в галузі освіти співробітників з безпеки, але деякі аналітики вважають, що проблема є нерозв'язною та постійною на певному рівні. Останній захід «Gone Phishin'», щорічний тест на фішинг, який проводить канадська організація Terranova Security, додає більше підтримки цьому погляду.

Близько 20% несвідомих піддослідних були скомпрометовані імітованим фішинговим електронним листом; Майже 15% не розпізнали шкідливий сайт для завантаження після натискання і почали завантаження зіпсованого файлу. Великі організації або ті, від яких слід очікувати, що мають більш надійні програми навчання з безпеки, як правило, йдуть найгірше.

Фішинговий тест має 19,8% компромісу електронної пошти; 14,4% кліків через шкідливі завантаження

Terranova щороку проводить «Турнір з фішингу» в рамках свого щорічного глобального звіту з показників фішингу, дослідження, яке вивчає безпеку тисяч організацій у 98 різних країнах (розсилаючи близько мільйона імітованих фішингових листів 20 різними мовами).

Тест на фішинг у 2021 році показує трохи відступу від 2020 року; кількість одержувачів, обдурених шкідливим електронним листом, залишилася приблизно незмінною, але спостерігалося помітне збільшення бажання завантажувати файли з схематичних імітованих веб-сайтів атак серед тих, хто переходив за посиланнями.

19,8% одержувачів, які натиснули посилання на електронну пошту фішингового тесту, не обов’язково були б скомпрометовані, але 14,4% одержувачів, які продовжили звідти, завантажили б шкідливе програмне забезпечення в аналогічній реальній атаці. Таким чином, результати дослідження показують, що понад 70% співробітників, яких обдурили початкове фішингове посилання, не зможуть визначити сайт, на який вони пов’язані, як загрозу безпеці, і можна очікувати, що вони встановлять зловмисне програмне забезпечення.

Були відзначені деякі регіональні відмінності, але більшість з них залишалася на рівні від 10% до 15% співробітників, обдурених, завантажуючи шкідливе програмне забезпечення. Північноамериканські організації показали найкращі результати в тесті на фішинг, за ними слідувала Європа; найгірше склався регіон Азіатсько-Тихоокеанського регіону. Але хоча Північна Америка була найбільш обережною в сукупності, розбивка за країнами показала деякі подібні відмінності. Учасники зі Сполучених Штатів показали дуже хороші результати з 8,7% кліків і 40,9% кліків для завантаження, тоді як їхні сусіди на півночі в Канаді, швидше за все, були обдурені з 14,1% кліків і 59,8% кліків. - швидкість завантаження.

Були більш різкі відмінності в залежності від організації та типу одержувача. На диво, працівники інформаційних технологій мали найвищий рівень проходження і завантаження імітованого файлу зловмисного програмного забезпечення (84% тих, хто натиснув початкове фішингове посилання). IT також були одними з найпопулярніших секторів для початкових кліків разом із

фінансами, освітою та страхуванням. Роздрібна торгівля, охорона здоров'я та транспорт мали значно нижчі показники, ніж інші галузі.

Тест використовує автентичні шаблони електронної пошти, надані Microsoft

Щоб бути справедливими до учасників, вони отримали реалістичні електронні листи (сформовані командою безпеки Microsoft за допомогою інтерфейсу компанії SharePoint), які б правдоподібно відображали те, що вони могли очікувати отримати в повсякденній роботі. Особлива увага приділялася створенню повідомлень, які не були «загальними», як-от фіктивні пропозиції безкоштовних подарункових карток, які зазвичай зустрічаються в папках зі спамом і як відповіді на публікації в соціальних мережах.

Організації зголосилися пройти тест на фішинг, але окремі співробітники, можливо, не знали, що надходить імітований електронний лист. Захід завжди проводиться в жовтні в рамках Національного місяця інформування про кібербезпеку.

Хоча цьогорічний фішинговий тест був зосереджений на тому, щоб переконати ціль відвідати сайт атаки та завантажити файл, у версії 2020 року виміряли їхню готовність ввести своє ім'я користувача та пароль, коли буде запропоновано. У цьому тесті близько 20% переходили за посиланнями і 13% надсилали паролі, при цьому близько 66% тих, хто натискав, продовжували відмовитися від своїх облікових даних для входу.

Чи працює навчання з фішингу?

Корпоративне навчання з фішингу стало спірною темою, і експерти різко розділилися між тим, хто бачить у ньому необхідність, і тими, хто бачить у ньому лише незначні покращення в проблемі, яка закорінена в людській природі.

Існує цілий ряд фішингових тестів, які показують різні результати, від того, що демонструє цей конкретний тест (майже неминучий рівень компромісу десь близько 15-20%) до деяких, які показали зниження до 3% більше. час. Незалежно від того, яку сторону ви берете в дискусії, одна річ, яка, здається, зрозуміла на даному етапі, полягає в тому, що навчання з фішингу дає лише тимчасовий приріст приблизно на кілька місяців, перш ніж співробітники, які схильні до поганих звичок гігієни безпеки, повернуться до них.

Зрештою, відсоток цих фішингових тестів може не мати значення; потрібно всього лише одного скомпрометованого працівника, щоб створити проріз у мережі, що призводить до встановлення програм-вимагачів або крадіжки конфіденційної інформації. Таким чином, деякі експерти з безпеки дотримуються позиції, що єдиний правильний підхід — запобігти потраплянню фішингових листів до вхідних поштових скриньок співробітників, можливо, за допомогою рішення для фільтрації на основі штучного інтелекту». ***(Scott Ikeda. One in Five Employees Fail the Gone Phishin' Test as Security Hygiene Remains a Chronic Problem // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/one-in-five-employees-fail-the-gone-phishin-test-as-security-hygiene-remains-a-chronic-problem/). 17.12.2021).***

***

«Кібербезпека швидко стала головною проблемою для виробників і промислових послуг у всьому світі. Згідно з опитуванням керівників виробничих компаній у вересні 2021 року, 61 відсоток визначили кібербезпеку як «високий/дуже пріоритет».

Ці проблеми особливо помітні, коли виробники звертаються до віддалених і гібридних команд, щоб залучити та утримати найкращі таланти, зберігаючи безперервність роботи.

В результаті виробники впроваджують потужність віддаленого управління для систем ОТ, що дозволяє співробітникам, підрядникам і довіреним третім сторонам керувати інфраструктурою на місці з будь-якої точки світу. Хоча переваги багатогранні, ризики для критичних систем реальні. Працівники, що працюють за межами сайту, частіше ставлять під загрозу цілісність ОТ, оскільки все, від фішингового шахрайства до відволікань, підриває ініціативи з кібербезпеки.

На жаль, багато організацій не мають належного захисту контролю доступу. Багато виробничих організацій все ще покладаються на застарілі системи контролю для своїх критичних операцій. У той же час, в одному галузевому звіті було виявлено, що майже половина організацій не можуть визначити порушення, а 25 відсотків не перевіряли свої методи кібербезпеки за останній рік.

Виробники повинні якнайшвидше оцінити методи кібербезпеки та усунути операційні ризики для своїх критичних активів ОТ. Для керівників C-suite, менеджерів із кібербезпеки та інших осіб, які приймають рішення, ось три найкращі методи покращення безпеки ОТ в цей трансформаційний час.

#1 Підготуйте гібридних працівників

Оскільки виробники розширюють віддалені операції, вони потенційно вносять нові вразливості в активи ОТ.

За межами сайту працівники часто використовують ноутбуки та планшети компанії для використання, що може мимоволі відкрити вектор атаки для доступу до активів ОТ, особливо якщо протоколи даних не ізольовані від мережі ОТ. Крім того, обмежені бюджети та недостатня підготовка користувачів можуть підірвати пріоритети кібербезпеки.

Одне дослідження показало, що 61 відсоток учасників не змогли пройти базову вікторину з кібербезпеки, що підкреслює необхідність виробників враховувати реалії гібридної роботи.

Іншими словами, кібербезпека починається з підготовки гібридних команд до моменту. Хоча це обов’язково виглядатиме по-різному для кожної організації, виробники повинні переконатися, що їхні команди можуть:

дотримуйтесь найкращих практик цифрової гігієни

визначити реагування на мінливі тенденції загроз

отримувати безпечний і надійний доступ до цифрових активів.

Гібридні співробітники представляють значну вразливість у сфері кібербезпеки, але їх можна перетворити на актив при належній підготовці.

#2 Впроваджуйте специфічні для ОТ рішення з кібербезпеки

Оскільки виробники переходять на гібридну робочу силу, у багатьох виникне спокуса використовувати інструменти автентифікації та контролю доступу

існуючої IT-інфраструктури та скопіювати їх, щоб захистити активи OT. Суб'єкти загроз добре знають, що ці технології вимагають відданих спеціалістів із кібербезпеки для виявлення вразливостей, виявлення загроз і керування ними. Оскільки ці ресурси корпоративної кібербезпеки рідко доступні для моніторингу систем OT, використання вразливостей в системах OT з часом буде зростати з потенційно руйнівними наслідками.

Ось чому виробники повинні використовувати прості специфічні для OT рішення для контролю доступу, включно з детальним контролем ролей і авторизацією на основі часу, які відстежують доступ співробітників, підрядників і третіх сторін до активів OT.

Найголовніше, виробники повинні звернутися до архітектури кібербезпеки з нульовою довірою, яка включає:

Багатофакторна аутентифікація на основі маркерів HW

Протокольна ізоляція

Опосередкована односпрямована безпечна передача файлів

Модерований «лобі очікування» для доступу користувачів до активів

Моніторинг з'єднання між користувачем і активом

Повний журнал доступу користувачів і запис сеансу.

Операційні можливості OT супроводжуються унікальними ризиками кібербезпеки, які вимагають специфічних рішень OT. Впроваджуючи ці рішення, виробники мають можливість радикально знизити ризики для своєї діяльності, а також підвищити операційну ефективність.

 # 3 Перейдіть до автоматизації

Залучити та утримати найкращих спеціалістів із кібербезпеки зараз надзвичайно складно. У США є понад 465 000 незаповнених робочих місць у сфері кібербезпеки. Між тим, вигорання та виснаження є ендемічними серед персоналу з кібербезпеки, що означає, що навіть найнятий талант може бути менш ефективним для захисту цифрового ландшафту компанії.

Технології автоматизації можуть допомогти зменшити навантаження на захист активів OT. Наприклад, сучасні інструменти управління загрозами, інтегровані з контролем доступу, а також відстежують і ефективно керують доступом до критичних активів OT на основі профілю ризику.

Забезпечення OT розширює можливості гібридних команд

Гібридна робота залишиться тут. Як повідомляє Всесвітній економічний форум, «промислові компанії, які вживають сміливих дій, щоб підтримати свою робочу силу та інвестиції в технології, стануть більш стійкими і з більшою ймовірністю досягнуть успіху, незалежно від того, які невизначеності трапляються на їхньому шляху».

Однак конвергенція IT та OT може надати суб’єктам загроз доступ до мереж OT, тому виробникам потрібно оновити свою оборонну позицію, щоб врахувати ці мінливі ризики. Ті, хто швидко адаптується, мають найкраще положення для забезпечення безпечного, безпечного та ефективного робочого середовища». ***(Bill Moore. Critical Infrastructure Is Under Attack: How Industry Can Secure OT Remote Operations Before It’s Too Late // Rezonen Pte. Ltd.***

(https://www.cpomagazine.com/cyber-security/critical-infrastructure-is-under-attack-how-industry-can-secure-ot-remote-operations-before-its-too-late/). 22.12.2021).

***

«Здається, що лідери в галузі кібербезпеки не можуть зупинитися, коли справа доходить до мережевих і хмарних ризиків. Під час розробки захисного підручника слід враховувати групу програм-вимагачів як послугу (RaaS), інсайдерські загрози, фішинг і численні загрози. Будь то інцидент із програмним забезпеченням-вимагачем JBS Foods, атака Colonial Pipeline чи російські хакери, які атакували міністерство фінансів та міністерство торгівлі США у 2020 році, зрозуміло, що кожна агенція та організація критичної інфраструктури повинні пам'ятати про вразливості — як відомі, так і невідомі — які можуть потенційно вплинути на конфіденційну інформацію.

Наслідки федеральної кібератаки

У звіті Thales Data Threat Report за 2021 рік 84% державних службовців США висловили занепокоєння з приводу збільшення кіберризиків і загроз, пов'язаних із співробітниками, які працюють віддалено. Респонденти вказали, що основним занепокоєнням є зниження рівня обережності віддалених працівників, а також відсутність довіри до своїх нинішніх систем безпеки. Оскільки існує пропозиція, щоб федеральні працівники були віддалені, існують додаткові ризики, про які слід пам'ятати, коли справа доходить до переміщення вмісту вгору по секретному каналу.

Крім ризику розкриття критичної інформації, можуть бути юридичні наслідки для жертв кібератак. Комісія з цінних паперів і бірж і Комісія з торгівлі товарними ф'ючерсами вказали, що може знадобитися додаткова звітність залежно від обставин атаки та типу даних, які було вилучено. Компанії та агенції також повинні повідомляти про інциденти відповідно до законів про порушення державного законодавства та клієнтів, які використовують їхні системи.

Вплив шкідливих програм на файли

Щойно зловмисне програмне забезпечення потрапляє в мережу через слабку точку, може розпочатися бічне переміщення. Під час складної атаки зловмисник намагатиметься пройти через організацію, непомітно, щоб заразити ширший діапазон пристроїв і файлів і зібрати якомога більше інформації. Коли документи потрапляють в державні системи в несекретному місці, вони доступні для широкої групи людей, а потім, як тільки вони переходять на рівень класифікації — конфіденційний, секретний або абсолютно секретний — до них все ще може бути приєднане шкідливе програмне забезпечення.

«Секретно» означає інформацію, яка з міркувань національної безпеки спеціально призначена урядовою установою Сполучених Штатів для обмеженого або обмеженого поширення чи розповсюдження. Коли ви отримуєте документи від низького до високого рівня конфіденційності, на кону стоїть не тільки конфіденційність. Якщо файли, які раніше не були секретними, містили в собі віруси, це могло б дозволити цифровим супротивникам проникнути до надсекретних мереж і навіть викрасти торговельні та зовнішньополітичні секрети

чи військову тактику, що може поставити під загрозу життя мільйонів людей і значущі дані.

SolarWinds, одна з найбільш сумнозвісних кібератак в історії, зазнала наслідків поширення зламаного коду в пропозиції, яка була надіслана тисячам підприємств і державних установ. Хакери, відповідальні за атаку, мали безперебійний доступ до департаментів Пентагону, внутрішньої безпеки, штату тощо протягом 14 місяців, перш ніж їх виявили. Завдяки безперешкодному доступу до секретної інформації протягом такого тривалого часу неможливо визначити справжній розмір збитку та потенційні секрети, які розкриваються.

Повинні існувати проактивні системи для захисту цих даних з наслідками для національної безпеки, оскільки вони проходять через цикл конфіденційності — зокрема, обов'язкові фільтри для забезпечення очищення файлів.

Дезінфекція файлів протягом усього циклу конфіденційності

Оборонні агенції повинні застосовувати проактивний підхід до безпеки файлів, і один з найефективніших способів зробити це – використовувати технологію Content Disarm and Reconstruction (CDR), яка миттєво очищає та відновлює файли відповідно до специфікацій відомого хорошого виробника – автоматично видаляючи потенційні загрози. Завдяки витонченості нової ери кібератак реактивна стратегія більше не може встигати з потенційними небезпеками, з якими стикаються. Це ставить користувачів і файли під загрозу, порушуючи продуктивність бізнесу та додаючи стресу для і без того зайнятих і недостатньо укомплектованих команд безпеки.

CDR не тільки використовує кібербезпеку як проактивний підхід, але й усуває сліпі плями та вразливості, на які можуть проникнути хакери. У випадку з конфіденційними урядовими документами це допомагає усунути будь-які лазівки та дає змогу керівникам наших урядів зосередитися на інших важливих завданнях, таких як стратегія та прийняття рішень…». ***(Sam Hutton. Defense Cybersecurity: How Changing Classified Document Status Can Unknowingly Affect Risk Levels // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/defense-cybersecurity-how-changing-classified-document-status-can-unknowingly-affect-risk-levels/).10.12.2021).***

***

«Оскільки пандемія впливає на організації всюди, можна з упевненістю сказати, що більшість компаній повинні працювати ще більше, щоб розширити свою клієнтську базу, прискорити цикли продажів і збільшити прибуток, щоб повернутися на правильний шлях. На жаль, багато постачальників (також відомих як треті сторони) стикаються з непередбаченими перешкодами при продажу нових продуктів і послуг. Це тому, що клієнти повинні оцінити ризики кібербезпеки, пов'язані з роботою з новим постачальником, щоб переконатися, що вони дотримуються політики безпеки компанії, правил і схильності до ризику. Це часто призводить до безперервних зв'язків із постачальником, щоб розібратися в анкетах та запитах на виправлення, що може затримати весь процес продажу.

На щастя, тепер доступні рішення для автоматизації оцінки ризиків безпеки третіх сторін і керування ними, різкого прискорення сторонніх процесів оцінки для компаній, які оцінюють нових постачальників, і скорочення циклу продажів для постачальників.

Цикли збуту можуть як стимулювати, так і порушувати зростання бізнесу; чим довший цикл продажу, тим менша ймовірність закриття угоди з жахливими наслідками для трубопроводів і доходів. Коли цикли продажів затягуються як прямий наслідок складних оцінок ризиків кібербезпеки, бізнес може бути втрачений. Тому цикли продажів повинні бути максимально короткими та ефективними. Найкращий спосіб зробити це – запровадити ефективний процес оцінки кібербезпеки.

Як правило, постачальники стикаються з кількома ключовими проблемами під час оцінки безпеки. Оцінка безпеки може бути довгим і виснажливим процесом, займати час і ресурси, подовжувати цикл продажів і ускладнювати зростання бізнесу. Наприклад, команда безпеки постачальника може втомитися відповідати на подібні таємні запитання та подальші електронні листи. Вони можуть втратити процес. Вони також можуть зіткнутися з тиском з боку відділу продажів, щоб якомога швидше завершити оцінку, що може негативно вплинути на внутрішні відносини в організації. Вони також повинні відповідати на запити на виправлення від оцінювачів, а також усувати неточності. Все це впливає на команди безпеки та їхню здатність захищати організацію.

Як це можна вирішити?

Технології від сторонніх постачальників управління безпекою можуть спростити процеси продажів і прискорити зростання бізнесу постачальників, яких оцінюють їхні клієнти. Наприклад, надаючи постачальникам можливість зареєструватися на платформі, вони можуть отримати повну видимість свого власного профілю безпеки, дозволяючи їм відстежувати будь-які прогалини в безпеці та мати повний контроль над своєю кібербезпекою навіть до того, як їх оцінять потенційні клієнти.

Крім того, деякі сторонні платформи ризику безпеки надають постачальникам можливість створити огляд безпеки своєї компанії та поділитися ним із потенційними клієнтами на початку циклу продажів. Вони можуть включати будь-яку інформацію, пов’язану з безпекою, включаючи питання для самооцінки, сертифікати та показники відповідності. Стати проактивним і ділитися оглядом безпеки ще до того, як вас попросять заповнити анкету безпеки, заощаджує час і ресурси, допомагаючи компаніям прискорити процес продажів.

Що ще важливіше, постачальники, які підписалися на сторонні платформи ризику безпеки, також можуть переглядати й керувати всіма запитами та анкетами своїх клієнтів щодо відновлення безпеки та контролювати їхній профіль безпеки на одній платформі, що забезпечує спрощену співпрацю та комунікацію, а також полегшує роботу. щоб підтвердити свою позицію безпеки.

Зрештою, оцінки безпеки більше не повинні бути блокувальником бізнесу тепер, коли є доступні рішення, які передають повноваження в руки постачальників. Суть? Компанії, які беруть активну роль у процесі оцінки безпеки своїх клієнтів, можуть прискорити свій цикл продажів і прискорити зростання

бізнесу». **(Hen Amartely. How Do Cybersecurity Assessments Impact Business Growth? // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/how-do-cybersecurity-assessments-impact-business-growth/). 10.12.2021).**

***

«Зміни є ворогом фахівців з IT та кібербезпеки, яким необхідно підтримувати безпечне та доступне середовище. Незалежно від того, наскільки безпечним є ваше середовище, одна погана зміна – це все, що потрібно, щоб відкрити двері поганому актору.

Несанкціоновані, неочікувані та небажані зміни критичних файлів, систем і пристроїв можуть швидко відкрити діру в системі кібербезпеки організації. На цьому етапі не має значення, наскільки якісні інші засоби контролю — порушення може бути неминучим.

Що таке зміна?

Усе, що відбувається в IT-середовищі (хороше чи погане), починається зі зміни: файл, налаштування конфігурації чи пристрій змінюються, видаляються, додаються або навіть просто читаються користувачем чи службою.

Кожна погана річ в середовищі організації починається зі змін, але також і кожна хороша річ. Завдання полягає у визначенні різниці. Тут також вступає в гру надійний базовий рівень. Все, що не включено до базової лінії, можна вважати поганим, поки не буде доведено протилежне.

Для кожної зміни організація може виконувати простий процес:

Визначте, що саме змінилося в навколишньому середовищі.

Перевірте, чи санкціонована зміна відповідно до базової лінії.

Дозволити, заблокувати або відкотити зміни відповідно до потреб.

Тоні Сейгер, старший віце-президент і головний євангеліст Центру інтернет-безпеки (CIS), пояснює це так:

«Ви повинні знати, що у вас є і які зміни є прийнятними. Тоді вам доведеться зупинити все інше і керувати винятком, де це необхідно. Це не обов'язково легко, тому що є багато змін. Якщо у вас є механізми, щоб контролювати це, у вас є основа доброчесності».

Чому зміни такі важливі?

Як ми бачили, все погане в IT-середовищі починається зі змін. Цей факт уточнює дослідження IDC, яке виявило, що величезна частина відключень IT спричинена людськими помилками, включаючи невідповідність процесам управління змінами. Іншими словами, нездатність належним чином керувати змінами в IT-середовищі є однією з найбільших причин незапланованих простоїв.

Донна Скотт, віце-президент і директор з досліджень Gartner, йде ще далі, заявляючи, що:

«80 відсотків незапланованих простоїв викликано проблемами людей і процесів, включаючи погану практику управління змінами, а решта спричинена технічними збоями та катастрофами».

Виходячи зі свого досвіду роботи з сотнями IT-організацій, автори The Visible Ops Handbook відзначають, що навіть після того, як інцидент стався, 80%

середнього часу відновлення (MTTR) витрачається даремно на непродуктивну діяльність, зокрема, на визначення змін. несе відповідальність за відключення.

Управління змінами як функція кібербезпеки

Дослідження, проведене на замовлення Міністерства оборони США (DoD), показало, що:

«Інформаційна безпека залежить від ефективності процесу управління змінами. У результаті нам потрібно запровадити детективний контроль, щоб перевірити відповідність [авторитетним базовим показникам] і вжити рішучих дій, коли процес не дотримується».

Зверніть увагу на формулювання. Управління змінами не просто важливе – це стрижень усієї функції інформаційної безпеки. З огляду на все це, чому постачальники кібербезпеки не намагалися вирішити проблему управління змінами?

Забезпечення цілісності системи (SIA)

Як зовсім інший підхід до кібербезпеки, System Integrity Assurance (SIA) зосереджується на основах. Замість того, щоб намагатися визначити і класифікувати всі погані речі, замість цього він визначає все, що це дозволено (включаючи зміни) в навколишньому середовищі, і блокує все інше.

Звичайно, потрібен певний рівень управління за винятком. Деякі зміни можуть не бути включені до базової лінії, але їх можна вважати прийнятними при подальшому аналізі. У цих випадках зміну можна дозволити та додати до надійної базової лінії для подальшого використання.

Завдяки цьому процесу забезпечення цілісності системи перевіряє цілісність, надаючи організаціям повний контроль над змінами в їхньому середовищі.

Це викликає ще одне запитання:

Що станеться, якщо ви знаєте щоразу, коли щось додається, видаляється або змінюється у вашому середовищі, і ви зупиняєте все, що не авторизовано і розширюєте цю можливість на всі класи активів?

Програми-вимагачі та інші шкідливі програми не можуть працювати в середовищі.

Зловмисники не можуть пройти через мережу або вилучити дані.

Ніхто не може змінювати файли чи конфігурації, щоб зробити їх небезпечними чи невідповідними.

Користувачі не можуть випадково запустити шкідливі вкладення.

Ніхто (навіть привілейовані адміністратори) не може змінювати важливі системні файли.

Цей підхід забирає масивну частину загроз, які можуть виникнути в IT - середовищі з мінімальною участю людини…» ***(Jacqueline von Ogden. The Role of Change in Cybersecurity // Cimcor, Inc (https://www.cimcor.com/blog/the-role-of-change-in-cybersecurity). 15.12.2021).***

***

«Несмотря на то, что каждый год в индустрии безопасности и соблюдения нормативных требований происходит так много всего, если бы мы выбрали одну тему, чтобы выделить ее в 2021 году, это было бы

следующее: ожидания в отношении кибергигиены организации и зрелости ее программы соблюдения нормативных требований возросли. После того, как компании и правительственные учреждения в течение многих лет подвергались многочисленным разрушительным атакам, в том числе крупным атакам на критически важные секторы инфраструктуры страны в этом году (например, были затронуты нефтепроводный, финансовый, продовольственный и транспортный секторы), организации, наконец, начали наращивать свои собственная киберзащита и надзор за продавцами и поставщиками.

Как поставщик SaaS, Hyperproof увидела, что эта тенденция повышенного внимания проявляется в нашем собственном цикле продаж. Раньше потенциальные клиенты задавали нам всего несколько вопросов безопасности в процессе проверки безопасности. Теперь многие потенциальные клиенты хотят видеть много подробной информации, чтобы убедиться, что наш сервис соответствует их требованиям безопасности. Они проводят подробный анализ нашего отчета SOC 2 и задают ряд дополнительных вопросов. Мы также видели больше случаев, когда клиенты просили нас взять на себя договорные обязательства по соблюдению определенных требований безопасности. Эти организации по закону обязаны просить своих поставщиков SaaS провести такую комплексную проверку в соответствии с их контрактом со своими клиентами. Многие клиенты Hyperproof - как компании из списка Fortune500, так и частные компании - находятся в аналогичной ситуации и сталкиваются с массой вопросов безопасности от своих клиентов.

Последние правила с требованиями к управлению рисками в цепочке поставок

Представление о том, что управление рисками в цепочке поставок должно стать программным (а не специальным), за последние несколько лет вошло в ряд нормативных актов и отраслевых стандартов. Вот лишь некоторые из наиболее известных организаций по нормативным актам и стандартам, на которые следует обратить внимание.

Общий регламент ЕС по защите данных (GDPR)

В сферу действия GDPR входят все организации Европейского Союза, которые собирают, хранят или обрабатывают персональные данные любого лица, проживающего в ЕС, а также любые организации, не входящие в ЕС, которые предлагают товары и услуги европейским резидентам или организации, не входящие в ЕС, которые обрабатывают идентифицируемые личности данные. Европейский союз ожидает, что обработчики данных, в том числе поставщики управляемых услуг (MSP) и поставщики SaaS, во всем мире будут соответствовать законодательству GDPR. Европейские организации (контроллеры данных), использующие обработчики данных за пределами ЕС, должны убедиться, что их поставщики по обработке данных соблюдают правила GDPR.

В соответствии с руководящими принципами GDPR обработчики данных обязаны защищать данные таким образом, чтобы обеспечить безопасность всех личных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери и повреждения. Должны быть приняты административные, физические и технические меры безопасности, поскольку

законодательство ЕС налагает равную ответственность на контроллеров и обработчиков данных.

Закон Калифорнии о правах потребителей на неприкосновенность частной жизни (CPRA)

CPRA, который вступит в силу 1 января 2023 года, налагает аналогичный набор требований на обработчиков данных - тех, кто обрабатывает персональные данные от имени другой компании - как GDPR. Он обязывает организации, которые собирают данные (например, любую компанию с потребителями, проживающими в Калифорнии), привлекать своих поставщиков услуг к ответственности за защиту данных таким образом, чтобы гарантировать безопасность всех личных данных.

NIST SP 800-53, Безопасность и контроль конфиденциальности для информационных систем и организаций

Любая организация, которая обрабатывает федеральную информацию, обязана внедрить средства контроля NIST SP 800-53 и подтвердить свою позицию соответствия, чтобы поддерживать отношения со своим государственным заказчиком. В сентябре 2020 года NIST SP 800-53 получил серьезное обновление. В него добавлено новое семейство средств контроля для управления рисками цепочки поставок, в котором четко сформулировано, что NIST хочет, чтобы организации ставили риск в центр управления цепочкой поставок. В этом контрольном семействе подчеркивается несколько ключевых моментов:

Все агентства и подрядчики должны иметь официальную политику и процедуры управления рисками для выявления и управления рисками в цепочке поставок.

Все агентства и подрядчики должны быть осведомлены об источниках и компонентах систем, которые они используют, чтобы гарантировать, что изменения на начальном этапе оцениваются и документируются.

Все агентства и подрядчики должны оценивать поставщиков на основе выявленных рисков и согласованных договорных или сроков и условий.

Все агентства и подрядчики должны идентифицировать ключевую информацию о цепочке поставок, относящуюся к чувствительным операциям и системам; определить меры безопасности для противодействия рискам третьих лиц, связанным с операциями и системами.

Сторонние соглашения или контракты должны четко подчеркивать любые меры контроля, связанные с конфиденциальностью, которых третьи стороны должны придерживаться в рамках разработки систем и услуг.

Должны быть заключены соглашения об уведомлении, чтобы третьи стороны знали, когда и как предупреждать организации в случае возникновения проблем.

Другими словами, NIST утверждает, что если ваша компания считается «поставщиком» государственного подрядчика, вам необходимо будет внедрить меры безопасности, которые ожидает от вас ваш заказчик, и подтвердить, что они у вас есть в вашем договорном соглашении с заказчиком. Если вы используете сторонний компонент в своем собственном приложении, вам необходимо будет оценить риски, связанные с использованием этого стороннего компонента, и

убедиться, что сторонняя сторона имеет адекватные меры защиты данных для нейтрализации рисков.

CMMC 2.0

Программа сертификации модели зрелости кибербезопасности (CMMC) была создана в 2020 году Министерством обороны для проверки того, что все компании оборонной промышленной базы - как подрядчики, так и субподрядчики - имеют достаточные меры безопасности и конфиденциальности для защиты федеральной информации (в частности, контролируемой несекретная информация) в их ведении. Первоначальная версия устанавливала пять уровней и требовала, чтобы все подрядчики и субподрядчики - независимо от того, обрабатывают ли они конфиденциальные данные или нет - прошли процедуру сертификации третьей стороной, чтобы проверить свои меры безопасности и соответствие требованиям.

В ноябре 2021 года Министерство обороны обновило программу (CMMC 2.0) до трех уровней и отменило требование сертификации третьей стороной для компаний уровня 1 - тех, кто не обрабатывает контролируемую несекретную информацию. Однако все компании уровня 1 (в основном малые предприятия) должны проводить ежегодную самооценку, и должностное лицо или руководитель компании должны подтвердить, что ответы, представленные в ежегодной самооценке, являются точными и полными.

Чтобы убедиться, что никто не делает ложных заявлений в своей самооценке безопасности, Министерство юстиции имеет законные полномочия расследовать правительственные подрядчики, которые якобы подавали «ложные заявления» относительно своей практики кибербезопасности в соответствии с Законом о ложных заявках (FCA). Министерство юстиции может наложить крупные штрафы на признанных виновными юридических и физических лиц.

Министерство юстиции заявило, что следующие типы ситуаций могут вызвать расследование в отношении организации или отдельного лица:

Сознательное предоставление несовершенных продуктов или услуг в области кибербезопасности

Умышленное искажение своих практик или протоколов кибербезопасности

Сознательное нарушение обязательств по мониторингу и сообщению об инцидентах и нарушениях кибербезопасности

Согласно FCA, лицо действует осознанно, когда оно: 1) действительно знает информацию, 2) действует, сознательно игнорируя правдивость или ложность информации, или 3) действует безрассудно в отношении информации. Кроме того, у человека не обязательно должно быть какое-то конкретное намерение обмануть правительство. Таким образом, что касается подтверждения самооценки CMMC 2.0, если утверждение неверно, компания DIB могла бы нести ответственность в соответствии с FCA, даже если ее руководство не намеревалось обманывать правительство и не имело фактических сведений о том, что ее утверждение было неверным. Компания DIB может быть обнаружена «в безрассудном пренебрежении правдой», если не провела достаточную должную осмотрительность своих практик и процедур кибербезопасности до своего подтверждения. Это подвергает компанию возмещению убытков и денежным штрафам.

Вот главный вывод из всех этих правил: «Когда организации не уделяют достаточного внимания своей программе соблюдения нормативных требований (в том числе не проводят достаточную должную осмотрительность в отношении собственных практик и процедур кибербезопасности своих третьих лиц), они могут потерять клиентов и столкнуться со значительной юридической ответственностью. Руководители, контролирующие деятельность компании, также могут нести личную ответственность в соответствии с определенными положениями, такими как CMMC 2.0».

Задача на 2022 год: работа в рамках модели непрерывного доверия

Чтобы уменьшить эту потенциальную ответственность, важно, чтобы организации полностью понимали требования, которые их просят выполнять, и внедряли средства контроля, необходимые для выполнения этих юридических и договорных требований. Организации должны тестировать свои средства контроля и собирать доказательства на постоянной основе, чтобы показать клиентам (и регулирующим органам), что они соблюдают свои договорные обязательства на протяжении всего срока действия договора.

Помимо снижения юридических рисков, постоянный анализ и управление средствами контроля имеют решающее значение для поддержания устойчивости. Схемы кибератак быстро развиваются. Новые риски безопасности и соответствия нормативным требованиям могут возникать при принятии рутинных бизнес-решений, например, когда сотрудники начинают использовать новую облачную службу для повышения операционной эффективности или когда подразделение решает запустить новый продукт.

На этом стыке организации должны принять новый вызов. Им необходимо создать возможности, необходимые для работы в рамках модели непрерывного доверия. Это включает поиск способа масштабирования деятельности по внедрению средств контроля - действий, предпринимаемых для выполнения требований законодательства, снижения рисков безопасности и конфиденциальности и повышения операционной эффективности. Организации должны будут придерживаться структурированного, повторяемого, непрерывного подхода к обучению нужных людей элементам управления, назначению прав собственности на элементы управления, оценке соответствия элементам управления и устранению пробелов.

Чтобы добиться успеха в использовании модели непрерывного обеспечения, организациям потребуется использовать технологии для централизованного управления своей программой соответствия и распределения ответственности за операционные средства контроля между людьми в рамках нескольких бизнес-функций. Технологии дадут людям возможность выполнять действия по контролю должным образом, вовремя и эффективно, так что работа по обеспечению уверенности становится инструментом, способствующим развитию бизнеса, а не чем-то, что слишком сильно его замедляет. Эта модель непрерывного обеспечения является большим отходом от вчерашней модели, ориентированной на аудит, когда организации полагались на точечные аудиты, чтобы измерить уровень своей безопасности и определить, какие исправления необходимы. Те, кто справится с проблемой работы в модели непрерывного доверия, будут организациями, которым

доверяют и любят их клиенты». ***(JINGCONG ZHAO. The State of Security Assurance in 2021 and Outlook on 2022 // Hyperproof (https://hyperproof.io/resource/security-assurance-outlook-2022/). 16.12.2021).***

***

«Вот основные тенденции кибербезопасности, которые мы ожидаем увидеть в 2022 году, что даст читателям некоторое представление о том, как может выглядеть будущее отрасли.

Для начала следует отметить, что многое из того, что мы ожидаем в 2022 году, отчасти было затронуто пандемией COVID в течение 2020 и даже 2021 года. тише за последние несколько месяцев. Беспокойство по поводу нового варианта Omicron постепенно растет, но это дело другого дня. Я пытаюсь подчеркнуть, что в связи с популяризацией в 2020 году множества цифровых тенденций, таких как работа из дома, массовые мобильные игры и растущая зависимость от онлайн-покупок, будущее, на которое мы смотрим сейчас, может отражать эти самые изменения в образ мышления населения. Интересно посмотреть, сколько крупных событий может привести к тому, что взгляды и практика будут изменены гораздо более постоянным способом, чем мы когда-либо ожидали.

Согласно прогнозам, в 2022 году, как и в предыдущем году, количество угроз кибербезопасности со стороны вредоносных программ будет продолжаться, причем наиболее ожидаемой их формой будут программы-вымогатели. Программы-вымогатели, для тех, кто не знает, - это разновидность вредоносного ПО, которое шифрует ключевые приложения и компоненты на технических устройствах. После этого злоумышленник свяжется с пострадавшим и попросит денежную сумму или другую денежную выгоду в обмен на разблокировку для него содержимого устройства. Раньше с программами-вымогателями не так часто сталкивались, но из-за того, что продаются наборы вредоносных программ, некоторые из которых также довольно легкодоступны, в 2022 году потенциально может возникнуть больше атак такого рода.

Еще одна форма угрозы кибербезопасности, от которой пользователи могут ожидать больше в 2022 году, - это рост атак через Интернет вещей (IoT). IoT означает, что все больше и больше базовых электронных устройств и устройств подключаются друг к другу через Bluetooth или Интернет. Когда даже к одному из холодильников можно получить удаленный доступ с мобильного телефона, киберпреступники получают больше точек доступа, чем они знают, что делать. В результате даже доступ к чайнику может привести к тому, что конфиденциальная информация на ноутбуках или мобильных телефонах будет полностью раскрыта. Хотя атаки через Интернет вещей уже встречаются, в 2022 году, скорее всего, произойдет рост не только отдельных угроз, но и дальнейшее совершенствование методов их доставки.

Из-за этого безудержного роста угроз кибербезопасности предприятия также должны изменить свою деятельность, чтобы приспособиться; в частности, они будут более избирательны в выборе партнеров. Когда для доступа к конфиденциальной информации (которая чаще всего находится в сети) можно использовать так много разных площадок, большие и малые предприятия больше

не смогут позволить себе большие риски. Каждому нужно будет придерживаться лучших практик с точки зрения кибербезопасности, если он хочет оставаться актуальным и оставаться на плаву.

Однако при всех этих угрозах будут усилены и превентивные меры. В 2022 году мы увидим рост кибербезопасности на основе искусственного интеллекта, причем технологии будут становиться все более и более сложными по мере развития машинного обучения для предотвращения всех видов проводимых атак. Конечно, хакеры становятся умнее, но и образные гвардейцы тоже. Наконец, мы можем ожидать усиления регулирования с созданием большего числа органов и правил в интересах выявления и наказания крупных и мелких киберпреступников. Взгляните на приведенную ниже инфографику и диаграммы от Embroker для получения дополнительной информации». ***(Arooj Ahmed. The Biggest Cyber Security Trends That We Can Expect To Encounter In 2022 // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/the-biggest-cyber-security-trends-that.html). 29.12.2021).***

***

«Четверо из пяти профессионалов в области кибербезопасности беспокоятся о возможности скрытой атаки злоумышленника с помощью квантового компьютера, которая сделает шифрование их данных неэффективным.

Это был один из результатов глобального опроса, опубликованного во вторник более 600 профессионалов в области кибербезопасности, проведенного Dimensional Research для Cambridge Quantum, компании по квантовой криптографии, которая недавно стала частью Quantinuum.

«В сообществе кибербезопасности много опасений, - заметил Дункан Джонс, глава отдела квантовой кибербезопасности в Cambridge Quantum.

«Наблюдается неуклонный рост изощренных кибератак, поэтому люди нервничают из-за того, что неожиданно произойдет что-то, что сделает существующие средства защиты недостаточными», - сказал он TechNewsWorld.

«Криптографические алгоритмы обычно создаются на основе математических задач», - пояснил он. «Проблемы легко решить, если вы знаете, что это за ключ, но невозможно решить, если вы не знаете, что это за ключ».

«К сожалению, алгоритмы, которые мы используем сегодня, используют математические задачи, которые квантовые компьютеры смогут решить, даже если у них нет ключа», - сказал он.

Квантовые компьютеры могут обрабатывать данные намного быстрее, чем большинство компьютеров сегодня, потому что они используют кубиты для обработки данных, которые не ограничиваются нулями и единицами.

Множество предупреждений

Микела Ментинг, директор по исследованиям в области цифровой безопасности в ABI Research, отметила, что квантовые компьютеры с возможностью атак не за горами, но сомневается, что когда они атакуют, это будет большим сюрпризом.

«Я думаю, что существует много информации о возможности того, что это произойдет, поэтому, если организации не прячут голову в песок, у них будет много предупреждений», - сказала она TechNewsWorld.

«В краткосрочной перспективе событие без предупреждения маловероятно», - добавила Хизер Уэст, старший аналитик группы IDC по инфраструктуре, системам, платформам и технологиям.

«Хотя квантовые вычисления находятся на переломном этапе, переходя от научного интереса к коммерческой жизнеспособности, они все еще очень молоды», - сказала она TechNewsWorld.

«Есть еще много улучшений, которые необходимо сделать, прежде чем его можно будет использовать для решения сложных проблем, например, взломать алгоритмы шифрования, защищающие наши данные сегодня», - продолжила она.

«Сегодня мы не должны терять сон из-за этого, но по мере развития технологий в течение следующих 10 лет мы должны начать беспокоиться», - добавила она.

Скрытие квантовых исследований

В настоящее время нет квантовых компьютеров, способных взломать существующие схемы шифрования, утверждает Марк Хорват, старший директор по исследованиям в Gartner.

«Однако, как и компромиссы SHA-1 середины 2000-х годов, мы ожидаем, что они добьются прогресса в течение следующих пяти лет, ослабляя существующие алгоритмы до такой степени, что их необходимо будет заменить», - сказал он TechNewsWorld.

Но Роджер Граймс, защитник из KnowBe4, поставщика услуг по обучению вопросам безопасности в Клируотере, штат Флорида, утверждал, что скрытая атака могла произойти из-за секретности, окружающей разработку квантовых компьютеров.

«Каждое способное национальное государство работает над тем, чтобы получить достаточно способные квантовые компьютеры, и если они сделают это раньше, чем публичный конкурент, то они скроют свои квантовые достижения. Это гарантировано», - сказал он TechNewsWorld.

«Это могло уже иметь место, и мы просто не знаем об этом», - сказал он.

«Что еще более важно, - продолжил он, - если у вас есть большие секреты, которые вам нужно хранить в секрете еще много лет, национальное государство или конкурентный противник уже может перехватить ваш теперь зашифрованный сетевой трафик и сохранить его на то время, когда они иметь в будущем достаточно мощные квантовые компьютеры».

«Конечно, национальные государства уже делают это, просто ждут своего дня», - добавил он. «И когда это произойдет, злоумышленники смогут прочитать любые секреты, ранее защищенные квантово-чувствительным шифрованием».

По этой причине есть исследователи, разрабатывающие так называемые постквантовые методы криптографии, - объяснил Дэниел Дж. Готье, профессор физики в Университете штата Огайо.

«В них используются математические методы, которые считаются безопасными против злоумышленника, у которого есть квантовый компьютер», - сказал он TechNewsWorld.

«Кроме того, некоторые страны разрабатывают методы квантовой связи, которые должны быть невосприимчивы к атаке со стороны субъекта с квантовым компьютером», - добавил он.

Взломать сейчас, расшифровать позже

«Взломать сейчас, расшифровать позже» может стать серьезной проблемой для организаций в будущем.

«Стратегия, применяемая противоборствующими странами и другими злоумышленниками для кражи зашифрованных сообщений сегодня для последующего дешифрования с помощью квантовых компьютеров, должна особенно касаться тех организаций, которые должны защищать критически важные данные в течение нескольких лет или более», - сказал Джонс в пресс-релизе.

«В наши дни хранить данные очень дешево и легко», - добавил он в интервью. «Таким образом, можно с уверенностью предположить, что злоумышленники записывают зашифрованный трафик сегодня, зная, что они могут взломать его через пять или десять лет».

Ментинг отметил, что взломать сейчас и расшифровать более поздние кампании - обычное дело. «Это в основном осуществляется национальными государствами и спонсируемыми государством группами, включая все крупные экономические и политические державы сегодня, и вполне реально предположить, что такие страны, как Китай и Россия, активно в этом участвуют», - сказала она.

Готье отметил, что этот метод полезен только для данных с длительным сроком службы. «Для информации с коротким сроком полезного использования эта атака неэффективна», - заметил он.

Стоит ожидания?

Даже если данные будут полезны через пять или десять лет, извлечь их из шифрования, даже с помощью квантового компьютера, может быть непросто.

«Хотя существует возможность взломать существующий ключ с помощью квантового компьютера, это не будет быстрым процессом, по крайней мере, не сразу», - сказал Хорват.

«Массовый взлом больших объемов данных - все с разными ключами - в этом десятилетии будет непрактичным», - продолжил он. «Выборочная ориентация некоторых документов будет возможна в течение пяти-десяти лет, но это потребует больших ресурсов».

Он пояснил, что, поскольку у большинства ключей шифрования короткий жизненный цикл - около двух лет, - долгосрочные документы, такие как ипотека, и некоторые секретные документы сейчас больше всего подвержены риску взлома, расшифруйте последующие атаки.

Хорват советует организациям тщательно анализировать свои потребности в криптовалюте, исходя из ожидаемой долговечности данных, и соответственно наращивать шифрование. В оставшееся десятилетие простого удлинения ключей должно быть достаточно, чтобы обеспечить безопасность наиболее важных документов.

Организации, которые хотят быть впереди в игре с шифрованием, должны постоянно обновлять свои системы, добавил Джесси Варсалон, адъюнкт-профессор компьютерных сетей и кибербезопасности в Глобальном кампусе Университета Мэриленда в Адельфи, штат Мэриленд.

«Что действительно должно вас беспокоить, так это старые технологии, которые были разработаны, когда вычислительные мощности были не такими, как сегодня», - сказал он TechNewsWorld. «Эти компьютеры будут особенно уязвимы для атак квантового компьютера по сравнению с новейшим и лучшим оборудованием». ***(John P. Mello Jr. Cybersecurity Pros Uneasy Over Prospect of Quantum Sneak Attack // ECT News Network, Inc. (https://www.technewsworld.com/story/cybersecurity-pros-uneasy-over-prospect-of-quantum-sneak-attack-87362.html). 08.12.2021).***

***

«По мере того, как 2021 год подходит к концу, для экспертов по кибербезопасности пора бросить свои руны и спрогнозировать, что ждет потребителей и практиков в наступающем году.

Киберпреступники перейдут от кражи личных данных к мошенничеству, предсказали в Центре ресурсов по краже личных данных в Сан-Диего.

Злоумышленники накапливают личную идентифицирующую информацию, но они не используют ее для нацеливания на потребителей в той мере, в какой они это делали раньше. Скорее, они используют его в атаках на учетные данные на предприятиях, объяснила некоммерческая организация, занимающаяся минимизацией рисков и смягчением последствий взлома личных данных и преступлений.

По прогнозам ITRC, рост мошенничества приведет к еще одному событию в 2022 году: потребители откажутся от определенных видов онлайн-активности.

«Постоянное улучшение легкости и качества фишинговых атак заставит некоторых потребителей переосмыслить онлайн-покупки и изменить привычки общения из-за страха стать жертвой идеально подделанных электронных писем, веб-сайтов или текстовых сообщений», - поясняет ITRC в пресс-релизе.

«Некоторые люди, вероятно, полностью откажутся от электронной почты, потому что считают, что риск слишком велик», - добавил он. «Это может привести к возвращению «старой школы» коммуникации, такой как телефонная и почтовая почта».

Вредоносное ПО в упадке

Центр также прогнозирует, что вредоносное ПО выровняется как основная причина утечки данных в следующем году, и темпы повторной виктимизации будут расти.

Он отметил, что программы-вымогатели могут догнать или превзойти нарушения, связанные с фишингом, как причину номер один утечек данных, в то время как атаки цепочки поставок будут передавать вредоносные программы как третью по распространенности первопричину утечки данных.

ITRC отмечает, что в 2021 году число потребителей, многократно пострадавших от онлайн-мошенников, продолжило расти, и эта тенденция сохранится и в 2022 году.

«Единичные инциденты, нацеленные на нескольких лиц или организаций, повлияют на большее количество жертв в разных сообществах и географических регионах», - прогнозируют в центре.

«Захват аккаунтов в социальных сетях, в частности, позволит использовать подписчиков и отдельные сети для создания новых цепочек жертв», - добавил он.

Согласно Lookout, поставщику мобильных фишинговых решений из Сан-Франциско, еще одной привлекательной областью для цифровых бандитов в наступающем году станет мошенничество с криптовалютой.

Он привел данные Федеральной торговой комиссии, которые показали, что с октября 2020 года по май 2021 года потребители сообщили о потерях в размере 80 миллионов долларов США в результате мошенничества с инвестициями в криптовалюту со средним убытком в размере 1900 долларов США. Это в 12 раз превышает количество отчетов за предыдущий год, отмечает Lookout в блоге компании.

«Поскольку счета в криптовалюте не застрахованы государством, как доллары США, а платежи в криптовалюте необратимы, риск для потребителей особенно высок», - пояснил он.

«По мере того, как люди принимают криптовалюту с большой скоростью, мошенничество будет продолжать расти, становясь все более изощренным, распространенным и ценным, поскольку злоумышленники работают над тем, чтобы обманом заставить людей отдать свою валюту», - добавлено в нем.

Целевые домашние сети

Еще одним событием в 2022 году станет более широкое использование домашних сетей в качестве инфраструктуры для хакеров, предсказал Илья Сотников, вице-президент по взаимодействию с пользователями и стратег по безопасности в Netwrix, разработчике платформы видимости и управления облачными средами в Ирвине, Калифорния.

«Домашнюю сеть намного легче заразить вредоносным ПО, чем профессионально защищенную корпоративную ИТ-среду», - сказал он TechNewsWorld.

«С увеличением вычислительной мощности и пропускной способности подключения в жилых домах домашние сети станут более привлекательными для злоумышленников», - сказал он.

«Например, - продолжил он, - заразив множество устройств, они смогут динамически изменять IP-адреса или даже доменные имена во время вредоносных кампаний, препятствуя распространенным мерам защиты, таким как блокировка IP-адресов и DNS-фильтрация».

Сотников также предсказал, что будет больше атак на поставщиков управляемых услуг. «Злоумышленники ухватились за очень эффективную стратегию получения доступа к крупным организациям - через относительно слабые ИТ-инфраструктуры малых и средних предприятий, которые предоставляют им услуги», - пояснил он.

«Соответственно, провайдеры управляемых услуг должны будут увеличить как широту, так и глубину своих мер безопасности, поскольку многие малые и средние предприятия полагаются на них в обеспечении своей безопасности», - сказал он.

Рост нулевого доверия

На уровне предприятия в 2022 году защита гибридных облаков станет неотложной задачей высшего руководства, считает Николас Браун, генеральный директор Hitachi ID Systems, компании по управлению доступом и идентификацией в Калгари, Альберта, Канада.

Он также предсказал, что сети Zero Trust, требующие непрерывной аутентификации и мониторинга сетевого поведения, перегрузят инфраструктуры безопасности гибридного облака.

«Традиционные виртуальные частные сети и безопасность на основе периметра уходят, что дает основания для продолжения расширения сетей Zero Trust и доминирования в обсуждениях безопасности гибридных облаков», - сказал он TechNewsWorld.

«С расширением внедрения SaaS состав сетей организаций становится более уязвимым для атак, что увеличивает потребность в защите без параметров, такой как архитектура Zero Trust», - добавил он.

По мере расширения Zero Trust в наступающем году, также будет использоваться система управления доступом к удостоверениям, утверждает Майкл Баньярд, глава отдела маркетинга IAM в WSO2, поставщике интеграции с открытым исходным кодом из Санта-Клары, Калифорния.

«Директора по информационной безопасности сделают IAM краеугольным камнем своих инициатив по обеспечению безопасности с нулевым доверием, особенно для облачных организаций», - сказал Буньярд TechNewsWorld.

«Хотя не существует единого решения, которое сделало бы Zero Trust идеальной реальностью, IAM - это необходимое начало, которое положит начало надлежащей гигиене кибербезопасности при разработке приложений, управлении удаленными сотрудниками и контроле развертывания IoT», - сказал он.

Демократизация безопасности

Еще одним событием в 2022 году станет повышение важности безопасности на периферии предприятия, предсказала Дженнифер Ферник, руководитель отдела исследований в NCC Group, консалтинговой компании по кибербезопасности из Манчестера, Великобритания.

«По мере распространения устройств IoT становится ключевым моментом в обеспечении безопасности самих новых подключенных устройств, а также ИИ и машинного обучения, работающих на них», - сказала она TechNewsWorld.

«Кибер-осведомленность также будет иметь решающее значение, поскольку некоторые организации начинают использовать полосу пропускания 5G, что приведет к увеличению как количества устройств Интернета вещей в мире, так и размеров поверхности атаки для пользователей и производителей устройств Интернета вещей, а также множества сетей, чтобы которые они соединяют, и цепочки поставок, по которым они движутся», - сказала она.

Важным событием в корпоративной сфере в следующем году станет дальнейшая демократизация безопасности.

«Традиция иметь единого администратора идентификации или безопасности быстро сокращается», - заметил Буньярд.

«Демократизация безопасности будет происходить, гарантируя, что каждый в организации ознакомится с лучшими практиками безопасности и сможет внести свой вклад в предотвращение нарушения безопасности», - продолжил он.

«Больше никто не сможет сказать, что безопасность «не моя работа». Разработчикам, в частности, придется носить разные шляпы, поскольку нехватка технических навыков усиливается», - сказал он.

«Это также означает, что кибербезопасность должна стать частью учебной программы по программированию, чтобы дать новым выпускникам программной инженерии больше навыков в области безопасности», - добавил он». ***(John P. Mello Jr. Cybersecurity 2022: More Fraud, More Fakes, More Crypto Scams // ECT News Network, Inc. (https://www.technewsworld.com/story/cybersecurity-2022-more-fraud-more-fakes-more-crypto-scams-87374.html). 29.12.2021).***

***

«По мере того как предприятия планируют и устанавливают бюджеты на новый год вперед, подавляющее большинство ожидают, что они направят больше долларов на усиление своих усилий в области кибербезопасности.

Организации, стремящиеся увеличить свои бюджеты на кибербезопасность

Согласно последнему опросу Neustar International Security Council (NISC), проведенному в ноябре 2021 года, 81% организаций взяли на себя обязательство увеличить свои бюджеты на кибербезопасность на 2022 год. 24% респондентов увеличивают ассигнования от 31% до 50%. за последний год 41% увеличивают бюджеты с 11% до 30%.

«По мере того, как ландшафт киберугроз продолжает развиваться, организации четко осознают острую необходимость в масштабировании своих систем и процессов, чтобы хотя бы на один шаг опережать злоумышленников», - сказал Карлос Моралес, старший вице-президент по решениям для Neustar Security Services.

«Наши последние данные показывают, что руководители высшего звена и члены совета директоров хорошо осведомлены о последствиях пробелов в системе безопасности для бизнеса, и поучительно видеть, что организации имеют поддержку на всем протяжении цепочки руководства для осуществления необходимых инвестиций для защиты себя и своих клиентов».

Когда дело доходит до усиления мер кибербезопасности, организации в основном принимают участие сверху вниз. Среди участников опроса 93% сообщили, что планирование кибербезопасности предполагает участие членов совета директоров, а 63% отметили, что активное участие совета директоров является значительным. Такое участие считается критически важным, особенно в связи с тем, что организации стремятся предотвратить то, что, по их мнению, является растущей угрозой со стороны преступников и неизвестных субъектов.

Проблема разрыва кибер-навыков

Кроме того, по мере того, как атаки становятся все более многочисленными, сложными и изощренными, 88% организаций ожидают, что нехватка кибер-навыков повлияет на их стратегию безопасности 2022 года. 50% респондентов заявили, что ожидают значительного воздействия, и отметили, что им потребуются новые члены команды для реализации своих стратегий безопасности на 2022 год. Только 12% респондентов считают, что на выбранный ими курс действий не повлияет пробел в кибер-навыках.

Многие организации обращаются к внешним партнерам, чтобы восполнить этот пробел: 71% респондентов заявили, что планируют больше полагаться на сторонних поставщиков. Создание существующих команд также будет приоритетом: 56% планируют добавить в команду новых членов в следующем году.

Между тем, все больше людей ищут дополнительную подстраховку. Половина респондентов заявили, что их организация в настоящее время имеет полис киберстрахования, и 94% из них считают его выгодным вложением. Еще 22% организаций планируют внедрить политику в 2022 году, а 18% рассматривают такую перспективу.

В ходе ноябрьского опроса 82% ответивших предприятий подтвердили, что они когда-то подвергались DDoS-атаке, что лишь незначительно больше, чем в предыдущий отчетный период, но значительно больше, чем 59%, о которых сообщали до пандемии. DDoS-атаки считались одной из самых серьезных проблем с точки зрения киберугроз, при этом компрометация системы и программы-вымогатели замыкали тройку основных проблем в период исследования.

«Организации в основном осознают, что они не могут предотвратить кибератаки, но на сегодняшнем рынке у них есть доступ к широкому спектру инструментов и услуг для создания глубокоэшелонированной защиты», - продолжил Моралес.

«Привлекая правильных партнеров, организации могут предпринять важные шаги к достижению своих целей в области кибербезопасности, одновременно снимая с себя определенную нагрузку по привлечению новых талантов на очень узком рынке экспертных знаний в области кибербезопасности». ***(Cybersecurity budgets surge, as skills gap wreaks havoc on 2022 plans // Help Net Security (https://www.helpnetsecurity.com/2021/12/21/enhancing-cybersecurity-budgets/). 21.12.2021).***

***

«Сфера кибербезопасности всегда была динамичной. Однако в прошлом году были выявлены уязвимости и векторы атак, которые будут определять тенденции и формировать глобальные ожидания в отношении безопасности в 2022 году. Вот некоторые из ключевых областей, за которыми, по моему мнению, руководители организаций и профессионалы в области безопасности должны внимательно следить в предстоящем году.

Злоумышленники будут нацелены на внутренних сотрудников для кражи данных.

В 2021 году мы стали свидетелями того, как злоумышленники применили новый подход к краже данных - они нацелены на внутренние группы поддержки, такие как служба поддержки клиентов или ИТ-службы, для доступа и, в конечном итоге, кражи конфиденциальных и конфиденциальных данных. Мы видели несколько примеров этого, некоторые из которых были успешными, а некоторые нет; однако мы, вероятно, увидим больше таких инцидентов в 2022 году, поскольку злоумышленники продолжат адаптировать свои методы.

Поскольку злоумышленники напрямую нацелены на сотрудников с целью установки программ-вымогателей или извлечения конфиденциальных данных, обучение навыкам безопасности станет более важным, чем когда-либо прежде. Организации с эффективными программами обучения безопасности и повышения осведомленности персонала должны гарантировать, что каждая команда должным образом подготовлена к угрозам как внутри компании, так и за ее пределами.

Сотрудники работают во множестве сетей, которые, вероятно, различаются по уровню безопасности, и каждое их действие может представлять угрозу для всей организации. Если сотрудник не имеет надлежащей подготовки для выявления потенциальных угроз для информации компании, будь то отправка файлов кому-то, кто, по его мнению, работает на компанию, или обмен документами через облачные приложения, его организация остается открытой для внутренних факторов риска, которых можно избежать.

Организациям необходимо будет использовать более проактивный подход, чтобы расширить возможности сотрудников, более осведомленных о рисках, и, в конечном итоге, защитить себя от событий инсайдерского риска в предстоящем году.

Возросшие опасения по поводу программ-вымогателей

Программы-вымогатели сыграли важную роль в кибербезопасности 2021 года, и эта тенденция сохранится в новом году. Я ожидаю, что в 2022 году частота атак программ-вымогателей будет неуклонно расти и что кража данных в рамках атаки программ-вымогателей станет более распространенной проблемой в будущем. Злоумышленники становятся все более искусными в том, как причинить наибольшую боль организациям и найти лучшие способы украсть у них как можно больше данных. Реальность такова, что пока есть деньги, которые можно заработать на программах-вымогателях, они никуда не денутся; организации должны быть к этому готовы.

Изменение культуры в практике безопасности

Сейчас, более чем когда-либо, сотрудники просто выгорели - с этим сталкиваются профессионалы в области безопасности среди самых высоких групп. С выгоранием приходит апатия и непреднамеренная халатность - и экономия на процессах безопасности. Более трех четвертей утечек инсайдерских данных в этом году не были признаны вредоносными. По мере того, как выгорание достигает новых высот, отрасли необходимо предпринять согласованные усилия, чтобы предотвратить ухудшение этой статистики.

Принимая во внимание такие факторы, как выгорание на рабочем месте и уровень удержания сотрудников, в тандеме с общим движением к более чуткой культуре на рабочем месте, руководители службы безопасности поощряют

большую чуткость среди членов команды и во всей практике. Печально известная стоическая культура кибербезопасности меняется; в 2022 году мы увидим, что больше организаций приспосабливаются к этому сдвигу, меняя традиционные названия, такие как «Менеджер безопасности» на «Менеджер культуры безопасности», чтобы соответствовать, возможно, назревшей потребности признать, что культура, которую группа безопасности привносит в бизнес в целом, является не менее важны для защиты бизнеса.

Ожидайте повышения кибербезопасности в предвыборном цикле 2022 года

В связи с предстоящими в 2022 году многочисленными спорными и громкими промежуточными выборами кибербезопасность станет главным приоритетом для местных властей и властей штатов. Несмотря на то, что для защиты выборов 2020 года были предусмотрены меры безопасности, разглашенные разговоры о неуверенности в их безопасности будут способствовать повышению осведомленности о каждом аспекте голосования в следующем году.

Крипто станет вектором атаки в результате минимального регулирования

Популярность криптовалюты в сочетании с ограниченными правилами ее покупки и торговли делает ее главной целью для злоумышленников. В преддверии 2022 года я ожидаю, что злоумышленники найдут способы проникнуть в криптовалюту, эксплуатируя организации, а также покупателей и продавцов для получения больших доходов.

Сейчас есть повышенные ожидания - и огромное давление - на кибербезопасность как отрасль. Эти ожидания выдвинули кибербезопасность на передний план бизнес-операций и вызвали общий сдвиг в культуре безопасности.

Хотя нет верного способа окончательно предсказать тенденции, которые будут формировать отрасль в предстоящем году, события прошлого года подчеркивают неоспоримый факт, что безопасность в настоящее время является важной функцией бизнеса и повседневной жизни. В 2022 году реальность такова, что проактивная стратегия кибербезопасности - единственный способ уменьшить потерю данных и репутационный ущерб в случае киберугрозы или события риска. Будь то безопасность на промежуточных выборах, правила торговли криптовалютой или изменения в культуре, отрасль стремительно движется в будущее, и мы должны не отставать». ***(Jadee Hanson. How will the cybersecurity industry evolve in 2022? // Help Net Security (https://www.helpnetsecurity.com/2021/12/28/cybersecurity-industry-2022/). 28.12.2021).***

***

«Tromzo опубликовал результаты своего отчета, основанные на опросе 403 практикующих специалистов по безопасности приложений из США, которые работают в организациях, где их команда разработчиков использует системы CI / CD.

«Полученные данные подтверждают нашу веру в то, что службы безопасности должны сделать улучшение своих отношений с разработчиками одним из основных приоритетов в 2022 году», - сказал Харшил Парих, генеральный директор Tromzo. «Они могут сделать это, упростив безопасность для

разработчиков. Это означает интеграцию проверок безопасности в SDLC и переход от ворот безопасности к ограждениям, чтобы служба безопасности могла раз и навсегда стать первоклассным гражданином».

Состояние безопасности приложения

Уверенность в обеспечении безопасности приложений остается высокой, однако в 67% случаев за последний год произошли инциденты. Сопоставление этих двух фактов подчеркивает необходимость лучшего понимания того, что происходит между командами AppSec и разработчиков. Если группы безопасности уверены, что меры безопасности реализуются в среде разработки, хотя на самом деле это не так, существует повышенный риск серьезного инцидента безопасности.

40% имеют 5000 или более уязвимостей безопасности, которые необходимо устранить, и этот показатель быстро увеличился за последние 12 месяцев. Этот взрыв уязвимостей - универсальная проблема, которую команды AppSec должны решить раньше, чем позже.

42% видят больше ложных срабатываний и шума, чем когда-либо прежде. Ложные срабатывания и предупреждающий шум - это побочные продукты инструментов безопасности, которые не имеют контекста и используются на этапе обеспечения качества, а не на сквозном подходе.

Уменьшение трений между разработчиками и безопасностью окажет наиболее значительное влияние на улучшение программы безопасности приложений. Любая попытка минимизировать конфликт между безопасностью и командой разработчиков, не включающая сдвиг безопасности влево, вряд ли увенчается успехом. Пока безопасность является воротами, реализуемыми в конце цикла разработки, это вызовет трения разработчиков и вызовет задержки в развертывании безопасных приложений.

Игнорирование безопасности разработчиков - самая большая проблема. Эту проблему можно решить только с помощью платформы, которая позволит командам AppSec идти в ногу с современными разработками и масштабировать свою программу безопасности приложений.

Включение проверок безопасности в SDLC резко улучшит отношения с разработчиками. Мы должны перейти от ворот безопасности к ограждениям безопасности, которые позволяют разработчикам разрабатывать безопасный код». ***(Need to improve application security? Reduce friction between developers and security teams // Help Net Security (https://www.helpnetsecurity.com/2021/12/29/improve-application-security/). 29.12.2021).***

***

«По данным SE Labs, организации рискуют позволить призраку атак программ-вымогателей отвлечь их от соблюдения общих мер безопасности. Компания заявляет, что предприятия, которые ставят под сомнение свою собственную среду безопасности и при необходимости вносят коррективы, будут лучше защищены от регулярных атак.

«Компании должны перестать думать, что программы-вымогатели чем-то отличаются от любых других атак», - говорит Саймон Эдвардс, генеральный директор SE Labs. «Пособие хакера не сильно изменилось за эти годы. Проводите

разведку, получайте доступ, повышайте привилегии и крадите или уничтожайте информацию. Если они могут установить постоянный доступ одновременно, это будет бонус. Злоумышленники не используют магию, потому что им это не нужно. Испытанные и проверенные методы взлома правят день».

Программа-вымогатель - это просто стадия атаки «украсть или уничтожить», когда злоумышленник запускает программу, шифрующую данные жертвы. Все до этого момента представляет собой одну и ту же обычную атаку, будь то намерение начать кампанию вымогателей, незаметно шпионить за организацией или использовать скомпрометированную систему в качестве ступеньки к другой сети.

«Люди склонны думать, что взлом включает суперсекретные программы и таинственные знания, известные лишь горстке теневых компьютерных ботаников. Но вы можете выступить в роли довольно компетентного злоумышленника, имея несколько широко доступных книг, некоторое бесплатное программное обеспечение и доступ к YouTube», - говорит Эдвардс.

Хотя это может показаться плохой новостью, обычно прямой и предсказуемый подход злоумышленника является хорошей новостью для защитников. Во многих случаях поставщики средств безопасности используют проверенные и надежные методы обнаружения и защиты для защиты от программ-вымогателей, потому что они работают.

«Настоящая проблема возникает, когда достаточно мотивированный злоумышленник учится обходить существующую защиту», - заключает Эдвардс. «Затем наступает гонка вооружений, в которой продукты безопасности блокируют злоумышленников, которые затем учатся прогрессировать, что затем вдохновляет поставщиков на адаптацию. И так далее. Так же, как это было десятилетиями. Но предприятия также могут сыграть роль в предотвращении атак, поставив под сомнение свою собственную среду безопасности».

Вместо того, чтобы сосредоточиться на одной проблеме, такой как программы-вымогатели, организациям следует сосредоточиться на обеспечении того, чтобы их собственная среда была в достаточной степени заблокирована, чтобы предотвратить инициирование любого типа атаки, независимо от ее полезной нагрузки. Подтверждение того, что меры безопасности и политики по-прежнему отвечают потребностям бизнеса на регулярной основе, поможет укрепить защиту». ***(Businesses need to stop thinking that ransomware is different from other attacks // Help Net Security (https://www.helpnetsecurity.com/2021/12/30/different-ransomware-attacks/). 30.12.2021).***

***

«69,1% профессионалов, отвечающих за безопасность, считают, что необходимо переосмыслить, чтобы справиться с угрозой кибербезопасности теперь, когда устройства и приложения вышли за пределы корпоративной сети, показывает исследование SentryBay.

Опрос был направлен на оценку отношения к киберугрозам и методам защиты уязвимых устройств. Выяснилось, что 58,3% респондентов считают, что подход с нулевым доверием к безопасности имеет важное значение, и 19,9%

считают его важным. Однако на вопрос, ввела ли их организация нулевое доверие, только треть (33,6%) ответили, что сделали это.

Одним из препятствий могут быть трудности, с которыми компании сталкиваются при внедрении моделей BYOD, для которых нулевое доверие является рекомендуемым подходом к защите корпоративных периметров.

Препятствия при внедрении BYOD

33,5% сказали, что внедрение BYOD было слишком сложным. Роль корпоративных пользователей также была проблемой BYOD: проблемы конфиденциальности пользователей указали 28,1% респондентов, а взаимодействие / трение пользователей - 19,9%. Накладные расходы на управление были проблемой для 19,9%.

«BYOD предлагает предприятиям огромную экономию капитальных затрат, но они ничего не стоят, если принятие модели подвергнет организацию риску кибератаки», - сказал Дэйв Уотерсон, генеральный директор SentryBay.

«Ключом к безопасности в этом сценарии является проактивная защита, которая обеспечивается с помощью программного решения, которое специально направлено на предотвращение потери или утечки конфиденциальных данных из удаленной конечной точки, и это должно быть неотъемлемой частью подхода с нулевым доверием».

Изменение методов и практик кибербезопасности - непростая задача

Опрос показывает, что, хотя 47,7% организаций еще не приняли нулевое доверие, 8,5% уже находятся в процессе, а 10,6% планируют сделать это в 2022 году.

Стремление к изменению методов и практик кибербезопасности по мере того, как устройства и приложения удаляются из физических офисов и контролируемых сетей, очевидно, важно почти для 70% тех, кто работает в сфере безопасности, но это не означает, что этого всегда легко достичь.

«Несмотря на то, что кибербезопасность должна быть приоритетом для всех предприятий, определение и развертывание правильных решений для конкретных нужд компании может быть сложной задачей», - продолжил Дэйв Уотерсон.

«Часто требуется изменение культуры, следует искать знания и опыт экспертов по безопасности, но, что наиболее важно, конечные устройства - наиболее уязвимый элемент технологического стека - должны быть защищены проверенным программным обеспечением». ***(Rethinking cybersecurity becomes imperative as devices and apps move away from physical offices // Help Net Security (https://www.helpnetsecurity.com/2021/12/21/cybersecurity-devices-applications/). 21.12.2021).***

***

«Компания Trend Micro прогнозирует, что в 2022 г. глобальные организации смогут преуспеть в сдерживании киберрисков благодаря комплексному, проактивному, ориентированному на облака подходу. Решающее значение для управления рисками и защиты сотрудников получат исследования, прогнозирование и автоматизация. Только в первой половине 2021 г.

решения Trend Micro заблокировали 40,9 млрд почтовых угроз, вредоносных файлов и URL-адресов, что на 47% больше, чем годом ранее.

Специалисты компании предполагают, что в 2022 г. злоумышленники сосредоточат атаки программ-вымогателей на рабочих нагрузках в облаках и центрах обработки данных, а также на незащищённых сервисах, воспользовавшись тем, что значительное число сотрудников продолжает работать из дома. Согласно докладу Trend Micro, злоумышленники смогут использовать вновь обнаруженные уязвимости в рекордно короткие сроки, причём эти уязвимости будут связаны с ошибками повышения привилегий, что в сочетании друг с другом повысит успешность атак.

В прицеле киберпреступников окажутся также системы интернета вещей, глобальные цепочки поставок, облачные среды и функции DevOps. Одновременно более сложные версии массового вредоносного ПО будут нацелены на малый и средний бизнес.

В то же время, Trend Micro прогнозирует, что многие организации смогут достойно ответить на эти вызовы, поскольку уже начали выстраивать и внедрять стратегию упреждающего снижения возникающих рисков. Для этого они используют такие методы:

следование строгим правилам усиления защиты серверов и контроля приложений, что помогает в борьбе с программами-вымогателями;

установка исправлений с учётом возникающих рисков и повышение внимания к выявлению брешей в системах безопасности;

для малых и средних предприятий, ориентированных на облачные вычисления, – улучшение базовой защиты;

мониторинг сети с целью обеспечения большей прозрачности сред интернета вещей;

использование принципа нулевого доверия, чтобы защитить международные цепочки поставки;

усиление облачной безопасности с ориентацией на риски DevOps и использование наиболее эффективных методов борьбы с угрозами, выработанных отраслью;

внедрение расширенного обнаружения и реагирования (XDR), позволяющих выявлять атаки по всей сети». ***(Trend Micro представила прогноз развития ситуации в области кибербезопасности на 2022 г. // Компьютерное Обозрение (https://ko.com.ua/trend_micro_predstavila_svoj_prognoz_razvitiya_situacii_v_oblasti_kiberbezopasnosti_na_2022_g_139794). 21.12.2021).***

***

Сполучені Штати Америки

«Департамент охорони здоров'я та соціальних служб запустив новий веб-сайт ресурсу з кібербезпеки, який має на меті допомогти організаціям охорони здоров'я та державному сектору будь-яких розмірів і типів краще боротися з кіберзагрозами, що постійно розвиваються.

Новий веб-сайт програми HHS 405(d) Aligning Health Care Industry Security Approaches Program був розроблений спільно HHS та її цільовою групою 405(d).

Програма HHS 405(d) та її консультативна група з кібербезпеки були створені відповідно до розділу 405(d) Закону про кібербезпеку 2015 року.

До групи входять понад 150 експертів з галузі охорони здоров'я та федерального уряду. Його робота включає допомогу HHS у кращому узгодженні галузевих практик безпеки та розробці на основі консенсусу керівних принципів, процесів і методологій для зміцнення позиції сектору охорони здоров'я та громадського здоров'я проти кіберзагроз, йдеться у заяві HHS про новий веб-сайт 1 грудня.

Центральне сховище

Новий веб-сайт надає єдине сховище для суб'єктів охорони здоров'я та громадського здоров'я, щоб отримати доступ до низки ресурсів, документів з найкращою практикою, відео, інформаційних бюлетенів та інших інструментів, спрямованих на підвищення обізнаності, зміну поведінки та досягнення послідовності в пом'якшенні найбільш актуальних загроз кібербезпеці. у секторі, каже HHS.

«Новий веб-сайт програми 405(d) – це крок вперед для HHS, щоб допомогти створити стійкість до кібербезпеки в секторі охорони здоров'я та громадського здоров'я», – сказав Крістофер Боллерер, виконуючий обов'язки CISO HHS.

«Цей [веб-сайт] можуть використовувати організації абсолютно будь-якого розміру», – каже Ерік Декер, CISO Intermountain Health та один із керівників робочої групи HHS 405(d).

«Якщо ви невелика компанія, ми створили багато контенту саме для вас. Якщо ви велика організація, ми розробили комплексні методи та інструменти кібербезпеки, які допоможуть вам».

«Веб-сайт містить не лише методи кібербезпеки в галузі охорони здоров'я, а й багато інструментів», – каже Декер. Наприклад, робоча група розробила матрицю підпрактики загроз для малих, середніх і великих організацій, каже він.

«Ця матриця дозволяє організаціям вибирати загрози, які їх найбільше хвилюють, і легко спрямовувати їх до підпрактики практики кібербезпеки в галузі охорони здоров'я, яка безпосередньо пом'якшує ці загрози», — каже він.

Спільні зусилля

Програма HHS 405(d) і робота її цільової групи є частиною загальних зусиль індустрії охорони здоров'я щодо спільного покращення кіберготовності країни та реагування, каже колишній CIO з охорони здоров'я Девід Фінн, член робочої групи з кібербезпеки HHS і віце-президент Коледж менеджерів з управління інформацією в галузі охорони здоров'я та його Асоціація керівників у сфері управління інформацією в галузі охорони здоров'я, професійна організація CISO в галузі охорони здоров'я.

«Ця спільна робота між промисловістю та федеральним урядом спрямована на підвищення обізнаності, надання перевірених методів кібербезпеки та просування організацій до послідовності у пом'якшенні поточних, найбільш актуальних загроз кібербезпеці для сектора», – говорить він.

За його словами, новий веб-сайт відіграє важливу роль у цьому. «Коли робочий продукт розробляється, має сенс зробити його максимально доступним для сектора – легко знайти, сортувати та використовувати», – каже Фінн.

«Найголовніше, веб-сайт і його вміст не викладені технічним жаргоном і «кібермовністю», а розроблені для того, щоб їх розуміли всі, хто працює в галузі охорони здоров'я», — каже Фінн.

«Керівники IT, IT та їхні відповідні команди можуть виявити, що багато з цих спеціально розроблених ресурсів можуть бути корисними для них у поясненні кіберризиків, операційних та корпоративних ризиків для спеціалістів, які не працюють у сфері IT, або вони можуть використовувати це як частину своєї програми загальної обізнаності та навчання для їхню організацію", - каже він.

«Має і не має»

Серед своєї попередньої роботи, робоча група з кібербезпеки HHS опублікувала звіт про кібербезпеку в галузі охорони здоров'я для Конгресу в 2017 році, який містить понад 100 рекомендацій щодо того, як охорона здоров'я може краще протистояти загрозам кібербезпеки. Так само, як і створення робочої групи, цей звіт був передбачений Законом про кібербезпеку 2015.

Головна мета HHS та її робочої групи з кібербезпеки – покращити загальну безпеку секторів охорони здоров'я та громадського здоров'я, каже Фінн.

«З самого початку було зрозуміло, починаючи зі звіту Робочої групи з кібербезпеки, що з точки зору безпеки, охорона здоров'я функціонує у світі «має» і «не має», — каже він.

«Багато організацій мали ресурси, персонал і інвестували в безпеку, але більше організацій з різних причин не робили кібербезпеку пріоритетом». Фінн каже, що великі організації, у тому числі більші комерційні постачальники та академічні медичні системи, як правило, краще працюють у сфері безпеки, тоді як невеликі сільські лікарні, приватні лікарні та постачальники послуг безпеки часто відстають, каже він.

За словами Фінна, охорона здоров'я є одним із найбільш «гіперпов'язаних» секторів із 16 секторів критичної інфраструктури в США. «Будь-яка організація охорони здоров'я може бути безпечною лише настільки, наскільки її найслабша ланка – медичні практики спільно з лікарнями, платники – з усіма типами постачальників, невеликі сільські лікарні – з великими академічними медичними центрами і так далі.

«Важливо, щоб ми підвищили рівень безпеки, щоб кожен із нас міг стати наступною жертвою кібератаки». ***(Marianne Kolbasuk McGee. HHS Launches Repository for Health Sector Cybersecurity Help // Information Security Media Group, Corp. (https://www.inforisktoday.com/hhs-launches-repository-for-health-sector-cybersecurity-help-a-18086). 08.12.2021).***

***

«Що якби можна було б передбачити з вимірним ступенем точності, які дії уряд і приватний сектор США вживуть протягом наступного року, щоб посилити загальну позицію Сполучених Штатів у сфері кібербезпеки?

Щоб відповісти на це запитання, ми можемо запитати урядових чиновників, аналітиків розвідки чи співробітників Конгресу, що вони очікують побачити. Ми можемо проаналізувати галузеві тенденції або заяви провідних команд безпеки. Ми можемо провести опитування керівників інформаційної безпеки (CISO) та експертів з політики. Ми можемо розвести руками і стверджувати, що спекулювати на подібних питаннях, зрештою, марні.

Або ми можемо спробувати передбачити майбутнє більш прямо. Останніми роками прогнозування натовпу повільно проникло в простір прийняття рішень, оскільки воно дає можливість передбачити — із достатньою точністю — які події можуть статися в майбутньому. Хоча прогнозування натовпу все ще є дещо новим і часом навіть суперечливим, привабливість прогнозування натовпу зосереджується на вірі в те, що досить великі групи людей, які мають стимул ділитися очікуваннями щодо майбутніх подій, точно передбачають результати. Прогнозування натовпу може використовувати різні методи та бути спрямоване на різноманітні результати, але в кінцевому підсумку воно намагається поставити запитання та відповісти на них, які можуть мати глибокі наслідки для окремих людей, промисловості та установ.

Враховуючи низку гучних хакерських і кібератак останніх років, зараз може бути оптимальний момент для застосування цих методів у сфері кібербезпеки. Спираючись на нашу попередню роботу, тут ми спочатку надаємо аналіз того, як дефіцит знань про кібербезпеку шкодить результатам безпеки. Потім ми запитуємо, як прогнозування натовпу може застосовуватися до кібербезпеки і чого це може навчити зацікавлених сторін. Роблячи це, ми зосереджуємось на здатності платформи для прогнозування натовпу задавати питання, які є значущими та корисними для тих, хто приймає рішення. На завершення ми пропонуємо деякі способи формування цих питань, а також деякі приклади того, як може виглядати цей підхід.

Дефіцит знань у сфері кібербезпеки

Інформація щодо кібербезпеки недостатньо визначена. Про кібербезпеку ми багато чого не знаємо — окремі особи, промисловість, уряд. Аналогічно, є багато речей, про які можуть знати лише деякі люди, але які відносно невідомі більшості людей в екосистемі кібербезпеки.

Цей дефіцит знань ускладнює уряду США ефективну діагностику та пом’якшення поточних проблем кібербезпеки. Незнання перешкоджає здатності досліджувати сліпі зони, перевіряти припущення та розуміти як масштаби існуючих проблем, так і можливості їх вирішення.

Тож питання в тому, чи можна щось зробити з цим дефіцитом. Наприклад, деякі спостерігачі вважають, що кращі вимірювання та консолідація існуючих традиційних показників допоможуть подолати дефіцит, і виступають за створення «Бюро кіберстатистики».

Однак деякі аспекти цього дефіциту знань, ймовірно, виходять за межі того, що зараз можливо виміряти та кількісно оцінити. Залишається відкритим питання, чи корисна інформація, яку збирають спільноти з кібербезпеки та інформаційної безпеки. Також далеко не очевидно, що уряд навіть знає правильні запитання, які потрібно поставити, тобто питання з відповідями, які можуть діагностувати поточні

або неминучі інциденти з достатньою ясністю, щоб діяти на ці події, або політику та правила, які могли б найкращим чином пом'якшити їх. Так само важко визначити глибину та «розв'язність» цього дефіциту знань. Оскільки відносини — між акторами та цілями, людьми та машинами, технологіями та навколишнім середовищем — є динамічними і їх неможливо повністю моделювати, існують цілі розділи кібербезпеки, як і в багатьох інших сферах,

Іншими словами, імовірно, існує різниця між тим, що по суті є пізнаним питанням, і тим, що є практично пізнаним питанням. Перші могли б розглянути, чи можна успішно застосувати традиційну концепцію безпеки як «стримування» до кібербезпеки, тоді як друге може брати участь у тому, чи мають нинішні зусилля зі встановлення стримування вимірний вплив.

Тут ми зосереджуємось на практично пізнаних питаннях: речах, які можна було б знати, але не є — або недостатньо широко. Цей дефіцит виникає тому, що люди не роблять певних речей: ставлять правильні запитання, повністю використовують наявні дані, правильно інтерпретують дані, не діляться цими даними з тими, хто найбільше цього потребує.

Ми вважаємо, що існує величезна кількість наявної інформації про кібербезпеку, яку можна знайти, поділитися, проаналізувати та вжити заходів, і що одним із способів отримати цю відсутню інформацію є прогнозування натовпу.

Обіцянка прогнозування натовпу, що застосовується до кібербезпеки

У попередній публікації ми стверджували, що платформою для прогнозування натовпу варто було б визначити тенденції в кібербезпеці, які потім могли б використовуватися політиками, CISO, дослідниками безпеки та іншими особами, які приймають рішення. Наразі існує надійний ландшафт ринків прогнозів та інших варіантів прогнозування, а також чимало досліджень щодо того, які методи є найбільш ефективними та чому.

Але перш ніж ми спробуємо створити ринок і перевірити цю гіпотезу, ми повинні спочатку відповісти на питання ефективності. Чи варто того? Чи можна передбачити відповідні тенденції у сфері кібербезпеки та вразливості за допомогою прогнозування натовпу?

Наша мета тут дуже конкретна: ми хочемо переконатися, що ми оцінюємо тенденції, які полегшать практикам і політикам покращити кібербезпеку на фундаментальному рівні. Ця зосередженість лежить в основі не тільки типу запитань, які ми можемо поставити, але й того, як в кінцевому підсумку буде структурована платформа для прогнозування натовпу. Що ще важливіше, ці зусилля повинні допомогти нам вирішити, чи можуть ці зусилля сприяти кібербезпеці.

Хоча, можливо, і не зовсім традиційно, прогнозування натовпу для отримання інформації про кібербезпеку досліджувалося іншими. Ми маємо підстави вважати, що було зроблено кілька приватних — і часто засекречених — спроб, записи про які, як не дивно, важко визначити, і вони існують переважно в анекдотах та чутках.

Наша мета в цій публікації — дослідити — і відповісти — на питання корисності. Ми робимо висновок (дещо на наш подив), що зусилля принаймні можна перевірити на практиці. У супровідній статті, яка буде доступна в грудні від

R Street Institute, ми викладемо практичні аспекти того, як може працювати такий ринок. Взяті разом, ці дві частини свідчать про те, що варто провести бета-тестування гіпотези в реальному світі.

Що може зробити прогнозування натовпу для кібербезпеки?

Наша мета — створити платформу для прогнозування кібербезпеки, яка може підтримувати такі зусилля:

Платформа могла б об'єднувати інформацію, перетворюючи приватну інформацію на колективну суспільну мудрість і дозволяючи нам краще зрозуміти галузь. Ми очікуємо, що структура платформи стимулюватиме збір і аналіз нових джерел, систематично об'єднуватиме нову інформацію та уявлення, а також спонукатиме людей та компанії повністю використовувати дані, які вони, можливо, вже мають, але наразі не мають стимулу для обробки чи використання.

На платформі для прогнозування натовпу хороша інформація зростає, а погана – штрафується. Оскільки «шум» або інформаційне перевантаження є постійною проблемою як для уряду, так і для промисловості, платформа могла б зменшити необхідну кількість і тип джерел.

Платформа може забезпечити полігон для перевірки інформації. Наприклад, висновки, зроблені іншими методами, можна порівняти з результатами краудсорсингової платформи, щоб побачити, чи досягаються подібні результати різними методами. Аналогічно, після того, як подія сталася, має бути можливість перевірити точність усіх методів щодо реального результату події, визначити передбачувану здатність платформи та краще зрозуміти, як формуються очікування учасників платформи та, у свою чергу, формуйте відповіді на платформі. Це може допомогти нам відкинути або підтвердити інші ідеї щодо того, що насправді корисно.

Постановка правильних запитань

Теоретично платформа для прогнозування натовпу може поставити практично будь-яке питання, яке чітко визначене та обмежене, містить взаємовиключні можливі результати чи відповіді, обмежене у часі та доступне для пізнання. Але для оптимізації корисності для практиків і політиків, отримана інформація має бути надійною, застосовною та мати широку апертуру. Питання, які стосуються дрібниць, можуть бути цікаві для спостерігачів за ринком, але менш актуальні для політиків. Коротше кажучи, які питання слід задати?

Життєвий цикл хорошої моделі прогнозування натовпу кібербезпеки включає триетапний процес — ідентифікацію, створення та введення в дію. Нижче ми опишемо кожен крок докладніше.

Крок перший: Ідентифікація

Якщо передумова для платформи прогнозування генерує корисні прогнози кібербезпеки, будь-які запитання повинні мати більш широке значення для галузі кібербезпеки.

Це означає, що перший і найважливіший крок — вирішити, що в ідеалі повинна нам розповісти платформа. Відповідь на це питання буде залежати від того, яка інформація доступна для подачі на ринок і яку інформацію хочуть бачити в сукупності чи згенеровано ті, хто приймає рішення. На нашу думку, потенційні питання будуть мати широкий спектр: одні будуть надзвичайно технічними, інші

будуть орієнтовані на галузь, а інші будуть орієнтовані на політичні переваги та результати. Усі є законними зонами для запиту щодо домену.

Для того, щоб питання було релевантним, його відповідь в ідеалі повинна надавати інформацію про стан галузі у спосіб, який уряд або приватний сектор можуть використовувати або можуть використовувати в майбутньому.

Це можна застосувати на практиці, повернувшись до початкового питання цієї публікації: які дії вжитимуть уряд США та приватний сектор протягом наступного року, щоб посилити загальну позицію Сполучених Штатів щодо кібербезпеки?

Це не те питання, яке можна поставити перед платформою прогнозування: воно занадто розпливчасте й відкрите, незважаючи на його цінність як питання політики. Однак на наступному етапі циклу можна скоротитися до більш реалізованого рівня запитань.

Наразі важливо те, що це питання високого рівня, на яке ми в принципі хочемо отримати відповідь: питання, яке, на нашу думку, має пряму користь не тільки для тих, хто приймає рішення, але також для акціонерів, CISO, юридичних та фінансових аналітиків. однаково. Справедливо сказати, що посилення позиції безпеки повинно, начебто, ускладнити скомпрометацію суб'єкта під час операції з викупу, а також ускладнити вимагання викупу навіть у разі компромісу. Тобто це питання може бути актуальним для тих, хто відстежує припливи та відпливи кризи програм-вимагачів. Аналогічно, він може бути корисним для регуляторів, аналітиків із кіберстрахування, спеціалістів із дотримання вимог, приватних охоронних компаній тощо.

Крок другий: генерація

Це простір, в якому працює платформа. Тут зосереджено увагу на наступних питаннях, визначених на першому етапі, відповіді на які є взаємовиключними і швидко перевіряються?

На деякі питання легко відповісти і легко довести. Деякі ні. Наприклад, в той час як можна відповісти на питання про те, розвідувальне співтовариство США готові офіційно віднести на SolarWinds зламувати російському уряду, це далеко інше питання, ніж росіяни зробили зробити SolarWinds зламати.

Далі: Які питання не слід задавати?

Платформа повинна залишатися на досить високому рівні, оскільки занадто велика конкретність може бути небезпечною. Якщо платформа надто глибоко занурюється в дослідження конкретних продуктів або ринків, це може стимулювати орієнтацію на організації, які вважаються слабкішими учасниками ринку — по суті, низькорослим плодом для злочинних кібер-акторів. Коротше кажучи, запитання типу «Чи стане публічно відомим, що системи невеликої компанії X були заблоковані внаслідок атаки програм-вимагачів у найближчі 12 місяців?» слід уникати. (Ця проблема стосується не лише кібербезпеки. На ринках політичних прогнозів цей тип виділення також викликає занепокоєння — наприклад, запит про дату смерті видатної знаменитості чи політика може перетворитися на ринок вбивств.)

Другий крок — структурувати відповідні питання з кібербезпеки на першому етапі, щоб їх можна було задавати на платформі. На цьому етапі учасники платформи можуть зробити свої прогнози.

Ось два приклади (з багатьох можливостей) відповідно структурованих питань, які б відповідали нашим попереднім інтересам до посилення заходів кібербезпеки:

Чи вирішить страхова компанія, зареєстрована в США, припинити обов'язкове покриття платежів із програмним забезпеченням-вимагачем до 31 грудня 2022 року?

Чи ухвалить уряд США закон «Знай свого клієнта» щодо криптовалют до 31 липня 2022 року?

Ці питання чітко визначені та охоплені, і, таким чином, належать до того типу, який можна поставити платформі для прогнозування натовпу. Вони також мають відношення до кібербезпеки, можуть бути перевірені вчасно, і не (здається) підіймають червоні прапорці як питання, які не слід задавати.

Ми визнаємо, що це зразкові запитання, і що нам потрібно буде чіткіше визначити, які події можуть спровокувати вирішення питання. Наприклад, нам потрібно було б уточнити особливості закону «Знай свого клієнта», додавши деякі нюанси та виключивши інші. Зверніть увагу, наприклад, на дрібний шрифт у цьому існуючому питанні про платформу.

Крок третій: Операціоналізація

Останній крок у цьому циклі знань — хоча, можливо, і не останній у хронологічному відношенні — полягає в тому, щоб переконатися, що зусилля, які витрачаються, дають значущі, точні та корисні результати, і що ці результати є придатними та доступними для тих, хто приймає рішення.

Розглянемо початкове питання цієї посади, яке є високопоставленим і орієнтованим на політику: чи вживуть уряд і приватний сектор США протягом наступного року заходів для посилення позиції кібербезпеки США? Як уже згадувалося раніше, здається надійним припущенням стверджувати, що посилення позиції кібербезпеки зробить компанії більш несприйнятливими до операцій із програмним забезпеченням-вимагачем і, таким чином, призведе до зменшення кризи програм-вимагачів, або створить нові спроби компромісу з боку учасників програм-вимагачів. Окремі запитання, поставлені на другому кроці, мають бути — якщо їх поєднати — вказувати на ширшу тенденцію щодо кіберзахисту США, здатність зацікавлених сторін координувати та працювати разом, а також нові вимоги чи виклики для навігації.

Але на індивідуальному рівні ми також очікуємо, що питання будуть мати цінність. Скажімо, ми поставили вищезазначене запитання: чи вирішить страхова компанія, зареєстрована в США, припинити обов'язкове покриття платежів із програмним забезпеченням-вимагачем до 31 грудня 2022 року?

Що ми особисто можемо зробити з позиції натовпу?

Зрозуміло, завжди існує ризик у приписуванні причинно-наслідкового зв'язку, і це технічно не входить до компетенції самої платформи прогнозування (крок другий) — тобто, як інформація використовується, а не як вона створюється. Тим не менш, імовірно, що функціональна платформа прогнозування не лише

збирає інформацію, але й пропонує метод дослідження припущень та причинно-наслідкових зв'язків. З цієї причини ми намалювали нижче, як можна обробляти інформацію, отриману з ринку. Під «сильними» та «слабкими» ми маємо на увазі ймовірність ймовірності, визначену більшістю респондентів; Сильний означає високу ймовірність, а слабкий означає низьку ймовірність:

Про те, що може сказати нам «сильне так»: збитки перевищують те, що готовий понести ринок, що платить ставки, і тому окремі страхувальники, швидше за все, залишаться самі по собі, коли страховики відмовляться.

Про що може сказати нам «слабке так»: вибір страховика став вирішальним у плані пом'якшення ризиків будь-якої компанії, оскільки страховики явно не мають повноцінного впливу на результати.

Про що може нам сказати «амбівалентність»: дивитися, як яструб.

Про те, що може сказати нам «слабке ні»: що припинена програма страхування є провалом керівництва цього страховика, а не провалом галузі.

Яке «рішуче ні» може сказати нам: ця програма-викуп досить поширена, що жодна страхова компанія не наважиться припинити її покриття, якщо вони не планують повністю згорнути свій портфель кіберстрахування.

Однак, зрештою, цінність платформи, яку ми прагнемо пропагувати, полягає в її корисності для осіб, які приймають рішення, включаючи їхню здатність довіряти платформі, їхню власну відкритість щодо інформації, отриманої за допомогою методів прогнозування натовпу, та їхню здатність сприймати інформацію та робити висновки та висновки. Ми віримо, що, хоча проста відповідь «так» або «ні» на запитання іноді може бути цінною — наприклад, чи переможе кандидат XX на президентських виборах 2024 року, — здатність осіб, які приймають рішення, використовувати інформацію в кінцевому підсумку залежатиме від їхніх власних процесів. для розгляду інформації та розподілу ресурсів.» ***(Mary Brooks, Paul Rosenzweig. How Crowd-Forecasting Might Decrease the Cybersecurity Knowledge Deficit // The Lawfare Institute (https://www.lawfareblog.com/how-crowd-forecasting-might-decrease-cybersecurity-knowledge-deficit). 06.12.2021).***

***

«Інститут цифрової трансформації C3.ai (DTI) запросив науковців, дослідників та розробників програмного забезпечення подати пропозиції щодо розвитку кібербезпеки за допомогою штучного інтелекту (ШІ). C3.ai DTI — це спільний дослідницький консорціум, яким керують Університет Іллінойсу в Урбана-Шампейн та Каліфорнійський університет Берклі.

Серед інших відомих партнерів – Microsoft, Університет Карнегі-Меллона, Массачусетський технологічний інститут (MIT), Національна лабораторія Лоуренса Берклі, Національний центр суперкомп'ютерних додатків, Прінстонський університет та Чиказький університет.

«Кібербезпека є екзистенційною проблемою», – сказав Томас М. Зібель, голова та генеральний директор C3 AI, у повідомленні.

«Ми збираємо найкращих розумів на планеті для розробки інноваційного AI, щоб досягти поетапного покращення в захисті систем IT, OT та критичної інфраструктури».

C3.ai DTI збирає пропозиції та вручить нагороди за дослідження за такими темами:

Методи штучного інтелекту для виявлення раніше невідомих шкідливих програм, програм-вимагачів і вразливостей нульового дня, що дозволяє ізолювати та нейтралізувати

Мережні та системні сканери з підтримкою штучного інтелекту, які можуть безперервно шукати та ідентифікувати механізми постійного доступу (бекдори), ботів, набори інструментів віддаленого доступу (RATS), щабельники та троянські програми

Криміналістична експертиза ШІ та методи атрибуції для виявлення джерел атак

Методи штучного інтелекту для автоматизації змодельованих змагальних атак для виявлення вразливостей системи та мережі

Методи штучного інтелекту для точного визначення та нейтралізації фішингових атак

Методи управління змінами, щоб запобігти зброї невинних інсайдерів

Методи штучного інтелекту для виявлення наявності розширених постійних загроз та інсайдерських загроз

Мережні та/або системні сканери з підтримкою штучного інтелекту, які отримують доступ та постійно оцінюють рівні безпеки системи

Методи штучного інтелекту, можливо в навчанні під наглядом або без нагляду, щоб забезпечити раннє виявлення системних та/або мережевих аномалій, які можуть свідчити про несанкціонований доступ, відмову в обслуговуванні або вилучення даних

Техніки та методи, що дозволяють розробляти алгоритми ШІ, стійкі до атак суперника

Методи штучного інтелекту для виявлення ризику концентрації в ланцюжку поставок програмного забезпечення та комп'ютерів

Управління змінами, щоб трансформувати організаційну поведінку, щоб реалізувати найкращі практики кібергігієни

Техніки реагування на атаки на організаційному та суспільному рівні

Кінцевий термін подання пропозицій – 7 лютого 2022 року. Переможці будуть оголошені в березні 2022 року та можуть взяти участь у щорічному симпозіумі C3.ai DTI Research, який також відбудеться у березні.

«Ми прагнемо розробити методи штучного інтелекту для виявлення та нейтралізації зловмисного програмного забезпечення, програм-вимагачів, фішингових атак і запобігання зброї невинних інсайдерів», – пояснив у повідомленні Р. Срікант, співдиректор C3.ai DTI.

Атаки на критично важливу інфраструктуру США за останні кілька років почастішали, що вказує на невідкладну необхідність захисту критично важливих структур. Кібератака на колоніальний трубопровід у травні 2021 року змусила президента Байдена видати указ про покращення кібербезпеки країни.

Тим часом суб'єкти загрози стають сміливішими щодо своїх цілей і методів атаки. Аналіз Інституту CyberPeace показав, що 12 груп програм- вимагачів виділили медичні організації за останні 18 місяців, незважаючи на те, що вони чітко заявляли, що не будуть орієнтуватися на цей сектор.

Для боротьби зі зростаючими кіберзагрозами нещодавнє дослідження The Economist Intelligence Unit досліджувало перспективні можливості використання інструментів штучного інтелекту для посилення зусиль із кібербезпеки.

«Інтегруючи технології штучного інтелекту з програмами та системами кібербезпеки, підприємства різних секторів мають неоціненну можливість подолати один із найскладніших і потенційно шкідливих факторів ризику, з якими сьогодні стикаються організації», – йдеться у звіті.

C3.ai DTI надасть до 10 мільйонів доларів грошової винагороди для фінансування досліджень, а також доступ до ресурсів суперкомп'ютерів, хмарних обчислень і програмного забезпечення для штучного інтелекту від Microsoft і C3.ai». ***(Jill McKeon. Industry Experts Team Up to Advance Cybersecurity With AI // TechTarget, Inc. (https://healthitsecurity.com/news/industry-experts-team-up-to-advance-cybersecurity-with-ai). 28.12.2021).***

***

«Закон Таиланда о кибербезопасности 2562 б.э. (2019) (CSA) вступил в силу 28 мая 2019 года. CSA налагает ряд обязательств на государственные и частные организации, которые считаются «организациями критически важной информационной инфраструктуры» (OCII), т. е. Организацией публичные или частные, предоставляющие услуги «Критически важной информационной инфраструктуры» (CII).

Вплоть до недавнего времени неясность в отношении того, считался ли поставщик услуг OCII, оставалась актуальной и требовала дополнительной ясности. В попытке внести ясность, 23 августа 2021 года регулирующий орган CSA (то есть Национальный комитет по кибербезопасности, «NCC») выпустил «Уведомление» 1, в котором систематически классифицируются определенные типы бизнеса по поставщикам услуг CII и делегируются надзорные функции. полномочия различным регулирующим органам («контролирующие организации»).

Список избранных услуг CII в соответствии с законодательством Таиланда можно найти здесь.

Ключевые обязательства OCII в соответствии с CSA заключаются в следующем:

Соблюдение Кодекса практики CSA и стандартных рамок для обеспечения кибербезопасности.

Проверка операций на соответствие минимальным стандартам кибербезопасности, установленным соответствующей надзорной организацией.

Проведение ежегодной оценки рисков по теме «Поддержание кибербезопасности». Эти оценки рисков должны проводиться аудитором информационной безопасности OCII, внутренним аудитором или внешним независимым органом, а результаты должны быть представлены в офис NCC.

Узнав, что это является предметом «киберугрозы», OCII должен сообщить об этом в офис NCC и соответствующую надзорную организацию. Затем OCII должен провести соответствующие расследования и проверки в отношении «киберугрозы».

Обязательства, налагаемые на OCII, в некотором роде совпадают с обязательствами других юрисдикций, таких как Сингапур и Китай, как показано здесь.

OCII также подпадают под юрисдикцию Управления NCC в случае «киберугрозы», которая достигает «критического уровня». Среди других обязательств в контексте «киберугроз», OCII должны будут сотрудничать во время рейда на рассвете, отвечать на запросы информации, а также отвечать на повестки в суд для получения информации, доказательств или свидетелей.

Несоблюдение OCII обязательств по CSA приведет к штрафам. Однако невыполнение приказов, отданных Управлением NCC, может привести к штрафу и / или тюремному заключению. Примечательно, что правонарушения в соответствии с CSA могут распространяться на директора и / или лицо, ответственное за деятельность организации, если установлено, что совершение правонарушения явилось результатом приказа или бездействия такого лица (лиц).

Кроме того, частные организации, подверженные «киберугрозе», приводящей к утечке данных, могут быть подвергнуты обязательствам по отчетности в соответствии с Законом Таиланда о защите личных данных 2562 (2019 г.), который должен вступить в силу 31 мая 2022 г., если такая организация считаться «Контроллером данных» в соответствии с этим законом». ***(Santipap Dumprapai, Prin Laomanutsak, Sammy Fang, Rishikeesh Wijaya. Are you Subject to Thailand's Cyber Security Laws? Know Your Rights and Obligations // DLA Piper (https://www.dlapiper.com/en/us/insights/publications/2021/12/seachange-issue-ii-december-2021/are-you-subject-to-thailands-cyber-security-laws-know-your-rights-and-obligations/). 17.12.2021).***

***

«В понедельник президент Джо Байден подписал Закон о разрешении на национальную оборону от 2022 года, который кодифицирует подход к кибербезопасности, который зависит от решений организаций частного сектора по защите большей части критически важной инфраструктуры страны.

NDAA стало законодательным инструментом для усилий по управлению федеральным правительством в целом и по регулированию частного сектора по вопросам кибербезопасности.

Что касается правительства, закон требует, чтобы Агентство по кибербезопасности и безопасности инфраструктуры раз в два года обновляло план реагирования на инциденты и консультировалось с отраслевыми агентствами и частным сектором при разработке программы учений для оценки ее эффективности.

По словам сенатора Мэгги Хассан, DN.H. Он также учреждает программу грантов в Министерстве внутренней безопасности для развития сотрудничества в

области технологий кибербезопасности между государственными и частными организациями в США и Израиле.

Законодатели также подчеркнули включение положений, кодифицирующих существующие государственно-частные партнерства в CISA, которые нацелены на обеспечение непрерывного мониторинга систем промышленного контроля - усилие, известное как программа CyberSentry, - и на разработку руководящих принципов «знай своего клиента» для таких компаний, как облачные и другие услуги. провайдеры, составляющие «интернет-экосистему». Такие компании описываются как участники совместного сотрудничества CISA в области киберзащиты.

Но все положения полагаются на добровольное участие отрасли, которая владеет и управляет подавляющим большинством критически важной инфраструктуры страны. Несмотря на призывы обеих партий после массовых взломов SolarWinds, Microsoft Exchange, Colonial Pipeline и других взломов, NDAA прошло через Палату представителей без обязательных требований к отчетности об инцидентах для частного сектора.

«NDAA предпринимает важные шаги в области кибербезопасности, в частности, для содействия укреплению партнерских отношений между государственным и частным секторами во всем правительстве», - заявила Лора Брент, старший научный сотрудник Центра новой американской безопасности, после того, как Сенат принял тот же закон неделю спустя. «Однако, учитывая масштаб киберпроблемы, NDAA не хватает необходимой постоянной срочности. Что наиболее важно, не были включены требования даже в отношении некоторых отраслевых отчетов о киберинцидентах и платежах с использованием программ-вымогателей правительству, несмотря на то, что они были ключевыми для правительства в получении более полного представления о киберугрозах».

Законодательство, требующее отчетности, также получило значительную поддержку в отрасли после того, как компании успешно обратились к законодателям с просьбой расширить окно для сообщения об инцидентах в CISA и исключить финансовые санкции в качестве правоприменительного механизма.

22 декабря во время телефонного разговора с репортерами конгрессмен Майк Галлахер, штат Висконсин, и сенатор Ангус Кинг, штат Айленд, штат Мэн - сопредседатели закрытой Комиссии по киберпространству по солярию, которой удалось создать должность национального кибердиректора. прошлогодний NDAA - сказал, что непреодолимым препятствием является то, что руководство комитета по строгому контролю предпочитает сохранять свою юрисдикцию.

В прошлом году «нам нужно было получить 180 разрешений от обеих сторон комитетов и подкомитетов обеих палат Конгресса, что дает вам представление о том, насколько сложен этот процесс», - сказал Кинг.

«В такой ситуации у вас просто не хватает времени на часах», - сказал Галлахер. Законодатели заявили, что внимание к кибербезопасности после громких атак в этом году помогло и навредило делу. Но оба согласились, что в целом это хорошо.

Эти инциденты «дали понять всем, что то, о чем мы здесь говорим, не является академической проблемой, абстрактной проблемой, а очень ясной и

актуальной проблемой», - сказал Кинг. «Я думаю, что это помогло нам в целом. Обратной стороной, если вы хотите это назвать, является то, что у вас действительно больше людей, которые вовлечены, и больше людей, которые хотят, чтобы с ними консультировались, хотели, чтобы с ними работали, хотели участвовать в процессе. Но, знаете, я возьму это. Я думаю, что это компромисс, но я думаю, что это нормальный компромисс».

Галлахер с оптимизмом смотрел на перспективы принятия более амбициозного законодательства о кибербезопасности в следующем году.

«Даже там, где мы не смогли получить что-то в NDAA, мы действительно добились большого прогресса в устранении определенных юрисдикционных ограничений комитетов и взаимодействии с нашими коллегами, которые, возможно, просто не отслеживали законодательство и как бы рефлексивно выступали против него», он сказал». ***(Mariam Baksh. Biden Signs NDAA Relying on Voluntary Private-Sector Cybersecurity Collaboration // Nextgov (https://www.nextgov.com/cybersecurity/2021/12/biden-signs-ndaa-relying-voluntary-private-sector-cybersecurity-collaboration/360217/). 28.12.2021).***

***

Країни ЄС та Великобританія

«Сполучене Королівство оприлюднило нову Національну кіберстратегію, яка, за її словами, забезпечить підхід до кібербезпеки для всього суспільства, що зміцнить позиції Великобританії як глобальної кібердержави.

Плани, викладені в стратегії для індустрії кібербезпеки Великобританії, яка в минулому році повідомила про доходи в 8,9 мільярдів фунтів стерлінгів, будуть підтримані інвестиціями в розмірі 2,6 мільярда фунтів стерлінгів, оголошених у цьогорічному огляді витрат, йдеться в повідомленні.

У стратегії є конкретні цілі та визначені результати, які мають бути досягнуті до 2025 року, але це не повторення наказу президента США Байдена з кібербезпеки, в якому детально викладено графік виконання завдань. Це скоріше стратегічне визначення того, як будуть вживатися постійні кроки, щоб максимізувати безпеку та відкритість використання Інтернету в цілому, і для Великобританії зокрема.

Визнаючи, що політичні проблеми в кіберпросторі не є виключно технологічними, у доповіді кіберсфера описується як створене людьми середовище, яке посилює людську поведінку, але впливає на фізичний світ.

Кіберпростір належить і керується приватними компаніями, урядами, некомерційними організаціями, окремими громадянами і навіть злочинцями, і уряди повинні співпрацювати з партнерами, щоб отримати владу в цій сфері та здійснити її.

Поряд з державами-супротивниками, деякі з яких мають технологічні лідери в деяких областях, а також зростаючий потенціал злочинних груп, зростаючі сфери занепокоєння, визначені у звіті, включали застарілі IT-системи, вразливості

ланцюга поставок, нестачу фахівців з кібербезпеки та відсутність комерційних стимулів для інвестування. у сфері кібербезпеки.

Відповідно, уряд заявляє, що прагне включити більше різноманітності в робочу силу, підвищити рівень кібер-сектору в усіх регіонах Великобританії, розширити наступальні та оборонні кіберспроможності та поставити пріоритет кібербезпеки на робочому місці, у залах засідань і цифрових ланцюгах поставок».

Стратегія «викладає чітке бачення розвитку кібер-експертизи в усіх частинах країни, посилення наших наступальних і оборонних можливостей і забезпечення того, щоб все суспільство відігравало свою роль у кібер-майбутньому Великобританії, і забезпечується рекордним фінансуванням», — сказав Стів. Барклай, канцлер герцогства Ланкастер і міністр кабінету міністрів, йдеться у заяві. За його словами, у цій стратегії уряд робить більше для захисту громадян і компаній Великобританії, а також її міжнародних партнерів, допомагаючи реалізувати своє бачення кіберпростору як надійного та стійкого місця для процвітання людей і бізнесу».

Зони фокусування

Навчання

Онлайн-платформа для навчання під назвою Cyber Explorers навчатиме молодих людей кібернавичкам у класах, йдеться у заяві. У ньому також сказано, що нова Королівська хартія Ради кібербезпеки Великобританії була схвалена, щоб «покращити кібер-кар'єру та привести кібер-працівників у відповідність з іншими професійними професіями, як-от інженерія».

Програма також буде спрямована на підвищення різноманітності за допомогою нової «схеми для дорослих, яка забезпечить людям різного походження доступ до цих висококваліфікованих, високопріоритетних робіт».

Кабінет міністрів Великобританії повідомляє ISMG, що безкоштовний курс Cyber Explorers призначений для дітей віком від 11 до 14 років, тоді як Королівська хартія не є програмою, а є визнанням «експертизу та авторитету Ради кібербезпеки Великобританії, яка є працювати над удосконаленням професії кібербезпеки».

«Статус ради як професійного авторитету допомагає привести професію кібербезпеки у відповідність із подібними професійними професіями, такими як інженер, і доповнює роль національного технічного органу, NCSC», – йдеться у повідомленні.

Подробиці про програму, плани впровадження тренінгів та схеми різноманітності будуть оприлюднені в Новому році, повідомили ISMG в Кабінеті міністрів.

Фінансові інвестиції

Уряд інвестує нерозкриту суму в рамках схеми Cyber Runway, яка, як стверджується в заяві, допоможе «107 інноваторам розвивати та розвивати свій бізнес, причому більшість компаній-членів за межами Лондона та Південного Сходу, 45% очолюваних жінками та 52% керують засновниками з чорношкірих та національних меншин».

«Фінансування цих програм зростання та підвищення кваліфікації буде переорієнтоване від великих ініціатив, які часто базуються в Лондоні, на

регіональну модель, що означатиме більше робочих місць та кращі можливості для людей по всій Великобританії», – йдеться у заяві.

Стратегія також передбачає:

Зміцнити правоохоронні органи та значно збільшити фінансування для боротьби з кіберзлочинністю;

Створюйте більш інтегровані та постійні кампанії, щоб порушити та стримувати супротивників;

Збільшити інвестиції в Національні кіберсили, військовий підрозділ, який базується в Самлсбері в Ланкаширі, який забезпечує наступальний потенціал Великобританії;

Розширити дослідницькі можливості Національного центру кібербезпеки Національного центру кібербезпеки, включаючи новий центр прикладних досліджень у Манчестері;

Впровадити законопроект про безпеку продуктів і телекомунікаційну інфраструктуру, щоб забезпечити дотримання мінімальних стандартів безпеки у всіх нових споживчих розумних продуктах;

Інвестуйте в кібербезпеку державного сектору.

Директор GCHQ Джеремі Флемінг каже, що стратегія «визнає життєво важливу роль приватного сектору у забезпеченні кібермайбутнього Великобританії через створення нової Національної кіберконсультативної ради», до складу якої входять керівники приватного та третього секторів, щоб кинути виклик, підтримати та інформувати про підхід уряду.

Паралельно уряд також створить Національну лабораторію безпеки операційних технологій, щоб об’єднати уряд, промисловість та наукові кола, щоб «переконатися, що економіка Великобританії побудована на найвищому рівні кіберстійкості», – каже він.

Уникнення ризику постачання технологій

У документі сказано: «Там, де Велика Британія має потенціал для встановлення лідируючої позиції або забезпечення конкурентної переваги в ключових сферах кібертехнологій, або де залежність від джерел постачання, що не є союзниками, створює неприйнятні ризики для безпеки, ми будемо прагнути розвивати нашу внутрішню промислова база», що має як дійсно суверенні можливості, так і співпрацю з міжнародними партнерами залежно від обставин.

Філ Робінсон, головний консультант і засновник консалтингової компанії з кібербезпеки Prism Infosec, говорить ISMG: «Документ передбачає, що суверенні можливості тепер будуть у центрі уваги, тому ми можемо очікувати, що залежність від постачальників або технологій за межами Великобританії, які не поділяють наші цінності, зменшиться.» У документі говориться, що загрози постійно «виходять від Росії та Китаю». Тож Робінсон пропонує: «Можна сказати, що будь-які іноземні інвестиції в інфраструктуру Великобританії будуть перевірятися».

«Усі організації, як у державному, так і в приватному секторі, повинні враховувати ризики своїх ланцюгів поставок, щоб включити ризики своїх цифрових можливостей», — каже Грант Шнайдер, колишній федеральний офіцер із інформаційної безпеки США та старший член Ради національної безпеки Білого дому. директора з політики кібербезпеки.

Шнайдер, нині старший директор із служб кібербезпеки у Venable та глобальний учасник контенту ISMG, сприяв створення в уряді США повноважень та можливостей для видалення або виключення продуктів, які становлять занадто великий ризик. Він каже: «Не дивно, що Сполучене Королівство стверджує, що вони також прийматимуть рішення на основі ризику щодо постачальників технологій, на яких вони покладаються. Я давно підтримую, що США повинні працювати на міжнародному рівні, щоб забезпечити наявність надійного ланцюга поставок для підтримки наших цифрових екосистем».

Усе суспільство працює разом

Нова стратегія кібербезпеки продовжує спиратися на основи, встановлені попередніми стратегіями, каже Браян Хонан, експерт з безпеки з Ірландії, Хонан каже, що стратегія детально розглянута, на відміну від багатьох стратегій кіберстратегій на корпоративному та національному рівнях, які окреслюють цілі, але не відповідають. скажіть, як вони будуть досягнуті.

За його словами, пропонована взаємодія з промисловістю та науковими колами вітається, оскільки «кібербезпека — це те, над чим усі частини суспільства повинні працювати разом». Він додає: «Приємно бачити мету охопити людей з різним походженням, оскільки вони можуть допомогти не тільки подолати розрив у навичках і надати більше ресурсів для забезпечення безпеки Великобританії, але вони також можуть залучити нові та різні ідеї, які можуть допомогти досягти цих цілей».

Повторюючи заяви Хонана, Карла Бейкер, старший директор з урядових питань у фірмі з кібербезпеки Palo Alto Networks, розповідає ISMG, що нова Національна кіберстратегія знаменує собою значний крок у тому, як уряд наближається до безпеки критичних технологій і цифрового середовища. «Ми підтримуємо підхід до безпеки на всій території країни, включаючи цілі кращого розуміння ландшафту загроз і розробки політичних заходів, які підвищують стійкість і захищають технологічну екосистему Великобританії», — каже вона.

Роль уряду

Сай Хук, директор Лондонського офісу швидкого розвитку кібербезпеки та керівник інноваційного відділу Plexal, який здійснює чотири урядові програми кіберінновацій, включаючи Cyber Runway, каже: «Нова Національна кіберстратегія визнає, що горизонтальні технологічні галузі, такі як кібер, зі своїми потенціал впливати та формувати структуру того, як наше суспільство взаємодіє та взаємодіє з технологіями, вимагає цілеспрямованого державного втручання».

«Ця стратегія ставить кібербезпеку в основу всіх майбутніх національних рішень щодо нових технологій, з особливим акцентом на.. впровадженні безпеки в наступне покоління проривних технологій, які формуватимуть наш цифровий та фізичний світ».

Для Джона Бамбенека, головного шукача загроз у компанії Netenrich, що займається цифровими IT та безпекою, найбільшою проблемою в стратегії є те, що не вистачає фахівців з кібербезпеки. «Ви можете вимагати багато стандартів, але вам або потрібні експерти, щоб запровадити ці стандарти у виробничий процес, або вам потрібні готові рамки, які дозволяють компаніям просто впроваджувати вже загартовані системи», — каже він ISMG.

Бамбенек також каже, що геополітична реальність, яка лежить в основі, не була розглянута. «Існують юрисдикції, які дивляться в інший бік, коли злочинці здичавіють. Ми можемо ідентифікувати всіх кіберзлочинців у світі, але якщо ми не зможемо нічого зробити, окрім розміщення їх зображення на веб-сайті, це не сильно зміниться». ***(Rashmi Ramesh. New UK Cyber Strategy Adopts Whole-of-Society Approach // Information Security Media Group, Corp. (https://www.govinfosecurity.com/new-uk-cyber-strategy-adopts-whole-of-society-approach-a-18132). 16.12.2021).***

***

«За даними Федерального управління інформаційної безпеки Німеччини (BSI), країна стикається з серйозною і зростаючою загрозою, оскільки суспільство стає все більш цифровим, а злочинці — більш витонченими. BSI заявив, що рівень загрози досяг червоного рівня тривоги.

Підвищився рівень загрози

BSI опублікував щорічний звіт «Стан IT-безпеки в Німеччині у 2021 році». У ньому підкреслюється, що найбільші ризики виникають від атак зловмисного програмного забезпечення та програм-вимагачів. Фактично з червня 2020 року по кінець травня 2021 року агентство виявило 144 мільйони нових варіантів шкідливих програм, що на 22% більше за рік. У лютому 2021 року BSI виявив 553 000 варіантів шкідливих програм за один день — новий рекорд. У звіті зазначається, що згодом загальний рівень загрози, створюваної зловмисними комп'ютерними атаками, підвищився з «напруженого» у 2020 році до «напруженого до критичного».

Причиною такого підвищеного рівня пильності є зростання професіоналізму кіберзлочинців у поєднанні з мережевим складом суспільства.

«Суттєве збільшення віддаленої роботи призвело до суттєвого зростання поверхні атаки з точки зору взаємозв'язку послуг та обладнання, що надається та використовується. Таким чином, ця тенденція сприяла можливому використанню недоліків безпеки для кіберзлочинних кампаній», – йдеться у спільній доповіді французького ANSSI та німецького BSI.

Пандемія коронавірусу посилила тенденцію зростання кіберзлочинності, оскільки все більше бізнес-службовців та державних службовців працюють віддалено. У звіті чітко вказується, що кібератаки не тільки стали більш поширеними, але й стали дорожчими. Bitkom, асоціація IT-індустрії, підрахувала, що втрати від шантажу та відключення системи з 2019 року зросли на 358%.

За даними BSI, злочинці працюють не тільки на себе. Вони також продають свої послуги в темній мережі. На цьому шляху вони стали більш витонченими у своєму підході, використовуючи багаторівневі стратегії атак, які раніше спостерігалися у випадках державного шпигунства. Наприклад, BSI відзначив метод, за допомогою якого зловмисники домовляються про викуп у жертви і натомість шукають дані.

Використання так званих «сторінок витоку» було одним із таких прикладів, коли зловмисники публікували вкрадені дані, щоб вимагати від жертв викуп. Агентство проілюструвало підхід шантажу, вказавши на випадок зламаного

кабінету приватного психолога, в якому зловмисники чинили тиск не лише на власника практики, а й на їхніх пацієнтів.

Загроза для критичної інфраструктури

За даними BSI, «атаки зачіпають області, які є фундаментальними для нашого суспільства, як-от енергетика та інфраструктура охорони здоров'я». Далі у звіті BSI зазначається, що «інформаційній безпеці необхідно надати значно більше значення і стати основою для всіх проектів оцифрування».

Ті самі занепокоєння висловлюються в спільному звіті ANSSI та BSI. Обидва агентства написали, що цифровізація виробничих процесів, що лежать в основі основної діяльності підприємства, через підключення операційних технологій (OT), буде нести ризики в найближчому майбутньому. Ці системи OT зазвичай мають тривалий життєвий цикл і дорогі. Вони не змінюються і не оновлюються на регулярній основі. Тому більшість сучасних систем OT були встановлені в той час, коли IT-безпека не була визнана життєво важливим фактором для роботи систем OT.

В іншому звіті Європолу, Internet Organized Crime Threat Assessment (IOCTA) 2020, зазначено, що програмне забезпечення-вимагач становить значну непряму загрозу для компаній та організацій у Європі, включаючи критично важливу інфраструктуру, націлюючись на ланцюги поставок і сторонніх постачальників послуг.

Окрім програм-вимагачів, європейське правоохоронне агентство повідомило, що зловмисне програмне забезпечення в більш широкому сенсі широко присутнє у справах про кіберзлочини. Злочинці перетворили деякі традиційні банківські трояни в більш просунуті модульні шкідливі програми, щоб охопити ширший діапазон функціональних можливостей. Ці розвинені форми модульного зловмисного програмного забезпечення є основною загрозою в ЄС, особливо тому, що їх адаптивний і розширюваний характер робить їх все більш складними для ефективної боротьби.

Німеччина ухвалила стратегію кібербезпеки

У відповідь на зростання загрози передових кібератак Федеральний уряд Німеччини прийняв Стратегію кібербезпеки Німеччини до 2021 року. Стратегія містить чотири основні рекомендації:

Встановити кібербезпеку як спільне завдання держави, бізнесу, суспільства та науки.

Зміцнити цифровий суверенітет держави, бізнесу, науки та суспільства.

Забезпечити безпечний розвиток цифровізації.

Зробіть цілі вимірюваними та прозорими…» ***(JEANNINE BALSIGER. State of Cybersecurity in Germany in 2021 // Tripwire (https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/state-of-cybersecurity-in-germany-in-2021/). 07.12.2021).***

***

«3 декабря Совет согласовал свою позицию по предложению о Директиве о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе («Директива NIS2»). Это следует за принятием отчета о NIS2 Комитетом по

промышленности, исследованиям и энергетике Европейского парламента 28 октября 2021 года.

Напомним, общая цель предложения Комиссии для Директивы NIS2 от 16 декабря 2020 года (которая призвана заменить текущую Директиву NIS) заключается в устранении расхождений в требованиях к кибербезопасности и реагировании на растущие угрозы, связанные с цифровизацией и всплеском кибератак. Для достижения этого предложение следует минимальному подходу к гармонизации и расширяет сферу применения действующей Директивы NIS, обязывая большее количество организаций и секторов принимать меры (включая, например, платформы социальных сетей и государственное управление). Он также направлен на усиление требований безопасности, обеспечение безопасности цепочек поставок, оптимизацию обязательств по отчетности и введение более строгих мер надзора и более строгих требований к обеспечению соблюдения, включая согласованные санкции на всей территории ЕС.

Таким образом, в своем общем подходе Совет отреагировал на озабоченность, выраженную в ходе обсуждений в ходе законодательного процесса. Одной из основных проблем было значительное увеличение количества организаций, подпадающих под действие Директивы, и, в частности, введение правила предельного размера, в соответствии с которым практически все средние и крупные организации, которые работают в секторах или предоставляют услуги, охватываемые Директивой. Директива NIS2 подпадает под ее действие. Другие проблемы, связанные, в частности, с взаимодействием Директивы NIS2 с отраслевым законодательством, в частности, Директивой по устойчивости критических организаций («Директива CER»), которая была предложена вместе с предложением NIS2, и инициативой по акту о цифровой операционной устойчивости. для финансового сектора («ДОРА»).

Основные изменения, внесенные Советом в отношении предложения Комиссии по Директиве NIS2, заключаются в следующем:

Повторное уточнение области применения Директивы NIS2: в предложении сохраняется общее правило предельного размера, введенное Комиссией, и включаются дополнительные положения для обеспечения «необходимой пропорциональности, более высокого уровня управления рисками и четких критериев критичности для определения субъекты, подпадающие под действие Директивы», как указано во введении Совета к его предложению. Кроме того, Совет расширяет объем обязательств NIS2, включая управление услугами ИКТ между предприятиями (охватывающее поставщиков управляемых услуг и поставщиков управляемых услуг безопасности) в качестве еще одного типа, подпадающего под категорию существенных субъектов.
Хотя в целом приветствовали этот позитивный шаг, некоторые отраслевые ассоциации также подвергали его критике. Они подчеркивают, что в эту новую категорию не входят поставщики программного обеспечения и микропрограмм, которые поддерживают критически важные функции, выполняемые регулируемыми организациями, и которые часто становятся неотъемлемой частью сетей и услуг, предоставляемых европейским гражданам и предприятиям. Учитывая важность безопасности важнейших цепочек поставок ИКТ, отраслевые

ассоциации призывают законодателей должным образом отразить важность безопасности цепочек поставок.

Чтобы принять во внимание специфику национальных структур государственного управления и обеспечить определенную степень гибкости для государств-членов, в соответствии с позицией Совета Директива NIS2 будет применяться к государственному управлению. субъекты центрального правительства, в то время как государства-члены могут также установить, что Директива применяется к субъектам государственного управления на региональном и местном уровнях. Кроме того, в тексте Совета также уточняется положение об исключении: Директива NIS2 не будет применяться к организациям, которые в основном осуществляют деятельность в области обороны, национальной безопасности, общественной безопасности или правоохранительной деятельности, или к деятельности, касающейся национальной безопасности или обороны. Судебная система, парламенты и центральные банки также исключены.

Согласование Директивы NIS2 с отраслевым законодательством: в тексте Совета содержится отдельная статья о отраслевых актах Союза для обеспечения правовой ясности и обеспечения согласованности между Директивой NIS2 и отраслевым законодательством, в частности, Директивой DORA и Директивой CER. Эта новая статья поддерживает первоначальный подход Комиссии, согласно которому Директива NIS2 должна быть базовой для минимальной гармонизации кибербезопасности, оговаривая, что там, где отраслевые правовые акты Союза требуют, чтобы существенные или важные субъекты принимали меры по управлению рисками кибербезопасности или уведомляли о значительных инцидентах или киберугрозах, и если эти требования по меньшей мере эквивалентны обязательствам, изложенным в настоящей Директиве, соответствующие положения данной Директивы должны не относятся к таким организациям. Тем самым Совет разъяснил в своей позиции, какие аспекты следует учитывать при определении эквивалентного действия обязательств, изложенных в отраслевых положениях правового акта Союза. Это, в частности, включает в себя то, что меры по управлению рисками кибербезопасности должны состоять из соответствующих и соразмерных технических и организационных мер для управления рисками, связанными с безопасностью сети и информационных систем, которые соответствующие субъекты используют при предоставлении своих услуг, и должны включать в себя: как минимум все элементы, изложенные в Директиве NIS2.

Что касается взаимодействия с Директивой CER, текст Совета обеспечивает большую ясность в отношении подхода «всех опасностей». Поскольку угрозы безопасности сети и информационных систем могут иметь разное происхождение, в тексте Совета указывается, что Директива NIS2 применяет подход «от всех опасностей». Этот подход включает в себя защиту сетевых и информационных систем и их физической среды от любых событий, таких как кража, пожар, наводнение, сбои электросвязи или электроснабжения, или от любого несанкционированного физического доступа и повреждения и вмешательства в информацию и средства обработки информации объекта, которые может поставить под угрозу доступность, подлинность, целостность или конфиденциальность

хранимых, передаваемых или обрабатываемых данных или услуг, предлагаемых или доступных через сеть и информационные системы.

Разъяснения в отношении обязательств по управлению рисками кибербезопасности: учет вышеупомянутого подхода «все опасности» согласно позиции Совета, меры по управлению рисками должны также касаться физической и экологической безопасности, включая меры по защите сети и информационных систем организации от сбоев системы, ошибок человека, злонамеренных действий или природных явлений в соответствии с европейскими или международно признанными стандартами., например, те, которые включены в серию ISO 27000. В этом отношении организации должны, в рамках своих мер по управлению рисками, также учитывать безопасность человеческих ресурсов и иметь соответствующие политики контроля доступа (такие меры были недавно введены по предложению Совета). Таким образом, эти меры должны соответствовать Директиве CER.

Кроме того, в тексте Совета уточняется, что при оценке соразмерности технических и организационных мер следует должным образом учитывать степень подверженности организации рискам, ее размер, вероятность возникновения инцидентов и их серьезность. Принимая во внимание уровень и тип риска, представляемого обществу в случае инцидентов, затрагивающих существенные или важные субъекты, меры по управлению рисками кибербезопасности, применяемые к важным субъектам (например, работающим в секторе утилизации отходов, производства, поставщиков цифровых услуг), могут быть меньшими. более строгие, чем те, которые предъявляются к основным организациям (например, работающим в секторах энергетики, транспорта, здравоохранения, цифровой инфраструктуры).

Принимая во внимание трансграничный характер определенных субъектов, текст Совета также предусматривает обязательство Комиссии принять имплементирующий акт, который должен способствовать реализации мер кибербезопасности и подчинять определенные субъекты (включая, в частности, поставщиков услуг облачных вычислений, данные центральных поставщиков услуг, сети доставки контента и доверенных поставщиков услуг) с более высокой степенью гармонизации на уровне Союза.

Оптимизация обязательств по отчетности: Позиция Совета поддерживает обязательства по отчетности основных и важных организаций в отношении инцидентов, оказывающих значительное влияние на предоставление их услуг. После опасений, выраженных государствами-членами, что это приведет к перегрузке организаций, подпадающих под Директиву NIS2, и приведет к завышению отчетности, обязательному сообщению о серьезных киберугрозах компетентным органам или группам реагирования на инциденты компьютерной безопасности (CSIRT) (которые эти организации идентифицируют и который потенциально мог привести к серьезному инциденту), однако, исключен из текста Совета.

Разъяснения в отношении юрисдикции: государства-члены выразили озабоченность последствиями наличия дифференцированной юрисдикции для организаций в секторе ИКТ, как это было предложено Комиссией. На этом фоне в тексте Совета уточнена юрисдикция в зависимости от типа юридических лиц.

Следующие шаги

Общий подход, достигнутый 3 декабря 2021 года, позволит председателю Совета начать переговоры с Европейским парламентом. И Совету, и Европейскому парламенту необходимо будет согласовать окончательный текст. После ее принятия государства-члены должны будут перенести Директиву NIS2 в свое национальное законодательство. Согласно тексту Совета, у государств-членов будет 24 месяца (а не 18 месяцев, как это предусмотрено в предложении Комиссии) с момента вступления в силу директивы для проведения такого включения». ***(Natallia Karniyevich. Cybersecurity: Council adopts its position on the NIS2 Directive // Bird & Bird (https://digitalbusiness.law/2021/12/cybersecurity-council-adopts-its-position-on-the-nis2-directive/#page=1). 21.12.2021).***

***

Російська Федерація та країни ЄАЕС

«За последние годы уровень информационной безопасности на промышленных предприятиях заметно вырос. Ситуация в этой сфере главным образом изменилась благодаря выходу 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Ранее многие заказчики даже не предполагали, каким угрозам подвержены информационные ресурсы и что с ними может произойти, если их не защищать. Сегодня же все понимают, насколько внедрение решений ИБ необходимо на предприятиях, и у большего числа заказчиков есть в штате специалисты, которые занимаются защитой промышленных сетей.

В то же время в нынешних обстоятельствах уже недостаточно просто выполнить все требования регулятора по обеспечению безопасности критической информационной инфраструктуры (КИИ) и отчитаться перед Федеральной службой по техническому и экспортному контролю (ФСТЭК). Главной задачей предприятий является создание такой системы защиты, которая будет соответствовать современным технологиям. Компания «Информзащита» в ходе работы с заказчиком как раз и занимается оформлением необходимых документов для регулятора (на начальном этапе), и обеспечивает безопасность КИИ.

Во время реализации проектов компания учитывает ландшафт информационной безопасности на предприятиях. Как правило, он состоит из средств защиты как от российских, так и от зарубежных вендоров. В таких случаях специалисты компании не строят новую систему с нуля, а стараются максимально все сохранить, при этом добавив функции, которые необходимы для надежной защиты. К промышленным проектам привлекаются непосредственно специалисты по АСУ ТП, так как в этих системах используются внутренние технологические протоколы. При внедрении средств защиты особенно важно сохранить все характеристики работы АСУ ТП, чтобы оборудование работало без задержек и не происходили аварии.

Центр безопасности

В «Информзащите» функционирует Центр промышленной безопасности, где трудятся специалисты по АСУ ТП — уникальные эксперты, которым приходится в том числе изучать оборудование без документации на старых предприятиях и выяснять, как именно работает АСУ ТП. Сотрудники Центра занимаются категорированием объектов КИИ по уровню защищенности – это одно из требований 187-ФЗ. Работы проводятся в два этапа. Объекты, которым нужна наиболее высокая степень защиты, изолируются, также выделяются демилитаризованные зоны.

После категорирования объектов КИИ на предприятии необходимо запустить мониторинг работоспособности ИТ-инфраструктуры, с помощью которой функционирует оборудование, реализуются бизнес-процессы и обеспечивается мониторинг событий ИБ. Для этой задачи требуется создать внутренний SOC, а если средств и возможностей у заказчика недостаточно, можно воспользоваться услугами аутсорсинга или заключить сервисный договор на обслуживание.

Теперь подробнее о том, какие решения применяет «Информзащита» для обеспечения безопасности промышленного сектора. Как известно, сегодня вредоносные программы распространяются через интернет, съемные носители и электронную почту. Стоит отметить, что использование обычного антивируса на производстве может быть проблемным, например, из-за отсутствия поддержки старых операционных систем, несовместимости с промышленными протоколами, необходимости перезагружать оборудование и т.д. Все эти недостатки стали толчком для создания специализированных продуктов, которые были бы адаптированы к работе на предприятиях и обеспечивали высокое качество защиты промышленных сетей от вредоносного воздействия, не допустив при этом ложных срабатываний.

Как собственные, так и вендорские продукты

Для обеспечения ИБ на различных производствах «Информзащита» предлагает как собственные, так и вендорские продукты. К примеру, партнер компании — «Лаборатория Касперского» предоставляет два продукта: Kaspersky Industrial CyberSecurity (KICS) for Nodes (защита промышленных конечных узлов) и Kaspersky Industrial CyberSecurity (KICS) for Networks (обнаружение аномалий и атак в промышленной сети).

KICS for Nodes — это средство комплексной защиты серверов и рабочих станций, которое обладает широкими возможностями по отслеживанию и предотвращению несанкционированного доступа к сети. Оно применимо там, где требуется дальнейшее развитие информационной системы и внедрение новых производственных линеек, а также активно развивается само производство. Во всех этих случаях продукт, безусловно, будет востребован. Это связано с тем обстоятельством, что в промышленном сегменте развитие систем ИБ должно идти параллельно развитию производства. Когда появляются новые системы автоматизации, в них встраиваются и новые технологии защиты. В этом отношении KICS for Nodes оптимальный продукт, поскольку, во-первых, он построен по модульному принципу, и в него можно добавлять либо исключать те или иные компоненты, а во-вторых, внедрять систему вместе с разработчиком намного комфортнее, чем заниматься этим самостоятельно. «Лаборатория Касперского»

является одним из основных партнеров «Информзащиты» и всегда участвует во всех проектах компании, поэтому можно рассчитывать на быструю реакцию вендора при возникновении тех или иных ситуаций.

KICS for Networks — это средство мониторинга промышленной сети и обнаружения аномальных информационных событий. По факту это обучаемая платформа, которая строит карту промышленной сети, а также знает все разрешенные и запрещенные операции. При обнаружении отклонений, KICS for Networks оповещает о них как обслуживающий персонал, так и специалистов по ИБ. Таким образом вычисляются кибератаки или некорректное обслуживание промышленных агрегатов. С одной стороны, полностью контролируются антивирус и некорректные подключения, с другой — отслеживаются возможные атаки на промышленную сеть.

Решения «Информзащиты» применяют как небольшие компании, так и металлургические и горнодобывающие холдинги. Подходы к кибербезопасности не сильно отличаются. Применительно к конкретному производству выбирается наиболее оптимальное решение.

На сегодняшний день у компании уже есть завершенные проекты для металлургических организаций в рамках 187-ФЗ. К слову, металлурги активно сотрудничают с нашим Центром промышленной безопасности, поскольку их ИТ-системы очень развиты и вопросы кибербезопасности для них особенно актуальны». ***(Как защитить промышленные сети от кибератак // CNews (https://www.cnews.ru/articles/2021-12-29_kak_zashchitit_promyshlennye_seti_ot). 29.12.2021).***

***

«После начала политического кризиса в Беларуси в стране появились так называемые «киберпартизаны» - анонимная команда IT-специалистов, которые пытаются нанести ущерб белорусскому режиму с помощью технологий. Так, за последнее время они заявили о взломе нескольких государственных баз данных. Кроме того, в своем телеграм-канале с более 70 тысячами подписчиков, который власти признали экстремистским, они публикуют сведения о чиновниках и аудиозаписи личных разговоров сотрудников силовых структур.

Такой масштаб взломов и сливов информации не может не вызывать вопросы о том, как вообще это может происходить в стране, которая гордится своими достижениями в IT-отрасли, что белорусское государство делает, чтобы защищать данные своих граждан, и чем это все грозит для белорусов.

Очень низкий уровень кибербезопасности Беларуси

Как рассказывали сами «киберпартизаны» в недавнем интервью для DW, у них есть доступ к базе данных «Паспорт» со всеми персональными данными белорусов. По их словам, в базе «Паспорт» есть 16 тысяч скрытых записей - силовики и приближенные чиновники Лукашенко. Также они рассказали общественности, что МВД создало отдельную базу «Беспорядки» с данными почти 39 тысяч белорусов, которых привлекали к ответственности за участие в протестах.

Кроме того, «киберпартизаны» взламывали компьютерные сети госорганизаций вроде «Беларуськалия» и заявляли, что имеют в распоряжении записи с камер наблюдения в ИВС на Окрестина. Много шума в Беларуси наделала публикация так называемой «карты доносов» с личными данными людей, обращавшихся в милицию с жалобами на протесты в Беларуси.

Белорусский военно-политический обозреватель Егор Лебедок в беседе с DW отмечает, что «нам доподлинно неизвестно, был ли это технический взлом или социальный хакинг, то есть использование источника внутри госаппарата». «Если же правда применяли сугубо технические средства, то это говорит об очень низком уровне кибербезопасности и непрофессиональном подходе к таким вещам. Думаю, власти даже не ожидали, что у них может случиться такая утечка», - считает Лебедок.

По его словам, был ли это внешний взлом, оперативная игра, или использовали кого-то внутри, на самом деле не столь важно - суть в том, что утекли большие объемы данных. «Это провал для безопасности страны: если база «Паспорт» попадет в спецслужбы других государств, это хорошее пособие для анализа всей страны, прогнозирования, выявления внешней разведки. И, конечно, такая база данных значительно упрощает возможности финансового мошенничества», - поясняет Егор Лебедок.

Как защищают персональные данные в Беларуси?

В белорусской неправительственной организации Human Constanta, которая занимается защитой персональных данных, DW сообщили, что сама система сбора и обработки персональных данных в Беларуси построена таким образом, что рано или поздно утечка должна была случиться: "У нас подход централизованный - собирается очень много данных о гражданах. Проблема в том, что баз данных очень много, больше 200, и данные там часто дублируются. Кроме того, эти базы разрабатывались в разные годы, на их поддержание нужны большие средства - а если база создавалась 20 лет назад, то обеспечить ее безопасность без полной модернизации невозможно".

В Human Constanta также поясняют, что в идеале в стране должны быть специальные службы, которые занимаются кибербезопасностью и защитой персональных данных: «Что касается кибербезопасности, то у нас за это отвечает Оперативно-аналитический центр при президенте (ОАЦ) - самый закрытый орган Беларуси, у нас даже не опубликовано постановление с перечнем его функций. Как он работает, как проверяет базы данных и заботится о нашей безопасности никто не знает».

Если говорить о защите персональных данных, то тут вопрос не только в утечке и реагировании на такие инциденты, но также в том, какие данные о нас собирает государство, на каких принципах, нет ли злоупотреблений. «С мая 2021 года у нас начал действовать Закон о защите персональных данных, а в ноябре был создан Орган по защите персональных данных, который должен быть независимым, но, по сути, подчиняется ОАЦ. Не совсем ясно, может ли этот орган прийти в МВД и проверить, как защищают данные граждан. Может, если бы он был создан раньше, то его можно было бы как-то привлечь к расследованию этих инцидентов», - отмечают в Human Constanta.

Власти Беларуси взломы и сливы не комментируют

Белорусские власти, в частности МВД, деятельность «киберпартизан» никак не комментируют - ни опровергают, ни подтверждают утечку данных. О каких-либо расследованиях и уголовных делах по фактам взломов также ничего не известно. Только однажды Александр Лукашенко во время совещания посоветовал чиновникам возвращаться к бумажным носителям, раз те не могут защитить информацию в компьютерах. «Пишите от руки и складывайте у себя в ящик», - сказал Лукашенко.

Белорусские эксперты считают, что власти, разумеется, должны провести расследование этих инцидентов. Это расследование должно быть публичным, учитывая масштаб произошедшего. "В Эстонии в 2008 году была масштабная хакерская атака, после которой были сделаны выводы, и сейчас их система защиты одна из передовых в мире. Вопрос, будут ли сделаны такие выводы в Беларуси, тем более в ситуации, когда почти не осталось механизмов взаимодействия общества и государства, а также нормальных правоохранительных институтов и независимых судов», - говорят специалисты по защите персональных данных из Human Constanta.

Слив данных имеет важное общественное значение

Каким бы ни был характер взлома и хакинга государственных баз данных в Беларуси, стоит признать, что сейчас личные данные белорусов находятся в руках никому не известных людей с неясными целями. Но сами «киберпартизаны» утверждают, что гарантируют безопасность данных, не планируют их использовать в коммерческих целях, а их деятельность – «это сопротивление захвату власти в Беларуси».

В Human Constanta отмечают, что данные белорусов 27 лет были тоже не у самых хороших людей, а сейчас просто этот круг лиц расширился: "Точно также, как мы не можем контролировать, как чиновники обрабатывают персональные данные граждан, у нас нет данных, насколько этично происходит обработка и использование утекших данных белорусов. Зато благодаря этим сливам мы узнали, что есть какие-то тайные базы и есть списки для политически неблагонадежных людей - это, очевидно, преступление».

Егор Лебедок также говорит, что сливы и взломы «киберпартизан» имеют важное общественное значение. «Они предметно показали нам, что происходит сейчас в белорусской политической системе. Кроме того, это обозначило для общества важность персональных данных, конфиденциальности, теперь каждый задумается о своем поведении в соцсетях и тому подобное", - резюмирует эксперт». ***(Богдана Александровская. Кибепартизаны могут взломать все? Как защищены данные белорусов // Deutsche Welle (https://www.dw.com/ru/kibepartizany-mogut-vzlomat-vse-kak-zashhishheny-dannye-belorusov/a-60046193). 07.12.2021).***

***

«Австралійський уряд хоче прийняти законопроект про поправку до законодавства про безпеку (критична інфраструктура) 2020 року, капітальну переробку, яка має на меті допомогти австралійському бізнесу відбиватися від кібератак. Законопроект розширює бізнес-сектори, які раніше були визначені як критична інфраструктура, додаючи до списку, серед іншого, продукти харчування та бакалію, фінанси та банківську справу, університети, зв'язок, оборону, енергетику та транспорт. Це також передбачає суворі вимоги щодо 12-годинного звітування про кібератаки, а також дозволить Австралійському управлінню сигналів «втрутитися» для захисту мереж під час чи після значної кібератаки.

У листі до члена австралійського парламенту, Ради промисловості інформаційних технологій, Австралійської асоціації інформаційної промисловості та Коаліції з кібербезпеки, які представляють численні технологічні фірми, включаючи Google, Microsoft, Intel, Adobe та Amazon, сказав: «Без значного перегляду законопроект створить невиконаний набір зобов'язань і створить тривожний глобальний прецедент». Крім того, «Ми також стурбовані глобальним впливом, який матиме такий законопроект, і тим, як він підриває цінності, які Австралія пропагує на міжнародному рівні». Далі в листі зазначається, що «це підриває хорошу роботу уряду на міжнародному рівні з цих питань і створює тривожний прецедент для інших урядів, які стикаються з подібними проблемами національної безпеки».

Державне втручання або ринкові системи

Це не єдиний випадок, коли Австралія створює глобальний прецедент проти технологічних лідерів. На початку 2021 року Австралія стала першою країною, яка вимагала від Facebook і Google платити за новинний контент, наданий медіа-компаніями за системою роялті. У своїй заяві до Комітету з економіки Сенату Мелані Сілва, керуючий директор Google в Австралії та Нової Зеландії, сказала: «У нинішній формі Кодекс залишається непрацездатним». «Принцип необмеженого зв'язування між веб-сайтами є основоположним для пошуку. У поєднанні з некерованим фінансовим та операційним ризиком, якщо ця версія Кодексу стане законом, це не дасть нам реального вибору, крім як припинити доступ до Пошуку Google в Австралії».

У відповідь на запропонований закон про цифрові медіа Facebook видалив новинний контент від австралійських користувачів. Це тривало цілий тиждень, перш ніж Facebook заявив, що «недавні дискусії з австралійським урядом його заспокоїли» і відновить новинний контент для своїх користувачів в Австралії. Зростає ймовірність того, що капітальний ремонт критичної інфраструктури в Австралії буде відбуватися подібним чином, оскільки три галузеві організації стверджують, що «законопроект залишається дуже проблематичним і в основному незмінним, незважаючи на широкий відгук від наших організацій».

Хоча австралійський уряд стверджує, що повноваження на примусове входження в мережі будуть використовуватися лише як крайній засіб, технічні групи стурбовані тим, що це надає «безпрецедентні та далекосяжні повноваження, які мають підпорядковуватися законодавчо визначеному механізму». Представники

галузі також критикували терміни звітності. Зазначаючи, що їх слід продовжити з «протягом 12 годин» до «принаймні 72 годин» або «без зайвої затримки».

Що це все означає

Законопроект навряд чи стане законом у той момент, коли він підготовлений. Двопартійний законопроект із подібними вимогами, Закон про інфраструктурні інвестиції та робочі місця, нещодавно ухвалив Сенат США. Цей законопроект, хоча і не для організацій критичної інфраструктури, які вже мають суворі вимоги щодо 12-годинної звітності до Департаменту внутрішньої безпеки, забезпечить більш розумні вимоги щодо 24-годинної звітності та продовження обміну інформацією протягом 72 годин після повідомлення про порушення. Законодавство передбачає забезпечення безпечного механізму, що дозволяє уряду отримувати ці звіти протягом 180 днів, а також захист від відповідальності компаній, які подають звіти про порушення даних, що звільняє їх від судових позовів. Такі міркування належним чином не інкапсуловані в австралійському законопроекті.

Якщо австралійський уряд намагатиметься досягти прогресу, не розглядаючи й не вирішуючи проблем, які поділяють технологічна галузь, цілком імовірно, що ми побачимо подібне відштовхування з боку цих органів та подальші переговори за закритими дверима. Неминуче дві сторони – уряд і техніка – зустрінуться десь посередині, і уряд, можливо, продовжить терміни звітності та погодиться на більш консервативні директиви щодо того, чи, коли і як вони будуть входити в мережі. Як наслідок будь-яких поступок, уряд може намагатися накласти більші штрафи та втрату державних контрактів для організацій, які не дотримуються вимог щодо звітності. Це також може посилити штрафи для компаній, які, на його думку, не проявили ініціативи щодо своєї кібербезпеки». ***(Jack Lindsay. Australia Leads with Controversial Cyber Laws // Tripwire, Inc. (https://www.tripwire.com/state-of-security/government/australia-leads-with-controversial-cyber-laws/). 09.12.2021).***

***

«Операторы социальных сетей и поисковых систем в Японии должны будут указать страны, в которых физически хранятся данные пользователей, в соответствии с запланированной поправкой к местным законам.

На этой неделе Министерство внутренних дел и коммуникаций объявило о планах внести изменения в Закон о телекоммуникационном бизнесе в начале следующего года.

Поправка, если она будет принята, требует от поисковых систем, операторов социальных сетей и компаний мобильной связи с более чем 10 миллионами японских пользователей раскрыть, где в мире они хранят данные, и указать любых иностранных субподрядчиков, которые могут получить доступ к данным.

Предлагаемый закон применяется к зарубежным компаниям, работающим в Японии, а это означает, что такие компании, как Twitter и Facebook, должны будут публично раскрыть свой выбор хранилища. Как ни странно, поисковые системы, которые покрывают только путешествия и еду, получают пропуск и не обязаны подчиняться.

Обеспокоенность противников закона, выраженная во вторник, заключается в том, насколько далеко будут распространяться меры, и что они могут быть

чрезмерно широкими и двусмысленными. Бизнес-операторы размышляли, столкнутся ли они с трудностями прогнозирования затрат на управление и техническими ограничениями управления информацией.

«Существует риск того, что затраты будут переложены на пользователей в виде более низких уровней обслуживания и повышения цен, что вызовет социальную неэффективность», - говорится в одном из ответов на слушания, проведенного министерством в отношении операторов связи.

Этот шаг отчасти является реакцией на чрезвычайно популярное в Японии бесплатное приложение для обмена мгновенными сообщениями LINE, в котором недавно произошли сбои, связанные с хранением и защитой данных.

В марте прошлого года выяснилось, что некоторые данные LINE дошли до Китая, что побудило японских правительственных чиновников прекратить использование приложения. Ранее LINE использовался для связи со многими региональными правительствами. Как один Reg читатель отметил, что запрет не продлилось долго, и использование линии было восстановлено некоторыми региональными государственными службами.

Несколько месяцев спустя 100 местных политических деятелей и их сообщения LINE были извлечены, когда в результате кибератаки удалось отключить функции шифрования.

И всего несколько недель назад было объявлено, что данные 133000 пользователей LINEpay были загружены в маловероятное местоположение GitHub, когда сотрудник исследовательской группы предположительно произвел ошибку.

Принимая во внимание эти инциденты, законодательный шаг правительства выглядит не столько реакцией коленного рефлекса, сколько оправданными превентивными действиями против будущих сбоев в данных, особенно с учетом того, что в разных странах применяются разные стандарты хранения и законы.

Компания, нарушившая предложенную Японией поправку, может столкнуться с приказами по улучшению бизнеса и многим другим. Помимо поправки к Закону о телекоммуникационном бизнесе, с апреля 2022 года предприятия должны будут соблюдать Закон Японии о защите личной информации». ***(Laura Dobberstein. Japan draws a LINE: web giants must reveal where they store user data // The Register (https://www.theregister.com/2021/12/16/japan_data_location_requirement/). 16.12.2021).***

***

Інші країни

«Точно так же пандемия COVID-19 перевернула мир с ног на голову, создав царство страха, неуверенности и потерь. Но в самый разгар этого кризиса, подобно скорости света, мир также был продвинут и преобразован в цифровую революционную парадигму, как никто другой. Независимо от того, было ли это средством предотвращения распространения вируса, обеспечения непрерывности ведения бизнеса, образования или просто придания некоторого

подобия повседневной нормальной жизни, информационные и коммуникационные технологии были на переднем крае в начале пандемии. Принеся с собой «волну» изощренных технологий, моделей, ориентированных на цифровые технологии, возможность подключения и поддержание связи, наращивание потенциала рабочей силы будущего, культурные и поведенческие изменения в ведении бизнеса и многое другое. Однако после этого а на другом конце спектра - усиление угрозы кибербезопасности. Хотя киберпреступления не являются новым явлением и, если на то пошло, явлением пандемии COVID-19, они, безусловно, оказались ее симптомом. К революционной изощренности цифровых технологий добавляются изощренные киберпреступления. Южная Африка тоже стала и остается целью и жертвой громких кибератак и киберпреступлений.

В связи с этим необходимость борьбы с киберпреступлениями и сдерживания их становилась все более насущной, и поэтому в Южной Африке был принят закон о киберпреступлениях. 26 мая 2021 года был подписан Закон № 19 от 2020 года о киберпреступлениях («Закон о киберпреступлениях»). В принципе, Закон о киберпреступлениях предусматривает преступления и наказания, которые имеют отношение к киберпреступлениям, это было раскрыто в предыдущей статье.

Адвокат доктор Машабане, генеральный директор Министерства юстиции и конституционного развития, описывает Закон Южной Африки о киберпреступлениях как «новаторский и решающий шаг в киберуправлении и политическом пространстве страны, а вместе с Законом о продвижении личной информации (POPI) 2020, формирует ключевой элемент арсенала Южной Африки в борьбе с киберпреступностью». Мы не можем договориться больше!

Хотя Закон о Киберпреступности не в силе, потому что ее начало еще будет провозглашены, подписание Президентской Минуты ознаменовало 1 ст декабря 2021 года как начало некоторых положений Закона о киберпреступлениях.

Вступили в силу следующие положения Закона о киберпреступлениях:

Глава 1, которая устанавливает определения и толкование положений Закона о киберпреступлениях;

В главе 2 (за исключением части VI) излагаются виды действий, которые считаются правонарушениями в соответствии с Законом о киберпреступлениях, включая незаконный перехват данных, кибермошенничество и раскрытие сообщений с данными, которые подстрекают к нанесению ущерба собственности или насилию;

Глава 3 предусматривает юрисдикцию судов Южной Африки по рассмотрению киберпреступлений в пределах и за пределами Южной Африки с учетом транснационального характера киберпреступлений;

Глава 4 (за исключением статей 38 (1) (d), (e) и (f), 40 (3) и (4), 41, 42, 43 и 44) регулирует полномочия сотрудников полиции по поиску, доступу и изъятию определенные статьи и расследование киберпреступлений;

В главе 7 представлены доказательства определенных фактов в виде письменных показаний под присягой.

Глава 8 (за исключением статьи 54) устанавливает обязанность Национального директора прокуратуры вести статистику судебных преследований

и способность обнаруживать, предотвращать и расследовать киберпреступления; И наконец

Глава 9 (за исключением разделов 11B, 11C, 11D и раздела 56A (3) (c) - (e) Закона об уголовном праве (сексуальные преступления и связанные с ним дела) с поправками) 32 от 2007 года в Перечне законов, отмененных или измененных в терминах статьи 58) содержит общие положения.

Министр юстиции и исправительных учреждений Рональд Ламола («Министр Ламола») отметил, что вводимые в эксплуатацию секции направлены на обеспечение того, чтобы:

Полицейские службы Южной Африки («SAPS») имеют надлежащие возможности и подготовку для борьбы с киберпреступлениями;

Имеются поддающиеся проверке статистические данные о масштабах киберпреступности в Южной Африке;

Можно оценить эффективность и возможности SAPS по расследованию киберпреступлений; и

Возможности Национальной прокуратуры по преследованию киберпреступлений можно оценить.

Разделы Закона о киберпреступлениях, которые не могли вступить в силу, включают, среди прочего, судебные приказы о защите от вредоносного раскрытия порнографии и злонамеренных сообщений, определенные требования по сохранению доказательств киберпреступлений или злонамеренных сообщений и создание функционального контактного лица в рамках SAPS для координации расследований киберпреступлений. в Южной Африке и для содействия международному сотрудничеству. После доработки положений Закона о киберпреступлениях эти разделы будут введены в действие.

С вступлением в силу только определенных разделов Закона о киберпреступлениях возникают вопросы - достаточно ли этого? Это эффективно?

Дело в том, что мы все остаемся уязвимыми для киберпреступлений и атак, но каждый из нас должен сыграть свою роль в борьбе с киберпреступностью. И хотя Южной Африке, возможно, придется догонять, учитывая новые и новаторские способы совершения преступлений в этом цифровом революционном пространстве, наша законодательная база не находится в состоянии паралича или инерции. Поэтому частичное вступление в силу Закона о киберпреступлениях приветствуется!

Фактически, учитывая рост числа киберпреступлений во всем мире, это прогрессивный шаг к тому, чтобы законы Южной Африки соответствовали международным стандартам в целях борьбы с киберпреступлениями». ***(Rakhee Bhoora, Jesicca Rajpal. Red Flag Series: Commencement of Certain Provisions of the Cybercrimes Act // Fasken Martineau DuMoulin LLP (https://www.fasken.com/en/knowledge/2021/12/6-red-flag-series-commencement-of-certain-provisions-of-the-cybercrimes-act). 06.12.2021).***

***

Створення та функціонування кібервійськ

«Cyber Command, хакерський підрозділ американських військових, вжив наступальних дій, щоб зруйнувати групи кіберзлочинців, які розпочали атаки програм-викупів на американські компанії, підтвердив CNN у неділю речник командування.

Речник відмовився уточнити, які дії вжило командування. Але це одне з перших недвозначних підтверджень від Cyber Command після травневої атаки програм-вимагачів Colonial Pipeline про те, що командування націлено на злочинні угруповання, які утримують комп'ютерні системи американських компаній в заручниках.

Нові коментарі генерала Пола Накасоне, керівника кіберкомандування та директора Агентства національної безпеки, про які газета New York Times повідомила раніше в неділю, свідчать про те, що комп'ютерні оперативники американських військових все більше бажають зламати злочинців, а не лише державних акторів. які становлять загрозу для критичної інфраструктури США.

Агенції безпеки по всьому уряду США активізували переслідування груп програм-вимагачів після того, як на початку цього року зломи зупинили Colonial Pipeline, основного транспортника американського палива та основного переробника м'яса. За словами джерел, знайомих із ситуацією, CNN повідомляв у червні, що уряд США вжив наступальних кроків у відповідь на програмне забезпечення-вимагач, включаючи компрометацію та спостереження за мережами кіберзлочинців.

Минулого місяця Накасоне заявив, що уряд США «провів сплеск» проти операторів програм-вимагачів, у тому числі намагаючись відрізати джерела фінансування хакерів.

Накасоне повторив це повідомлення в інтерв'ю New York Times на цих вихідних.

«Раніше, під час і після, з низкою елементів нашого уряду, ми вжили заходів і ми наклали витрати», - сказав Накасоне газеті. «Це важливий елемент, про який ми повинні завжди пам'ятати».

Контрнаступ уряду США проти груп програм-вимагачів, багато з яких базуються в Східній Європі та Росії, також включав обвинувачення передбачуваних вимагачів і санкції проти криптовалютної біржі, звинуваченої у відмиванні грошей для хакерів.

Білий дім намагався тиснути на російський уряд, щоб він розправився з кіберзлочинцями, які діють з російської землі. Залишається побачити, чи станеться це – Москва часто закриває очі на хакерів, які не націлені на російські організації, кажуть аналітики…». ***(Sean Lyngaas. US military's hacking unit publicly acknowledges taking offensive action to disrupt ransomware operations // Cable News***

Network (https://edition.cnn.com/2021/12/05/politics/us-cyber-command-disrupt-ransomware-operations/index.html). 06.12.2021).

***

«Агрессивный взлом мобильного телефона известного адвоката, представляющего ведущих деятелей польской оппозиции, произошел в последние недели решающих парламентских выборов 2019 года. Два года спустя прокурор, оспаривая попытки популистского правого правительства провести чистку в судебной системе, взломал ее смартфон.

В обоих случаях злоумышленником была шпионская программа военного уровня от NSO Group, израильского агентства по найму, которое правительство США недавно внесло в черный список, говорят цифровые сыщики из Citizen Lab из Университета Торонто, интернет-сторожевого пса.

Citizen Lab не может сказать, кто заказал взлом, а NSO не идентифицирует своих клиентов, кроме того, что она работает только с законными правительственными учреждениями, проверенными Министерством обороны Израиля. Но обе жертвы считают, что ответственность за это несет все более нелиберальное правительство Польши.

Представитель государственной безопасности Польши Станислав Зарин не подтвердил и не опровергнул, заказало ли правительство взломы или является заказчиком NSO.

Адвокат Роман Гертых и прокурор Ева Врзосек присоединились к списку критиков правительства по всему миру, чьи телефоны были взломаны с помощью продукта компании Pegasus. Шпионское ПО превращает телефон в подслушивающее устройство и позволяет операторам удаленно перекачивать все, от сообщений до контактов. Среди подтвержденных жертв были мексиканские и саудовские журналисты, британские адвокаты, палестинские правозащитники, главы государств и американские дипломаты из Уганды.

Но слухи о взломе в Польше особенно примечательны, поскольку правозащитные группы требуют запретить шпионское ПО на всей территории ЕС. Европейский Союз, состоящий из 27 стран, ужесточил ограничения на экспорт шпионского ПО, но критики жалуются, что злоупотребления им со стороны государств-членов ЕС необходимо срочно решить.

Citizen Lab ранее выявляла в Польше несколько случаев заражения, начиная с ноября 2017 года, хотя на тот момент не выявила отдельных жертв. Шпионское ПО Pegasus также было связано с Венгрией, которую, как и Польшу, осудили за антидемократические злоупотребления. Сообщается, что среди клиентов NSO находятся Германия и Испания, причем каталонские сепаратисты обвиняют Мадрид в том, что они нацелены на них с помощью Pegasus.

«Как только вы начнете агрессивно нацеливаться с помощью Pegasus, вы присоединитесь к братству диктаторов и автократов, которые используют его

против своих врагов, и этому определенно нет места в ЕС», - сказал старший исследователь Джон-Скотт Рейлтон из Citizen Lab.

Бывший член парламента ЕС Мариетье Шааке из Нидерландов, ныне директор по международной киберполитике в Стэнфордском университете, заявила: «ЕС не может достоверно осуждать нарушения прав человека в остальном мире, закрывая глаза на проблемы дома».

Польские цели рассматривают взлом как свидетельство опасной эрозии демократии в той самой стране, где советская гегемония начала рушиться четыре десятилетия назад.

Всего за несколько часов до того, как Зарин ответила на вопросы по электронной почте о взломе от Associated Press, областной прокурор подал ходатайство об аресте Гертыха, адвоката, в рамках расследования финансовых преступлений.

Зарин не стала комментировать, могут ли эти два вопроса быть связаны между собой. Он сказал, что Польша ведет наблюдение только после получения судебного приказа.

«Предположения, что польские службы используют оперативные методы для политической борьбы, необоснованны», - сказал Зарин.

Представитель NSO заявил в понедельник, что компания является «поставщиком программного обеспечения, компания не управляет технологией, и при этом компания не осведомлена о целях и данных, собранных клиентами». Однако исследователи Citizen Lab и Amnesty International говорят, что NSO, похоже, поддерживает инфраструктуру заражения.

Представитель компании также назвал неясными утверждения о неправомерном использовании польской компании Pegasus: «Если демократическая страна на законных основаниях, следуя надлежащей правовой процедуре, использует инструменты для расследования лица, подозреваемого в совершении преступления, это никоим образом не будет считаться неправомерным использованием таких инструментов.»…» ***(FRANK BAJAK and VANESSA GERA. AP Exclusive: Polish opposition duo hacked with NSO spyware // THE ASSOCIATED PRESS (https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e). 21.12.2021).***

***

«После явного отказа заплатить выкуп российские хакеры в ответ передали в даркнет выборку из 13 миллионов записей с данными полиции Великобритании.

Записи были украдены у полицейского подрядчика, и российские хакеры освободили лишь небольшую часть того, что они украли, но пригрозили выпустить еще больше, если их требования будут и далее отклоняться. Остается неясным, какая именно личная информация была взломана, но образцы даркнета содержат указания на то, что данные были украдены из национальной системы мониторинга дорожного движения, и содержат фотографии водителей, которые были пойманы на превышении скорости.

Данные полиции Великобритании взяты у подрядчика, отказ от выкупа приводит к частичной утечке

Взлом приписывается банде Clop, группе программ-вымогателей, которая действует с 2019 года и была особенно активна в начале 2021 года (два из ее крупнейших предыдущих взломов были связаны с ExecuPharm и компанией Accellion). Некоторые члены банды были арестованы в Украине прошлым летом, но российские хакеры быстро вернули ее в бизнес. Группа заработала десятки миллионов долларов на некоторых своих атаках и считается крупным игроком среди киберпреступников.

Известно, что группа управляет темным веб-сайтом, через который она доксирует жертв, которые не платят. В данном случае жертвой была шотландская компания по поддержке ИТ-служб Dacoll Group. Dacoll заключает контракт с правительством Великобритании на обслуживание Национального компьютера полиции (PNC), общей системы, используемой многими правоохранительными органами страны.

По всей видимости, Dacoll был успешно подвергнут фишингу, что дало российским хакерам доступ примерно к 13 миллионам записей с данными полиции Великобритании. После этого фирма отказалась выплатить выкуп, сумма которого неизвестна. В настоящее время мало что известно о том, какая информация была скомпрометирована, но группа разместила сотни образцов данных на своем темном веб-сайте в качестве доказательства атаки и пригрозила выпустить еще больше, если подрядчик не пересмотрит свою позицию в отношении выкупа.

Национальный центр кибербезопасности заявил, что он работает с Dacoll и правоохранительными органами над расследованием инцидента. Даколл недавно опубликовал заявление, в котором говорилось, что нарушение произошло 5 октября. Выборка данных полиции Великобритании была удалена с темного веб-сайта, и неясно, намерены ли российские хакеры выполнить свои угрозы и выпустить больше данных.

Российские хакеры утекают информацию о краже данных с камер дорожного движения

Среди образцов данных полиции Великобритании, загруженных в даркнет, были изображения с камер дорожного движения, которые автоматически срабатывают при обнаружении транспортного средства, превышающего допустимую скорость. Это означает, что записи были украдены из системы автоматического распознавания номерных знаков (ANPR). Некоторые из просочившихся образцов показывают изображения лиц водителей крупным планом, пойманные камерой контроля скорости.

Граждане Великобритании, несомненно, хотели бы получить более подробную информацию о том, к чему именно имели доступ российские хакеры, но британские агентства и Dacoll, естественно, очень умалчивают о мелких деталях атаки. Есть основания для беспокойства, учитывая, что Dacoll предоставляет услуги 90% правоохранительных органов Великобритании через свою дочернюю компанию NDI Technologies. Фирма NDI Recognition Systems поддерживает системы ANPR; Данные полиции Великобритании передаются Highways England и DVLA через программные продукты компании.

Российские хакеры еще раз подчеркнули тот факт, что организационная кибербезопасность настолько хороша, насколько хороши самые слабые звенья в цепочке поставок поставщиков с надежным доступом, но на этот раз с потенциально более серьезными последствиями, чем обычно.

Как отмечает Сарью Найяр, генеральный директор Gurucul, «неясно, являются ли опубликованные доказательства ценными, хотя кажется возможным, что их можно использовать для идентификации и шантажа автомобилистов и других лиц… В данном случае данные, хотя они должны были быть рассматривался как конфиденциальный, легко поддавался фишингу и скачивался. У полиции и ее продавца Dacoll нет особых стимулов платить именно этот выкуп, поэтому бремя идентификации ляжет на тех, кто цитируется в доказательствах. Очень жаль, что ошибка Даколла наносит потенциальный ущерб другим, поэтому полиции следует укрепить свои собственные системы и поступать правильно с теми, чьи доказательства просочились».

Этот инцидент поднимает вопрос о том, что можно ожидать от обычного человека, когда правительственные учреждения, которым доверена самая важная из их личной информации, имеют сбой в системе безопасности. В преддверии курортного сезона еще предстоит увидеть, что правительство Великобритании сделает, чтобы исправить ситуацию; Гражданам Великобритании все еще необходимо точно знать, чем похитились российские хакеры. В худшем случае доступ к информации об их водительских удостоверениях является ключевым элементом, с помощью которого воры могут изменить адрес в целях мошенничества с личными данными.

Гаррет Граек, генеральный директор YouAttest, отмечает, что импульс в основном падает на государственных подрядчиков, которые имеют доступ к этой конфиденциальной информации: «Настоящий вопрос - что предприятия делают со всем происходящим хаосом? Главное - сосредоточиться на надежных методах обеспечения безопасности. Рекомендации NIST по нулевому доверию (SP 800-27) и облачной безопасности (SP 800-210) - хорошее место для начала. Идентификация является ключом ко всем этим директивам и мерам противодействия. Это начинается с того, что предприятие знает, какие личности имеют право доступа к каким ресурсам, и это необходимо для кибербезопасности».

Бабер Амин, главный операционный директор Veridium, предлагает дополнительные предложения по обеспечению безопасности данных полиции Великобритании в корневом каталоге: «В этом случае и ИТ-компания, и полиция Великобритании должны внедрить соответствующий контроль доступа. Предотвращение успешных фишинговых атак, как обычно, требует многоуровневого подхода к безопасности и доступу.

Исключите любой доступ без аутентификации, потребовав аутентификации каждого соединения.

Избавьтесь от однофакторной аутентификации, включив несколько факторов.

В зависимости от информации, к которой осуществляется доступ, назначьте различные факторы аутентификации в зависимости от их уровня доверия.

Создайте стратегию многоканальной аутентификации, чтобы один скомпрометированный канал не подвергал риску систему.

Не разрешайте полный доступ ко всем системам, даже если пользователь аутентифицируется через какой-то MFA. Разделите весь доступ.

Внедрите инструменты, которые ищут необычную активность, например зондирование, множественные отказы, прием больших объемов данных или извлечение больших объемов данных.

Внедрите инструменты, которые оценивают доверие конечных точек и могут идентифицировать ботов и автоматизированные процессы.

Внедрите поведенческую биометрию, чтобы отличать обычных пользователей от ботов и злоумышленников».

Учитывая, что российские хакеры добровольно сняли свой тизер с данными полиции Великобритании, вполне возможно, что инцидент закончится незаметно, поскольку Клоп опасается, что он может привлечь такой же уровень жара, как в последнее время REvil (группа уже пережила одну волну арестов). Но жители Великобритании будут иметь дополнительное беспокойство в преддверии курортного сезона, с которым им не придется иметь дело, поскольку Министерство внутренних дел пытается преуменьшить значение инцидента и медлить с публичной оценкой потенциального ущерба». ***(Scott Ikeda. UK Police Data Leaked to Dark Web; Russian Hackers Hold 13 Million Records to Ransom // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/uk-police-data-leaked-to-dark-web-russian-hackers-hold-13-million-records-to-ransom/). 27.12.2021).***

***

«Правоохоронні органи Великобританії поділилися понад півмільйона скомпрометованих паролів, знайдених у хмарному сховищі, з Have I Been Pwned, провідним сайтом для безпечної перевірки, чи не було зламано облікові дані для входу.

Заголовок полягає в тому, що більше однієї третини цих паролів (близько 225 мільйонів) не були зареєстровані раніше, що втричі перевищує кількість населення всієї Великобританії.

Сотні мільйонів нових скомпрометованих паролів потрапили в темну мережу, стають загальнодоступними

Скарбничка скомпрометованих паролів надходить із хмарного сховища, захопленого Національним агентством Великобританії зі злочинності (NCA). Агентство вважає, що набір паролів був зібраний з різних порушень даних, але близько 225 мільйонів з них раніше не були відомі Have I Been Pwned і, можливо, були отримані від раніше невідомих зломів. Наразі NCA не приписує жоден зі зламаних паролів будь-які конкретні порушення. Однак деякі були знайдені в парі з обліковими записами електронної пошти.

NCA вважає, що зламані паролі доступні у відкритому доступі, враховуючи обсяг і широту компіляції, ідея підтверджується тим фактом, що більше половини вже відомі Have I Been Pwned. Враховуючи величезну кількість, експерти з кібербезпеки рекомендують всім користувачам Інтернету перевірити сайт, щоб перевірити, чи не були зламані їхні логіни.

Хоча Have I Been Pwned є надійним ім’ям для перевірки на наявність зламаних паролів (і використовується з цією метою 27 національними урядами по

всьому світу), правоохоронні органи досить рідко передають вкрадені логіни, які вони відновлюють, з будь-яким приватним підприємством. Це сталося лише вдруге; ФБР встановило постійні відносини з сайтом у травні цього року. Широка громадськість може використовувати розділ «Pwned Passwords» на сайті Have I Been Pwned, щоб побачити, чи не був зламаний пароль, не підключаючи його до адреси електронної пошти чи імені користувача; адміністратори також можуть завантажити необроблений список паролів для локальних перевірок при створенні нових облікових записів або зміні паролів.

Навіть якщо зламані паролі не пов'язані з адресами електронної пошти чи іншою ідентифікаційною інформацією, вони все одно використовуються в атаках «грубої сили» та «розпилення пароля», які просто перевіряють потенційно релевантні сегменти цих гігантських списків проти відомих імен користувачів або входу в електронну пошту. Сайт Have I Been Pwned не пов'язує скомпрометовані паролі з іншою інформацією для входу на стороні користувача, але дозволяє шукати будь-який елемент, щоб визначити, чи він з'явився під час відомого порушення.

Список паролів Have I Been Pwned розширюється до понад 5 мільярдів записів, 847 мільйонів унікальних паролів

Заснована в 2013 році, Have I Been Pwned була створена насамперед у відповідь на масові зломки Adobe, Yahoo Voices і Sony, які сталися незадовго до цього. Політика сайту полягає в тому, щоб додавати скомпрометовані паролі до бази даних якомога швидше після того, як вони стануть загальнодоступними, щоб користувачі могли бути попереджені.

Нові скомпрометовані паролі, надані NCA, тепер становлять приблизно 1/4 бази даних оригінальних записів Have I Been Pwned. Дамп паролів з Великобританії представляв зростання на 38% для цього конкретного сегмента бази даних. Було б непогано дізнатися більше про те, хто збирав паролі та звідки вони походять, але NCA наразі відмовляється надавати додаткові відомості.

Хоча 5,5 мільярда скомпрометованих паролів у базі даних Have I Been Pwned містять досить багато повторів, і хоча середній користувач Інтернету зараз має близько 100 облікових записів, які потребують входу (в ідеалі кожен з унікальними паролями), кількість унікальних паролів у база даних зараз нараховує 1 мільярд. Подальша передача інформації від ФБР і NCA, ймовірно, призведе до того, що в якийсь момент це число перевищить 1 мільярд. При загальній чисельності населення світу, що користується Інтернетом, близько 5 мільярдів, може статися так, що приблизно кожен п'ять використовуваних паролів у певний момент був зламаний та доступний для громадськості.

Деякі, наприклад Бабер Амін, головний виконавчий директор Veridium, бачать неминучу відповідь на це як кінець пароля повністю: «Це вказує на самий розмір проблеми, проблема полягає в паролях, архаїчному методі підтвердження власної правдивості. Якщо коли-небудь був заклик до дій, спрямованих на усунення паролів і пошук альтернативних, то це має бути це… за допомогою аналітичних інструментів, заснованих на штучному інтелекті, погані актори можуть почати визначати закономірності того, як людина створює паролі». Але деякі з запропонованих альтернативних рішень, наприклад біометрична

ідентифікація, потенційно можуть загрожувати конфіденційності та анонімності в Інтернеті.

Рон Бредлі, віце-президент відділу спільних оцінок, вважає, що паролі все ще є життєздатною формою безпеки, якщо користувачі краще дотримуються гігієни (і потенційно використовують менеджер паролів):

«Виходячи з того, що Інтернет стає все більш ворожим і щодня стає складнішим для навігації, він іноді нагадує мені попереджувальну лампу на приладовій панелі вашого автомобіля, яка горить так довго, що ви буквально більше її не бачите. Отже, на п'яту річницю щорічних резолюцій Рона (я придумую це, але говорю те саме протягом багатьох років), ось короткий список:

Купуйте та використовуйте універсальний менеджер паролів (безкоштовно, але ви отримуєте те, за що платите)

Увімкніть багатофакторну аутентифікацію всюди, де це можливо (особливо програми, які переміщують гроші)

Будьте частиною 1% людей, які не знають, що таке їх банківський пароль, тому що він занадто довгий і складний

Рішення приходять і зникають, і їх легко порушити, тому почніть з малого. Вирішіть додати один важливий обліковий запис до свого менеджера паролів, а решта піде. Не бійтеся функції скидання пароля, якщо пароль якимось чином зіпсовано, для цього і існує функція. Тримайте робочі паролі якомога далі від особистих. Нарешті, припустимо, що вас поранили, і захистіть себе відповідно». ***(Scott Ikeda. UK Law Enforcement Shares 585 Million Compromised Passwords With "Have I Been Pwned" Website, 225 Million Are New // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/uk-law-enforcement-shares-585-million-compromised-passwords-with-have-i-been-pwned-website-225-million-are-new/). 28.12.2021).***

***

«В наши дни существует бесчисленное количество компаний, которые в той или иной степени будут иметь доступ к вашим данным, а это означает, что вероятность утечки ваших личных данных намного выше, чем это могло быть раньше. В конце концов, каждая база данных является потенциальной точкой входа для злонамеренного хакера, поэтому люди должны быть осведомлены о том, как они могут защитить себя от утечки данных, а также о том, что им следует делать в случае взлома.

Согласно отчету, опубликованному ФБР, только в 2020 году было подано около 791000 жалоб на киберпреступления. Многие из этих киберпреступлений, по сути, связаны с ситуациями, когда кого-то обманом заставили отправить кому-то деньги, но даже если бы мы не принимали во внимание эти мошенничества, довольно ясно, что утечки данных - довольно обычное явление, и все обстоятельства были учтены и приняты во внимание. Это делает еще более важным иметь план игры, которому вы можете следовать, чтобы уменьшить часть ущерба.

Два самых серьезных примера утечки данных связаны с взломом вашего электронного адреса или кражей информации о вашем банковском счете. Последнее, очевидно, вызывает гораздо большее беспокойство из-за того, что это

та вещь, которая потенциально может позволить злоумышленнику получить доступ ко всем вашим финансам и потенциально относительно легко украсть ваши деньги. Однако взлом электронной почты может быть не менее опасным, поскольку многие другие ваши учетные записи будут связаны с вашей электронной почтой разными способами.

Если хакер получит доступ к вашей электронной почте, он сможет выбрать опцию «Забыли пароль» для любой учетной записи, связанной с этим электронным письмом. Затем они могут изменить ваш пароль и использовать эту учетную запись, как если бы она была их собственной, поэтому первый шаг, который вы должны предпринять, чтобы уменьшить размер ущерба, который может быть нанесен, - это включить двухфакторную аутентификацию. Это процесс, с помощью которого вы получите код на свой телефон, который будет иметь важное значение для входа в систему, тем самым предотвращая получение злоумышленниками незаконного доступа к вашим учетным записям.

Учитывая все вышесказанное, важно отметить, что лучшее время для принятия необходимых мер предосторожности - это до того, как нападение произойдет. Ваш аккаунт не обязательно будет взломан, если база данных компании будет взломана, но есть вероятность, что ваш пароль мог быть частью взлома. Одна вещь, которую вы можете сделать, - это использовать уникальные пароли для всех ваших учетных записей вместо одного и того же.

Основное преимущество этого заключается в том, что даже если злоумышленник узнает об одном из ваших паролей, это никоим образом не позволит им получить доступ к другим учетным записям, поскольку ни один из них не будет использовать тот же пароль. Вам придется иметь дело только с одним нарушением учетной записи, если вы примете такие меры предосторожности, вместо того, чтобы беспокоиться о нескольких нарушениях, произошедших одновременно. Еще многое предстоит сделать, но у вас, по крайней мере, будет немного меньше на вашей тарелке.

Использование диспетчера паролей также полезно по той причине, что он может помочь вам получить уведомление, если какой-либо из ваших паролей был частью утечки данных. Подобные шаги очень важны, потому что мы начинаем жить во все более взаимосвязанной технологической экосистеме, и есть много вещей, которые могут пойти не так, если мы не сможем этого понять. Практичность и осторожность - первый шаг к обеспечению безопасности в онлайн- или цифровом пространстве. Взгляните на приведенную ниже инфографику от SecurityHQ, чтобы узнать больше о том, как защитить вашу цифровую информацию». ***(Zia Muhammad. How to Deal With Personal Data Breaches // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/how-to-deal-with-personal-data-breaches.html). 18.12.2021).***

***

«Погана кібер-гігієна та слабкі паролі роблять організації вразливими до зловживання медичними даними. Майже третина опитаних IT - фахівців з

різних галузей промисловості повідомили слабке управління паролями в якості ключового фактора порушення безпеки, виявлено у звіті від GoodFirms.

Опитування показало, що 63% онлайн-користувачів змінюють свої паролі лише за запитом, а майже половина користувачів зберігають той самий пароль для кількох сайтів або програм. Більше половини користувачів також повідомили, що ділилися своїми обліковими даними для входу та паролю з колегами, членами родини та друзями.

Майже третина онлайн-користувачів повідомили, що вони стали жертвами порушень безпеки, спричинених слабкими паролями в минулому, хоча 88 відсотків респондентів сказали, що вони використовують двофакторну аутентифікацію.

«Безпека паролів є нагальною проблемою для компаній усіх вертикалей. Незалежно від того, чи відбувається це за допомогою грубої сили, неправильної конфігурації, передтекстування, програм-вимагачів, випуску бекдорів, зловживання привілеями чи інших методів злому, крадіжка паролів є неприємністю, з якою організації, співробітники і навіть експерти з кібербезпеки стикаються щодня», – йдеться у звіті.

«Хоча паролі можуть певною мірою захистити дані, повна безпека даних і конфіденційної інформації все ще залежить від того, наскільки добре керуються паролями. У більшості випадків уразливості паролів виникають через недотримання найкращих методів паролів, запропонованих експертами з кібербезпеки».

Існують різні способи, якими зловмисник може скористатися перевагами вразливості пароля, щоб отримати доступ до мережі. Фішинг є однією з найпоширеніших тактик, які використовують учасники загроз. Співробітники можуть отримати електронний лист із проханням скинути пароль, ввівши облікові дані, що змусить їх передати свої паролі та ідентифікатори користувачів хакерам.

Під час фішингової атаки хакери націлюють на користувачів електронні листи, які, схоже, надійшли від друзів, щоб змусити жертву натиснути посилання, згодом дозволивши хакерам отримати доступ до облікових даних. Атака грубої сили відбувається, коли хакери використовують метод проб і помилок, щоб вгадати паролі, поки не зможуть зламати код. Користувачі, які вибирають паролі без справжніх слів, мають більше шансів бути захищеними від атак грубої сили.

Уразливості паролів часто звинувачують на співробітниках, але організації зобов’язані навчати та надавати ресурси кібер-гігієни, щоб запобігти тому, щоб співробітники не полюбилися поширеним методам фішингу. Крім того, організації повинні забезпечити мережеву безпеку та системи виправлень, щоб підтримувати міцну позицію кібербезпеки.

Опитані IT-фахівці рекомендували користувачам створювати облікові записи лише в надійних компаніях, використовувати безпечні сеанси VPN та уникати словникових термінів під час створення паролів.

Організації повинні впровадити багатофакторну аутентифікацію, наймати етичних хакерів, щоб вони знайшли вразливості раніше, ніж справжні хакери, і прийняти політику блокування системи, щоб запобігти доступу до мережі хакерам, які намагаються вгадати паролі.

У звіті також припускається, що посилення входу за протоколом віддаленого робочого столу (RDP) має важливе значення для будь-якої організації, щоб бути попереду кіберзагроз. Експерти рекомендували створювати довгі та складні паролі для RDP, щоб запобігти доступу хакерів до критичних даних». ***(Jill McKeon. Weak Passwords, Poor Cyber Hygiene Invite Healthcare Data Breaches // TechTarget, Inc. (https://healthitsecurity.com/news/weak-passwords-poor-cyber-hygiene-invite-healthcare-data-breaches). 13.12.2021).***

***

«Преемник Facebook Meta в четверг заявила, что аннулировала 1500 учетных записей в социальных сетях, которые использовались семью фирмами по найму для проведения онлайн-атак против критиков правительства и членов гражданского общества.

Эти учетные записи в основном использовались для наблюдения за целями и привлечения их к посещению вредоносных веб-сайтов или получения сообщений с заминированными ловушками, которые, как правило, ставили под угрозу их устройства и онлайн-профили. Десятки тысяч людей, потенциально являющихся мишенями этих групп, были предупреждены в частном порядке через Facebook.

«Глобальная индустрия слежки по найму нацелена на людей, чтобы собирать информацию, манипулировать и взламывать их устройства и учетные записи через Интернет», - сказал Дэвид Агранович, директор по устранению угроз, и Майк Двилянски, глава отдела расследований кибершпионажа, в своем блоге.

«Хотя эти «кибернаемники» часто заявляют, что их услуги нацелены только на преступников и террористов, наше многомесячное расследование пришло к выводу, что нападения на самом деле являются неизбирательными и включают журналистов, диссидентов, критиков авторитарных режимов, семьи оппозиции и активистов-правозащитников».

Агранович и Двилянски заявили, что, хотя израильская компания NSO Group, производитель шпионского ПО Pegasus, получила широкое внимание как частного, так и государственного сектора за содействие слежке при поддержке государства, существует более широкая глобальная индустрия кибернаемников.

Эта отрасль недавно привлекла внимание законодателей после того, как WhatsApp запустил в октябре 2019 года иск против NSO Group за якобы помощь в слежке за своими клиентами. Microsoft выступила против кибернаемников в 2020 году, и в прошлом месяце Apple решила подать иск против NSO Group.

В среду 18 американских законодателей-демократов обратились с просьбой о том, чтобы NSO Group, DarkMatter Group из ОАЭ и Nexa Technologies и Trovicor из ЕС подверглись санкциям в соответствии с Глобальным законом Магнитского за допущение нарушений прав человека. А ранее в этом месяце 81 группа гражданского общества обратилась к законодателям ЕС с просьбой наказать NSO Group за содействие нарушениям прав человека.

Группа NSO постоянно настаивала на том, что продает свое программное обеспечение только для предотвращения террора и преступности, и после этого не использует свое программное обеспечение - это требование оспаривается в судебных процессах против производителя шпионского ПО.

В электронном письме для The Register в ответ на просьбу законодателей США ввести жесткие санкции против бизнеса, официальный представитель настаивал на том, что разработчик приветствует регулирование.

«NSO выступает за международное регулирование отрасли, чтобы гарантировать, что критически важные технологии, которые спасают жизни, такие как мы развиваем, не могут быть использованы правительствами разных стран», - сказал представитель. «Несмотря на то, что мы уже внедряем нашу уникальную политику соответствия, мы стремимся принять участие в любых усилиях по введению дополнительных правил и ограничений».

Мета не может назначить столь серьезное наказание, как правительственные санкции. Вместо этого он закрыл сотни учетных записей в своих сервисах Facebook и Instagram за нарушения стандартов сообщества и условий обслуживания и запретил ответственным лицам пользоваться своими услугами. Он также поделился своими выводами с другими платформами и исследователями и заблокировал поддельные домены.

Спорные счета использовались для проведения разведки; взаимодействовать с целями (ради завоевания доверия и социальной инженерии); а также для взлома других онлайн-аккаунтов целей с помощью фишинга или взлома их устройств с помощью эксплойтов уязвимостей системы безопасности. Сообщается, что фальшивыми учетными записями управляют Cobweb Technologies (200 учетных записей), Cognyte (100), Black Cube (300), Bluehawk CI (100), BellTroX (400), Cytrox (300) и неизвестная организация в Китае (100).

Meta также сообщила, что уведомила около 50 000 человек, которые, по ее мнению, стали объектами наблюдения за наемными объектами.

Фейковые новости

Имейте в виду, что Facebook, как и другие службы социальных сетей, в течение многих лет не мог помешать людям регистрировать поддельные учетные записи. В период с октября по декабрь 2020 года Facebook заявила, что отключила более 1,3 миллиарда из них. Нет оснований полагать, что эти фирмы не смогут воссоздать новые поддельные учетные записи, учитывая изощренность их кибероперацій.

В отчете об очистке аккаунтов Meta [PDF] Агранович, Двилянски и Натаниэль Глейхер, глава отдела политики безопасности, признают это, но выражают надежду, что их игра «Whac-a-Mole» против этих фирм станет проще.

«Организации, стоящие за этими операциями по наблюдению, настойчивы, и мы ожидаем, что они будут развивать свою тактику», - говорится в их отчете. «Однако наши системы обнаружения и исследователи угроз, а также другие группы в более широком сообществе безопасности продолжают совершенствоваться, чтобы им все труднее оставаться незамеченными».

Citizen Lab, исследовательская группа по кибербезопасности из Университета Торонто в Канаде, в четверг опубликовала отчет с участием одной из этих компаний, Cytrox, которая производит шпионское ПО под названием Predator.

Исследовательская группа сообщила, что двое египтян - политик в изгнании Айман Нур и ведущий популярной новостной программы, пожелавшие остаться

неизвестными - были взломаны в июне 2021 года с помощью шпионской программы Cytrox's Predator.

Нур стал мишенью двух разных клиентов организации, подозреваемой в том, что это правительство Египта. Его iPhone, работающий на тогдашней iOS 14.6, был взломан Predator и Pegasus NSO Group через ссылки с одним или нулевым щелчком, отправленные из WhatsApp. В атаке Pegasus использовался эксплойт FORCEDENTRY от NSO Group (CVE-2021-30860). Входной эксплойт, использованный шпионским ПО Predator и считающийся уязвимостью нулевого дня, не раскрывается. Похоже, что при взломе устройства были задействованы ссылки в изображениях, доставленных через WhatsApp.

Citizen Lab заявила, что раскрыла данные судебно-медицинской экспертизы Apple и Meta, которой принадлежит WhatsApp, и отметила принудительные меры Meta в отношении учетных записей в социальных сетях, связанных с Cytrox.

Мета заявляет, что выявила клиентов Cytrox в Египте, Армении, Греции, Саудовской Аравии, Омане, Колумбии, Кот-д'Ивуаре, Вьетнаме, Филиппинах и Германии, и что фирма оказывала услуги злоумышленнику, известному охранным фирмам как Сфинкс.

Citizen Lab заявила, что можно ожидать, что наемные фирмы-шпионы будут продолжать удовлетворять потребности автократических правительств до тех пор, пока национальные и международные правила не запретят такие услуги.

«При отсутствии международных и внутренних правил и гарантий журналисты, правозащитники и оппозиционные группы будут продолжать подвергаться хакерским атакам в обозримом будущем», - заявили в группе». ***(Thomas Claburn. Facebook locks out 1,500 fake accounts used by cyber-spy firms to snoop on people, alerts 50k potential targets // The Register (https://www.theregister.com/2021/12/17/cyber_spying_firms_facebook_meta/). 17.12.2021).***

***

Кіберзлочинність та кібертерроризм

«Цього року відбулося значне збільшення шкідливих атак на сервери та мережі компанії. Звіт, опублікований Ресурсним центром Identify Theft, показав, що порушення даних, про які повідомлялося в Сполучених Штатах із січня по вересень 2021 року, перевищили загальну кількість порушень, про які повідомлялося за весь 2020 рік. Збільшення було визначено на 17 відсотків.

За три місяці до 2021 року атаки не сповільнюються. Фактично, нещодавній інцидент показує масштаби небезпеки, з якою стикаються організації. Цього місяця експерти з кібербезпеки повідомили, що найбільший ботнет, який спостерігали за останні шість років, заразив понад 1,6 мільйона різних пристроїв. Атака була зосереджена переважно в Китаї. Кінцевою метою цього конкретного ботнету є в кінцевому підсумку монтувати розподілені атаки відмови в обслуговуванні (DDoS). Другорядною метою було вставлення реклами на веб-сайти HTTP, які відвідуватимуть користувачі.

Ботнет, який був ідентифікований командою безпеки Qihoo 360 Netlab, отримав назву «Рожевий», оскільки багато назв функцій бота починалися зі слова «рожевий».

Рожевий ботнет — це вид шкідливого коду, який може мати потенційно серйозні наслідки для мережі організації. Якщо його не помітити, це може завдати серйозної шкоди будь-якому бізнесу. Ботнет і його потенціал хаосу підкреслюють той факт, що постійний моніторинг системи, щоб переконатися, що немає вразливостей, надзвичайно важливий.

Це підкреслює необхідність такого методу безпеки, як моделювання злому та атаки, щоб допомогти пом'якшити випадки потенційної атаки. Метод тестування комп'ютерної безпеки, такий як BAS, імітує атаки на систему без шкоди для цілісності та безпеки мережі. Він буде імітувати потенційні шляхи атак на системи та використовувати ті ж методи, які використовуються зловмисниками для атаки на мережі.

Метод ботнету Pink

Як ботнет Pink потенційно проникає в системи? Основними точками входу в нього є оптоволоконні маршрутизатори на основі MIPS. Він використовує поєднання сторонніх платформ, таких як GitHub, мережі P2P і сервери C2, щоб намагатися контролювати потік комунікації. Неприємне тут полягає в тому, що він також намагатиметься зашифрувати канали передачі, щоб перешкодити контролю пристроїв.

Аналіз було проведено після того, як неназваний постачальник і технічна група/координаційний центр реагування на надзвичайні ситуації комп'ютерної мережі або CNCERT/CC координували виявлення та виправлення ботнету. Аналіз показав, що ботнет був досить хитрим.

По суті, Pink боротиметься з постачальником, намагаючись зберегти контроль над зараженими пристроями. Коли постачальник намагається вирішити проблему, оператор бота буде знати, які дії він виконує одночасно. Потім оператор створить різні оновлення мікропрограми на заражених маршрутизаторах. Цей метод перетворює його на гонку між постачальниками та майстром ботів – і в такій ситуації здавалося б, що перевагу має майстер бота.

Вплив ботнету Pink

За даними охоронних компаній, понад 96 відсотків зомбі-вузлів були розташовані в Китаї. Ботнету вдалося проникнути на багато пристроїв і встановити шкідливі програми, які використовували вразливості нульового дня, виявлені на пристроях мережевого шлюзу. Хоча значна частина зараженого обладнання була відремонтована, кажуть, що ботнет Pink все ще залишається активним, і за оцінками, понад 100 000 вузлів все ще заражені. На сьогоднішній день Pink приписують понад 100 DDoS-атак, і це показує, як ботнет може бути надзвичайно потужним інструментом для кібератак на IT-інфраструктуру.

Важливість BAS

Розгортання ботнету Pink у дикій природі та те, як його власний метод атаки ускладнює відновлення, одразу підкреслює давнє прислів'я, яке можна застосувати до кібербезпеки – профілактика завжди краще, ніж лікування.

Такий метод безпеки, як моделювання порушення та атак, ідеально інкапсулює цю парадигму запобігання надмірному лікуванню.

Як згадувалося вище, BAS, як метод тестування безпеки, забезпечує безперервний спосіб перевірки стану безпеки будь-якої організації. За проектом, BAS виконуватиме дії, які будуть імітувати реальні реальні загрози, які зустрічаються в дикій природі, щоб гарантувати, що засоби контролю безпеки в організації є достатньо надійними, щоб уловити та усунути ці дії. BAS використовує базу знань MITER ATT&CK — вичерпний збірник усіх відомих тактик і прийомів кібератак, які використовуються суб'єктами загроз у всьому світі. Використання цієї бази знань означає, що BAS фактично використовуватиме відомі дії кіберзлочинців.

Застосовуючи ці контрольовані дії атаки в мережі, команда з кібербезпеки може визначити будь-які недоліки в IT-інфраструктурі, які вони потім можуть виправити або виправити залежно від серйозності слабкості.

Команди з кібербезпеки дуже виграють від впровадження BAS, оскільки це більш рентабельне та ефективне рішення безпеки. Дії BAS автоматизовані, що означає менше проблем з точки зору накладних витрат. Його навіть можна налаштувати на багаторазовий або безперервний запуск, що забезпечує рівень оцінки безпеки, який було б важко зробити, якби все це виконували люди. Автоматизація також має ще одну перевагу — менше людського втручання означає усунення людських помилок, які, як виявилося, є основною причиною злому даних. Насправді, звіт показав, що 90 відсотків випадків порушення даних можна пояснити людськими помилками та помилками.

Висновок

Поширення атак на кібербезпеку за останній рік показує, що кіберзлочинці наполегливо працюють, намагаючись використовувати організації для своїх підступних цілей. Нещодавно відкритий ботнет Pink, який поширився на сотні тисяч пристроїв у Китаї, чітко ілюструє цю небезпеку. Хоча атаки та експлойти є цілком реальною проблемою, команди з кібербезпеки можуть пом'якшити, якщо не усунути вразливості в організації, запровадивши сувору політику безпеки, яка покликана запобігти атакам до того, як це станеться. Симуляція злому та атаки є одним із найефективніших методів забезпечення надійності та безпеки організації. ***(EVAN MORRIS. Largest Botnet Malware Highlights Need for Breach and Attack Simulation // Xpective, Inc. (https://techspective.net/2021/12/10/largest-botnet-malware-highlights-need-for-breach-and-attack-simulation/). 10.12.2021).***

***

«…Какие вызовы необходимо будет преодолеть в области кибербезопасности в 2022 году?

Империя вымогателей

Анализ, проведенный исследовательским подразделением SILIKN, показал, что на конец сентября 2021 года было совершено около 640 миллионов попыток атак с использованием программ-вымогателей, поэтому к концу года это число, по прогнозам, приблизится к 890 миллионам попыток. В секторе банковских и

финансовых услуг только в Мексике количество попыток атак программ-вымогателей увеличилось более чем на 2500% в 2021 году.

Какие сектора были и будут наиболее уязвимыми для программ-вымогателей в 2022 году?

Как мы знаем, программы-вымогатели стали одной из самых быстрорастущих областей киберпреступности в новейшей истории. Следует отметить, что в 2021 году атаки программ-вымогателей происходили каждые 10,2 секунды.

Ущерб от программ-вымогателей в 2021 году оценивается примерно в 32 миллиарда долларов. К сожалению, прогнозируется, что к 2030 году ущерб от атак программ-вымогателей достигнет 299 миллиардов в год, причем атаки будут происходить каждые 1,8 секунды.

Важно отметить, что текущие отчеты содержат разные данные (отчасти потому, что многие компании, пострадавшие от атак программ-вымогателей, не сообщали о таких инцидентах), поэтому трудно узнать точные данные о пострадавших организациях. Но по данным исследовательского подразделения SILIKN, 57,8% организаций в Мексике пострадали от атак программ-вымогателей и в течение 2021 года в среднем неактивны в течение девяти дней. И хотя общие цифры могут иметь определенные различия, это правда, что программы-вымогатели могут взорваться в следующем году.

Секторы, наиболее пострадавшие от программ-вымогателей в 2021 году (и, по оценкам, к 2022 году серьезных изменений не произойдет):

Правительство: 22,9%

Финансовые услуги: 18,7%

Услуги здравоохранения: 15,3%

Образование: 12,4%

Технологии: 7,9%

Производство: 4,7%

Розница - Розничные продажи: 3,1%

Прочие отрасли: 15,0%

Узурпация фирменного стиля

В этом году большое внимание было уделено программам-вымогателям, но одна из тенденций, которые мы увидим в 2022 году, - это клонирование веб-сайтов и проблемы с онлайн-мошенничеством. Потребителей и бренды обманывают кибератаки, совершаемые за рубежом. Мошенники нацелены на известные бренды, будь то банки, технологические компании или даже криптовалюты, в надежде, что потребитель не поймет, что ссылка, по которой они нажимают, ведет на клон настоящего веб-сайта. Думая, что он находится в нужном месте, потребитель вводит свой логин и другую конфиденциальную информацию, что приводит к краже учетных данных, захвату учетных записей и более серьезным проблемам.

Противодействие клонированию веб-сайтов требует наступательной атаки. Организации должны будут использовать инструменты кибербезопасности, которые могут выявлять мошенничества, как только они материализуются, и закрывать их до того, как они достигнут потребителей, сотрудников или других онлайн-пользователей.

Инсайдеры продолжают настораживать организации

В 2020 году сотрудники оставались дома, чтобы избежать заражения и распространения COVID-19. В 2021 году многие сотрудники останутся дома, потому что хотят чего-то большего, чего не предлагает их работа.

Кибербезопасность, которая уже решала проблему нехватки навыков и миллионов вакансий, теперь затронута Великой отставкой, когда люди меняют работу, забирая с собой свои знания. Будь то досрочный выход на пенсию или переход на менее напряженную работу или карьеру, перед организациями будет стоять задача восполнить растущий пробел в знаниях, и это должно быть главным приоритетом.

Инновации и обучение темной стороне

Ключевым моментом, который следует учитывать в 2022 году, является готовность и новаторские подходы киберпреступных групп к разработке, распространению и запуску программ-вымогателей. К сожалению, преступники лучше обучены и финансово мотивированы для совершения этих атак.

Киберпреступные группы действуют структурированно. В дополнение к тому факту, что, в отличие от властей и правительств, нет бюрократии, и они делятся информацией, методологиями, инструментами и, как правило, поддерживают тех, кто меньше разбирается в технических вопросах.

Поскольку ФБР, АНБ, Интерпол, Европол и другие агентства охотятся за киберпреступниками, которые атакуют крупные корпорации, правительства или критически важные инфраструктуры наиболее развитых стран, преступники воспользуются этим, чтобы проводить более масштабные, более частые и изощренные атаки. против организаций. в Мексике, где кибербезопасность все еще является медленно развивающейся проблемой.

В 2022 году мы увидим экспоненциальный рост атак программ-вымогателей на малые и средние компании (МСП), особенно те, которые расположены в Мексике и других странах Латинской Америки. Кроме того, модель RaaS позволит все большему количеству преступных группировок действовать и расширять свои операции в разных частях мира. Предполагается, что в 2022 году Латинская Америка станет одним из наиболее атакованных регионов.

И Организация американских государств, и Межамериканский банк развития указали, что киберпреступности иногда удавалось превосходить незаконный оборот наркотиков - как по размаху, так и по прибылям, - для которых, по прогнозам, 2022 год будет сложным для властей страны. по всему миру, поскольку мы видим все больше и больше союзов между торговцами наркотиками и киберпреступниками.

Наихудшие киберугрозы, вопреки тому, что появляется в СМИ и социальных сетях, - это не программы-вымогатели, DDos-атаки, социальная инженерия или фишинг. Наихудшая киберугроза - это способность киберпреступных групп действовать, организовываться, атаковать, учиться, понимать, делиться информацией и быть гораздо лучше подготовленными, чем власти и правительства.

Это реальная угроза: легкость, с которой киберпреступники действуют анонимно и применяют все свои экспертные знания для совершения злонамеренных действий. Понимание того, как работают эти группы

киберпреступников, имеет решающее значение для их остановки». ***(Vнctor Ruiz. Cybersecurity challenges in 2022: are we ready to stop cyberattacks? // Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/402132). 10.12.2021).***

***

«Sainsbury's, друга за величиною мережа супермаркетів у Великобританії, підтвердила, що вона зазнала збою в системі нарахування заробітної плати через кібератаку, яка вплинула на її хмарного постачальника послуг з нарахування заробітної плати - американську транснаціональну компанію Ultimate Kronos Group, яка постраждала від кібератака тижнем раніше.

Речник Sainsbury's повідомив Information Security Media Group: «Ми тісно спілкуємося з Kronos, поки вони розслідують проблему системи. Тим часом у нас є надзвичайні заходи, щоб переконатися, що наші колеги продовжують отримувати свою зарплату».

Згідно з повідомленням BBC, Sainsbury's втратила «тижневу кількість даних для своїх 150 000 співробітників, які працюють у Великобританії».

«Кілька відділів, включаючи нарахування заробітної плати, людські ресурси (HR) та бухгалтерію, тепер використовують історичні дані та робочі моделі, щоб переконатися, що працівникам вчасно отримують правильну суму», – повідомляє BBC.

Стівен Хоуп, генеральний директор і співзасновник Authlogics, каже: «Плани на випадок непередбачених ситуацій є ключовими. У цьому випадку заспокійливо знати, що Sainsbury's має надзвичайні обставини, щоб забезпечити співробітникам оплату на Різдво, особливо тому, що на даний момент працівники неоплачувані року може бути дорогим у багатьох відношеннях».

Коли ISMG запитав Sainsbury's про вплив цього збою, чи постраждали його дані в результаті інциденту з програмним забезпеченням-вимагачем Kronos і очікувані терміни для повного вирішення проблеми, речник сказав: «Щодо подальшого на цьому етапі, найкраще говорити до Кроноса».

Ultimate Kronos Group, або UKG, повідомила ISMG: «Ми визнаємо серйозність проблеми і мобілізували всі доступні ресурси для підтримки наших клієнтів і старанно працюємо над відновленням постраждалих послуг».

Ні Sainsbury's, ні Kronos не зробили офіційної заяви про наслідки відключення.

Оновлення атаки Kronos

У оновленні, опублікованому в неділю, компанія Kronos підтвердила, що дізналася про кібератаку 11 грудня, і її первинне розслідування встановило, що це була атака програмного забезпечення-вимагача. Згідно з оновленням, атака вплинула на середовище Kronos Private Cloud - або KPC, в якому розміщуються UKG Workforce Central, UKG TeleStaff, Healthcare Extensions і Banking Scheduling Solutions.

У вівторок KPC оновила свій список поширених питань, пов’язаних з цим інцидентом, і повідомила клієнтів, що вплинули лише згадані продукти та рішення. «Kronos Private Cloud — це приватне середовище, яким керує UKG, де ми

розміщуємо рішення з одним клієнтом. На відміну від цього, UKG Dimensions, UKG Ready, UKG Pro та UKG HR Service Delivery — це повністю окремі бази коду, які працюють у абсолютно окремих середовищах і хмари з Kronos Private Cloud», – йдеться у повідомленні.

«Ми працюємо з провідними експертами з кібербезпеки, і під час наших розслідувань на сьогоднішній день не було виявлено жодних доказів впливу на інші хмарні середовища», — підтверджує Кронос.

Окремі локальні рішення для клієнтів UKG Workforce Central і TeleStaff також не постраждали від цього інциденту і залишаються функціональними, повідомляє UKG у своєму нещодавньому оновленні.

Розгнівані клієнти

Клієнти UKG висловили занепокоєння щодо вирішення всієї ситуації з боку компанії. У твіті Вілл Вейдер, інформаційний директор PeaceHealth, назвав інцидент «катастрофою».

Речник PeaceHealth повідомив ISMG, що на нього не вплинула атака програм-вимагачів Kronos і що Вайдер висловив свою особисту думку.

У каналі спільноти UKG клієнти висловили гнів на компанію за непрозорість щодо розслідування та термінів відновлення нормальної роботи.

«Зв'язок із UKG щодо цієї ситуації був поганим. Я адміністратор нашої системи і не отримав електронної пошти, про яку йдеться вище. Це буде величезною проблемою для наших агентств», – каже клієнт з іменем користувача dgraves51530.

Інший клієнт запитує, чому для відновлення служб не використовувалися резервні копії, а інший згадує про блокування/вимкнення всіх з'єднань ADFS і LDAP до UKG/Kronos Cloud, називаючи це «ненадійним об'єктом».

Альтернатива безперервності бізнесу

Атака програм-вимагачів на Kronos вплинула на кількох клієнтів UKG – хоча імена не згадуються, – але найбільше постраждали погодинні працівники, які не можуть відстежувати свої зміни та виходити з них, стежити за зарплатою чи відстежувати оплачувану відпустку. Ашик Ахмед, генеральний директор компанії, що займається плануванням робочого часу та постачальником рішень для управління змінами.

Він каже, що атака на Kronos вплинула на мільйони змінних працівників, поставивши під загрозу їхню оплату та оплачувану відпустку під час свят, і що, щоб допомогти підприємствам, що застрягли, Депуті надає клієнтам Kronos альтернативу безперервності бізнесу без додаткових витрат, поки криза не буде вирішена. Це дозволить їм продовжувати складати графік роботи персоналу, керувати часом і відвідуваністю, а також розраховувати заробітну плату за допомогою точних табелів обліку робочого часу, — каже Ахмед.

Kronos рекомендував своїм клієнтам оцінити та впровадити альтернативні протоколи безперервності бізнесу, — каже Ахмед: «І це саме те, що ми плануємо зробити — дати альтернативу, поки ситуація не буде вирішена», — сказав він ISMG». ***(Mihir Bagwe. Attack on Kronos Causes Sainsbury's Payroll System Outage // Information Security Media Group, Corp. (https://www.govinfosecurity.com/attack-on-kronos-causes-sainsburys-payroll-system-outage-a-18172). 22.12.2021).***

***

«10 грудня шведський виробник автомобілів Volvo Cars заявив, що третя сторона отримала незаконний доступ до одного з його сховищ і що суб'єкти загрози викрали «обмежену кількість» майна компанії, що займається дослідженнями та розробками під час вторгнення.

Злом даних Volvo є останньою кібератакою, спрямованою на автомобільну промисловість. Виробники автомобілів не тільки запобігають традиційним формам кібератак, таким як програмне забезпечення-викуп, але також стикаються з загрозами, що виникають через телематику та підключені компоненти транспортних засобів. Масштаб, геолокація та величезні обсяги даних, які генеруються з мільйонів кінцевих точок, додають складності.

Останні кібератаки в автомобільному секторі

Дослідження показують, що у 2020 році було зареєстровано понад 200 інцидентів із кібербезпекою, і цього року також спостерігається значна частка кібератак.

У лютому американська автомобільна компанія Kia Motors зазнала атаки програм-вимагачів з боку банди DoppelPaymer. Згідно зі звітом Bleeping Computer, інцидент був подвійним вимаганням, коли банда програм-вимагачів вимагала 20 мільйонів доларів за ключ дешифрування на додаток до своєї гарантії, що вона не дасть витоку даних.

Після інциденту Kia Motors зазнала «загальнонародного відключення IT», що вплинуло на мобільні додатки, телефонні послуги, платіжні системи, веб-сайти для користувачів і додатки внутрішнього ланцюга поставок.

У червні особиста інформація 3,3 мільйона клієнтів, включаючи конфіденційні дані 90 000 клієнтів Volkswagen і Audi, була розкрита після несанкціонованого доступу третьої сторони. Розслідування показало, що дані залишалися незахищеними протягом 21 місяця.

У жовтні німецький постачальник автокомпонентів Ebersрdcher Group був змушений відправити свою робочу силу в оплачувану відпустку після того, як цілеспрямована кібератака пошкодила її IT-системи, йдеться у звіті новинної платформи The Record.

У той час як більшість попередніх атак або збивали діяльність компанії, або вплинули на ланцюжок поставок фірми, кібератака на Volvo Cars була спрямована спеціально на дані дослідження фірми.

Інцидент відкриває питання щодо кіберстійкості автомобільних компаній, особливо щодо захисту інтелектуальної власності.

Захист даних НДДКР

«Захист ключових активів, таких як дослідницькі дані, є особливо важливим на високоінтенсивному ринку, як-от автомобільний. Виробники повинні продовжувати дивитися на те, як вони обробляють, зберігають і обмінюються даними, щоб захистити ці активи», – Кріс Кларк, архітектор рішень в автомобільному програмному забезпеченні. та безпеки в автомобільній технологічній компанії Synopsys Inc., розповідає Information Security Media Group.

Полін Лоссон, директор з кібероперацій французької фірми із захисту цифрових ризиків CybelAngel і колишній аналітик з безпеки Міністерства оборони Франції, визначає два основних ризики, пов'язані з даними досліджень і розробок або інтелектуальною власністю, які скомпрометовані через програмне забезпечення-викуп або крадіжку даних: «Один з ризиків полягає в тому, щоб побачити Дослідження та розробки, якими ділиться конкуренти, можуть зіпсувати роки інвестицій у дослідження. Інший трапиться, якщо погані хлопці готові використати цю інформацію, щоб розпочати нову атаку", - розповідає вона ISMG.

Лоссон каже, що глибше знання програмного забезпечення автомобілів може дати хакерам інструменти для націлювання на самі автомобілі та клієнтів на кінці ланцюжка.

Більшість інцидентів зі зломом даних є результатом того, що дані досліджень і розробок залишаються в незахищеному хмарному відділенні, диску або пристрої, підключеному до мережі, каже вона. Походженням, у більшості випадків, є третя чи четверта сторона, яка проявила недбалість.

Щоб захистити інтелектуальну власність виробників автомобілів або автокомпонентів, Вільям Теллес, головний спеціаліст із інформаційної безпеки Autoglass Brazil, каже, що компанії повинні продовжувати розвивати засоби контролю доступу, щоб запобігти як несанкціонованому доступу, так і законному доступу, а також враховуючи зміни в поведінці. За його словами, недостатньо захистити середовище за допомогою технологій, які обмежують доступ із підозрілих країн чи IP-адрес.

«Велика проблема виникає, коли законну особистість викрадають і використовують у зловмисний спосіб». Щоб запобігти цьому, каже Telles, організації повинні вдосконалити управління ідентифікацією та доступом як перший крок у захисті даних досліджень і розробок.

Складність ланцюга поставок

Лоссон каже, що довжина та складність ланцюга поставок в автомобільній промисловості є основною слабкістю галузі, і CISO повинні співпрацювати з іншими відділами — закупівель, продукту, маркетингу та логістики — щоб краще оцінити своїх партнерів з точки зору інформаційної безпеки.

Кларк каже: «Програмне забезпечення лежить в основі інновацій, і нещодавня хвиля програм-вимагачів і атак на ланцюжок поставок продемонструвала, що зламане програмне забезпечення може мати руйнівний вплив на організацію».

Повторюючи наказ адміністрації Байдена з кібербезпеки, Харшіні Кері, стратег із інформаційної безпеки та консультант у фірмі з кібербезпеки Trustwave, каже, що ведення списку програмного забезпечення та активів значною мірою допомагає захистити інтелектуальну власність в автомобільних компаніях.

Заходи безпеки наступного покоління

Деякі експерти з автомобільної безпеки кажуть, що поява телематики та підключених пристроїв в автомобільному секторі збільшила поверхню атаки, і тому традиційних методів захисту IT, таких як тестування на проникнення, управління життєвим циклом програмного забезпечення та створення операційних центрів безпеки, просто недостатньо.

«Прагнення скоротити 200 платформ, які повинні підтримуватися до 20 або менше, є постійно зростаючою потребою, так само як і зосередженість на розробці внутрішньої SOC та мереж нового покоління в автомобілі», - каже Кларк.

Автомобільний SOC, або ASOC, розроблявся протягом кількох років. Керування ASOC значно відрізняється від використання традиційного IT SOC. Як каже компанія Argus з автомобільної та авіаційної кібербезпеки: «Ефективне запуск процесу ASOC потребує постійного вдосконалення та розширення бібліотеки варіантів використання автомобільної техніки».

Це означає, що виробникам автомобілів доведеться постійно додавати нові канали даних і створювати нові правила виявлення. І ASOC стикаються з підвищеними проблемами, пов'язаними з масштабом і геолокацією, а також необхідністю керувати мільйонами кінцевих точок, кожна з яких генерує величезні обсяги даних. Це проблеми, з якими не стикаються традиційні IT SOC.

Вилучити групу програм-вимагачів, відповідальну за порушення Volvo?

У той час як такі публікації, як Bleeping Computer і Autoevolution повідомили, що група вимагачів Snatch взяла на себе відповідальність за напад на Volvo Cars, шведський автовиробник говорить ISMG, що не писали або писали групу хакерів.

«Ми знаємо, що організація під назвою Snatch взяла на себе відповідальність за крадіжку майна, яку Volvo Cars розслідує. Volvo Cars не контактує з третьою стороною», – каже Мерхавіт Хабте, глобальний відділ зв'язків з громадськістю Volvo Cars.

За її словами, компанія співпрацює зі сторонніми фахівцями, триває розслідування порушення. Компанія відмовилася поділитися своїми висновками про те, як хакери отримали доступ до її інтелектуальної власності та скільки даних досліджень і розробок було вкрадено». ***(Soumik Ghosh. Volvo Breach Highlights Need for Securing Auto R&D Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/volvo-breach-highlights-need-for-securing-auto-rd-data-a-18146). 23.12.2021).***

***

«Міністерство оборони Бельгії, яке відповідає за національну оборону та бельгійські військові, оголосило в понеділок, що стало жертвою кібератаки, за словами чиновників, пов'язаної з широко поширеною вразливістю Apache Log4j. Як повідомляється, напад «паралізував діяльність міністерства на кілька днів».

У коментарях, наданих бельгійській газеті De Standaard, військовий представник заявив, що атака на IT-мережу міністерства була вперше виявлена минулого четверга, і для ізоляції постраждалих районів були вжиті «карантинні заходи». Невідомо, чи це був інцидент із програмним забезпеченням-вимагачем.

У міністерстві повідомили бельгійській газеті, що кібератака сталася через Log4j від Apache, який надає можливості ведення журналів для додатків Java і широко використовується, в тому числі для програмного забезпечення веб-сервера Apache.

Бельгійський командувач Олів'є Северен також сказав виданню: «Все вихідні наші команди були мобілізовані, щоб контролювати проблему, продовжувати нашу діяльність та попереджати наших партнерів».

Звертаючись до Facebook після атаки, Міністерство оборони пише: «Через технічні проблеми ми не можемо обробити ваші запити через mil.be або відповісти на ваші запити через Facebook. Ми працюємо над рішенням і дякуємо вам за ваше розуміння».

Представники як міністерства, так і міністра оборони Людівін Дедондер не відповіли на запит медіагрупи Information Security Media Group про коментар. Бельгійські чиновники також не повідомили De Standaard про особливості нападу.

Бельгійський інцидент є однією з перших гучних атак, пов'язаних із вразливістю Log4j, хоча експерти з кібербезпеки попереджають про активне сканування та використання вразливості віддаленого виконання коду.

Небезпечно високого ступеня тяжкості

Уразливість, яка спочатку відстежувалась як CVE-2021-44228 і була виявлена в бібліотеці журналів Java Apache Log4j, може призвести до повного захоплення сервера і залишити вразливими незліченну кількість програм. Компонент використовується для реєстрації подій і є частиною десятків тисяч розгорнутих програм і хмарних сервісів. CVE-2021-44228 має рейтинг серйозності 10 за шкалою від 1 до 10, оскільки зловмисники можуть дистанційно використовувати його без будь-якого введення з боку жертви, і для його розгортання потрібні обмежені технічні можливості.

Після виявлення недоліку некомерційна організація, яка обслуговує Log4j, Apache Software Foundation, випустила кілька нових версій, включаючи останню версію 2.17, щоб виправити подальші серйозні вразливості відмови в обслуговуванні.

Останній патч відповідає директиві щодо надзвичайних ситуацій, виданій Агентством США з кібербезпеки та безпеки інфраструктури, яка вимагає від федеральних цивільних відомств та агентств «негайно» виправити свої системи або вжити відповідних заходів щодо пом'якшення наслідків. Раніше CISA давала агентствам до п'ятниці, щоб виправити подвиги Log4j через свій Каталог відомих використаних вразливостей.

Dridex, Meterpreter, що використовується в атаках

Група досліджень безпеки Cryptolaemus тепер встановила зв'язок між уразливістю Log4j і банківським шкідливим програмним забезпеченням Dridex, а також інструментом для тестування пера Meterpreter для пристроїв Linux, який потенційно може дозволити бічні переміщення та вилучення даних.

Не вистачає нових спроб атаки, що виникли внаслідок використання Log4Shell, включаючи діяльність національних держав та групи кіберзлочинних, які запускають нові фішингові кампанії. Деякі експерти повідомили минулого тижня, що вони виявляли близько 100 000 спроб атаки на хвилину, пов'язаних з Log4j (див.: Apache Log4j: Нові вектори атак, виявлені програми-вимагачі).

Dridex, відстежений CISA як AA19-339A, використовувався разом із уразливістю Log4j з боку загроз для запуску атак на системи Windows. Експерти

кажуть, що оператори шкідливих програм також використовують такі інструменти, як Meterpreter, для збереження в мережах, включаючи пристрої Linux.

За даними CISA, Dridex, одна з найбільш поширених штамів шкідливого програмного забезпечення проти фінансових установ, була вперше виявлена в 2012 році. Ранні версії Dridex використовувалися для перехоплення транзакцій клієнтів і збору облікових даних для входу. З тих пір банківський троян використовувався для зараження пристроїв програмним забезпеченням-вимагачем і був пов'язаний із горезвісною російською хакерською групою Evil Corp.

Зловмисники традиційно просувають зловмисне програмне забезпечення Dridex за допомогою фішингових кампаній, і воно було пов'язано з різноманітними тактиками, прийомами та процедурами або TTP, включаючи встановлення програмного забезпечення для клавіатури та запуск зловмисних атак із криптоблокуванням, повідомляє CISA.

Як вперше повідомляє Bleeping Computer, один із ідентифікаторів загроз Dridex, які використовують уразливість Log4Shell, включає імена файлів та URL-адреси, позначені принизливими термінами, включаючи релігійні та расові образи.

Якщо експлойт не може запустити команди Windows, зловмисне програмне забезпечення припускає, що це пристрій Linux, і виконує сценарій Python. Повідомляється, що зловмисники також встановлюють інструмент для тестування пера Meterpreter для підключення до зламаного сервера та віддаленого виконання команд, повідомляє Bleeping Computer». ***(Dan Gunderman. Log4j: Belgian Defense Ministry Reports It Was 'Paralyzed' // Information Security Media Group, Corp. (https://www.govinfosecurity.com/log4j-belgian-defense-ministry-reports-was-paralyzed-a-18163). 21.12.2021).***

***

«Відповідно до заяви Роба Лукаса (скарбник Південної Австралії) 16 листопада через напад вимагачів на Frontier Software до на темної мережі просочилася «значна особиста інформація» тисячів державних службовців Південної Австралії.

Лукас посилався на оновлення в четвер від компанії-розробника програмного забезпечення, чию HR і систему нарахування заробітної плати Chris21 атакували. У оновленні йдеться, що дані уряду штату були вкрадені з його мережі під час інциденту та опубліковані в темній мережі.

Frontier Software під час інциденту запевняв клієнтів, що «на сьогоднішній день наше розслідування не показало жодних доказів вилучення або крадіжки даних клієнтів». У ньому сказано, що дані й системи австралійського клієнта з персоналу та нарахування заробітної плати були відокремлені від корпоративних систем і не були скомпрометовані.

Але розслідування, проведене експертами з кібербезпеки з CyberCX, залучене Frontier Software в листопаді, показало, що дані були вилучені з внутрішнього австралійського корпоративного середовища Frontier Software.

Що було просочено?

За словами Лукаса, Frontier Software надає послуги з нарахування заробітної плати від імені уряду Південної Австралії з 2001 року. "Були доступні записи

щонайменше 38 000 співробітників, і до 80 000 співробітників могли отримати доступ" з боку учасників програм-вимагачів, каже він. Уряд, додає він, найближчим часом встановить точнішу цифру.

За словами Лукаса, дані, до яких було отримано незаконний доступ, містять такі деталі, як ім’я та прізвище, дата народження, номер податкової справи, домашня адреса, реквізити банківського рахунку та винагорода, утриманий податок, тип платежу, тип та сума одноразової виплати, пенсійний внесок., а також податок на додаткові пільги державних службовців.

Серед постраждалих може бути прем'єр-міністр Південної Австралії Стівен Маршалл, повідомляє інформаційне агентство ABC News з посиланням на Лукаса.

І Лукас, і уряд Південної Австралії не вказали департаменти, чиї дані були злиті, але підтвердили, що жодного працівника Департаменту освіти не постраждав, оскільки вони не використовують Frontier Software для нарахування заробітної плати.

Надзвичайне оновлення щодо кібербезпеки, опубліковане урядом Південної Австралії в п’ятницю, показує, що працівники державного сектору та особи, які входять до відомства уряду штату, включаючи австралійське податкове управління, Services Australia, Super SA – систему пенсійного забезпечення державних службовців, фінансові установи, Maxxia – Про це порушення було попереджено постачальник заробітної плати уряду Південної Австралії та профспілки працівників.

Атрибуція

Ні CyberCX, ні Frontier Software не відповіли на запит Information Security Media Group щодо інформації про особу зловмисника.

Перевірка ISMG публікації групи програм-вимагачів Conti на її сайті витоку даних - Conti News - показує, що загроза може бути відповідальна за атаку. На сайті витоку даних показано 10 файлів [.]rar, які нібито містять 3,75 ГБ або 10% даних Frontier Software, виставлені на продаж.

Відтоді публікація була видалена, що викликало припущення про те, чи був сплачений викуп – незважаючи на підхід австралійського уряду «без викупу» – чи дані були продані.

План реагування

Frontier Software у своєму листопадовому оновленні заявила, що посилила периметр безпеки, активно відстежуючи всі середовища за допомогою експертів із безпеки CyberCX.

У своїй останній заяві Лукас говорить, що уряд Південної Австралії співпрацює зі службою підтримки кібербезпеки IDCARE, некомерційною організацією, яка спеціалізується на крадіжці особистих даних та кризовому управлінні, щоб розробити конкретний план реагування та запропонувати постраждалим працівникам особисту підтримку протягом усього процесу.

Уряд повинен мати більш надійну програму тестування та аудиту, щоб гарантувати, що все стороннє програмне забезпечення є безпечним, каже ISMG Кіаран Бірн, керівник відділу операцій платформ у фірмі з кібербезпеки Edgescan. Він каже, що там, де це має сенс, бажано зберігати певні елементи всередині будинку.

«Як би легко не було сказати, що кожен повинен розробляти власне програмне забезпечення, щоб піклуватися про власні дані, це непрактично і в довгостроковій перспективі викличе більше проблем із безпекою, ніж покладатися на перевірених і надійних третіх сторін, які повинні мати більше досвіду в створенні програмного забезпечення в їхніх конкретних галузях", - говорить він.

Головне — вибрати правильного постачальника, підтримувати програмне забезпечення в актуальному стані та переконатися, що воно адмініструється правильно, каже Бірн.

Інцидент ще раз продемонстрував важливість пріоритету безпеки ланцюга постачань, сказав ISMG Аарон Бугал, інженер із глобальних рішень для Азіатсько-Тихоокеанського регіону та Японії в фірмі з кібербезпеки Sophos.

«Організаціям недостатньо лише зосередитися на власній інфраструктурі безпеки; вони повинні розуміти та мати впевненість у безпеці всього свого ланцюга поставок. Незалежно від того, чи існують ланцюги поставок у фізичних чи цифрових каналах, вони повинні бути включені в моделювання ризиків і включені до плану реагування на інциденти, оскільки вони є розширенням бізнесу». ***(Mihir Bagwe. Australian Government Staff Data Leaked in 3rd-Party Breach // Information Security Media Group, Corp. (https://www.govinfosecurity.com/australian-government-staff-data-leaked-in-3rd-party-breach-a-18096). 10.12.2021).***

***

«Кібератаки з'являються в новинах щотижня і завдають мільярди доларів збитків світовій економіці. Незважаючи на те, що витрати на безпеку продовжують зростати, звіт показує, що 78% опитаних керівників безпеки все ще не впевнені у своїй позиції кібербезпеки, незважаючи на зроблені інвестиції. Це пояснюється тим, що більшість порушень безпеки не є результатом неадекватної технології безпеки; вони є результатом людської помилки.

Успіх і швидке зростання кіберзлочинності є свідченням того факту, що більшість організацій продовжують залишатися неефективними захисниками. Давайте розглянемо п'ять основних причин, чому підприємства можуть бути неефективними у своєму підході до кібербезпеки:

1. ПЕРЕВАЛЬНА КІЛЬКІСТЬ УЗЛИВОСТІ ТА ПОПЕРЕДЖЕННЯ

Оскільки щороку виявляється близько 10 000 нових вразливостей програмного забезпечення, служби безпеки можуть не розуміти ризику кожної потенційної загрози. Групи безпеки використовують інструменти безпеки (наприклад, сканери вразливостей і SIEM) для виявлення закономірностей і ризиків. У великих компаніях нерідко можна побачити 1000 або більше на день, при цьому від 25% до 75% сповіщень виявляються хибними. Обтяжені попередженнями безпеки, команди часто не можуть правильно ідентифікувати або розставити пріоритети ризиків. Деякі навіть зізнаються, що закривають очі на попередження безпеки, коли їхні тарілки переповнюються.

2. НЕДОСТАТНО ФОКУСУВАТИСЯ НА АНАЛІЗІ ОСНОВНИХ ПРИЧИН

Поширеною помилкою, яку роблять команди з кібербезпеки, є лікування симптомів, а не причини, пояснюючи, чому в опитуванні понад 1200 спеціалістів із

кібербезпеки 80% респондентів повідомляють про повторні атаки. Подібно до головного болю, лихоманки та втоми, проникнення шкідливого програмного забезпечення зазвичай є ознакою чогось набагато більш небезпечного. Важливо не тільки очистити зловмисне програмне забезпечення, але також важливо, щоб служби безпеки розуміли, як зловмисне програмне забезпечення змогло порушити їхній захист. Основні причини включають фішинг, соціальну інженерію, вразливості програмного забезпечення, людські помилки, зловмисних інсайдерів, витік облікових даних, неправильну конфігурацію та скомпрометовані ланцюжки поставок.

3. ЗАБАГАТО ПРОЕКТІВ ТА ПРІОРИТЕТІВ

Коли вдарила пандемія, кібербезпека відійшла на другий план, і безперервність бізнесу стала пріоритетом; майже 50% з більш ніж 200 фахівців в області безпеки, опитаних звіт рухаються уваги на IT обов'язок в той час як 91% IT - працівників обстежитися повсть тиском на компромісну безпеку. У корпоративному середовищі ресурси обмежені, IT-командам та командам із кібербезпеки доводиться робити занадто багато, тоді як команди керівництва інколи мають домашні проекти, які можуть мати пріоритет над такими речами, як кібербезпека.

Дотримання - це ще одна річ, яка створює помилкове відчуття безпеки. Крім того, відповідність зосереджена на вимогах нормативних документів, а не на реальних потребах організації в кібербезпеці. Більшість порушень стосуються людей, а контроль за дотриманням вимог не визначає пріоритетність людського фактора або підкреслює його важливість.

4. ПРОБЛЕМА БЕЗПЕЧНОГО ЗВ'ЯЗКУ

Більше половини опитаних спеціалістів із кібербезпеки називають брак таких навичок, як комунікація та лідерство, одним із найбільших недоліків у навичках у колі професіоналів. Ці навички є вирішальними для ефективної програми управління ризиками. Це означає, що навіть коли групи IT-безпеки можуть ідентифікувати загрози, вони не можуть повідомити про них по всій організації.

Прогалини в комунікації призводять до того, що кінцеві користувачі не можуть виявляти підозрілу поведінку, старше керівництво не знає про основні проблеми безпеки, а бізнес не може надати потрібну кількість ресурсів і впровадити потрібну кількість засобів контролю для пом’якшення кіберзагроз. реальний час. Кібербезпека має бути проактивною, а не реактивною, і саме тут комунікації відіграють головну роль.

5. ЛЮДИ БІДНІ НА ОЦІНКУ РИЗИКУ

Близько 1,25 мільйона людей гинуть від автомобільних катастроф щороку, тоді як середня річна смертність від літака рідко перевищує 1000, проте людей більше бояться авіаперельотів, ніж використання автомобілів. Аналогічно, комарі вбивають більше людей за один день, ніж акули за 100 років; проте наш людський інстинкт робить нас обережнішими з акулами. Те саме правило стосується і кібербезпеки. Більшість команд із кібербезпеки мають упередження, і на їхні рішення щодо безпеки зазвичай впливають декілька факторів, таких як розповіді постачальників та засобів масової інформації, вимоги дотримання та регулювання,

загрози без рейтингу або неправильне оцінювання, а також відсутність точності та впевненості у визначенні прогалин у кібербезпеці.

БІЗНЕС ПОТРІБНО ПРИЙНЯТИ ПІДХІД ЗАХИСТУ, керований даними

Підхід, керований даними, означає, що бізнес дозволяє функції безпеки приймати рішення на основі фактичних даних. Це включає розуміння основних причин загроз безпеці, вивчення того, як в організації ламаються речі, оцінку речей, які найімовірніше спричинять це, ранжування цих ризиків у порядку пріоритетності та розробку стратегії для пом'якшення пріоритетних ризиків. Це не одноразова вправа, а постійний процес, що розвивається, який зосереджується на розвитку можливостей бізнесу відповідно до мінливого ландшафту загроз. Існує три основні елементи підходу до захисту, керованого даними:

Фокус на початкових першопричини: Фішинг на сьогоднішній день є найбільш поширеним вектором атаки, стрибки більш ніж 500% протягом перших двох місяців пандемії. Пам'ятайте, що проблема не в програмі-вимагачі; це те, як воно потрапило. Коли ви скорегуєте своє мислення, ви зрозумієте, що рекламне програмне забезпечення або бекдор так само тривожні, як і програми-вимагачі.

Зосередьтеся на основних методах експлойтів: зосередьтеся на подвигах, які активно використовуються проти вас, подвигах, які, ймовірно, будуть використані проти вас, і подвигах, які були успішно використані проти вас. Навіть якщо ваше антивірусне програмне забезпечення або програмне забезпечення для виявлення кінцевих точок виявляє зловмисне програмне забезпечення та видаляє його, якщо воно було живим у вашій системі навіть на секунду, це означає, що ваш захист якимось чином зламано.

Зосередьтеся на розвідці локальних загроз: не забувайте дивитися на власні дані, оцінювати власні ризики та в першу чергу застосовувати свій локальний досвід, замість того, щоб приймати рішення щодо безпеки на основі галузевих і колег. Це правда, що ландшафт загроз розвивається; однак не всі середовища, загрози та ризики створені однаковими.

Знайте, що кібербезпека – це проблема даних і людини. Створення потужного людського брандмауера як останньої лінії захисту є обов'язковим». ***(STU SJOUWERMAN. Why data-driven defense is key in cybersecurity // Mansueto Ventures, LLC (https://www.fastcompany.com/90701936/why-data-driven-defense-is-key-in-cybersecurity). 06.12.2021).***

***

«У першому півріччі 2021 року в порівнянні з 2020 роком глобальні атаки програмного забезпечення зросли на 151% у порівнянні з 2020 роком, оскільки хакери стають все більш нахабними, повідомляє розвідувальне агентство Канади.

Ключова інфраструктура Канади регулярно стає мішенню атак програм-вимагачів, під час яких хакери, по суті, тримають комп'ютерну інформацію в заручниках до тих пір, поки їм не отримають гроші, йдеться у звіті Communications Security Establishment (CSE), опублікованому в понеділок.

Агентство заявило, що йому відомо про 235 інцидентів з використанням програм- вимагачів проти канадських цілей з 1 січня по 16 листопада цього року.

Більше половини були постачальниками критичної інфраструктури, включаючи лікарні.

«Оператори програм-вимагачів, ймовірно, будуть ставати все більш агресивними у своїх цілях, у тому числі проти критичної інфраструктури», – йдеться у звіті, опублікованому Канадським центром кібербезпеки, підрозділом CSE.

Середня загальна вартість відновлення після інциденту з програмним забезпеченням-вимагачем у 2021 році зросла більш ніж вдвічі до 1,8 мільйона доларів, повідомляє агентство Reuters.

CSE повторив, що актори з Росії, Китаю та Ірану становлять серйозну загрозу для кіберінфраструктури таких країн, як Канада.

«Російські спецслужби та правоохоронні органи майже напевно підтримують стосунки з кіберзлочинцями через асоціацію чи вербування, і дозволяють їм діяти майже безкарно, доки вони зосереджують свої атаки на цілях, розташованих за межами Росії», – заявили в CSE.

Ювілей зламу SolarWinds

Звіт канадського уряду з'явився після того, як американська фірма з кібербезпеки попередила, що атаки елітних російських державних хакерів ледь зменшилися після торішньої масової кампанії кібершпигунства SolarWinds, спрямованої на урядові структури США, включаючи Міністерство юстиції та компанії.

У річницю публічного розкриття вторгнень SolarWinds американська фірма з кібербезпеки Mandiant заявила, що хакери, пов'язані з російським агентством зовнішньої розвідки SVR, продовжують красти дані, «відповідні російським інтересам».

Хакерська кампанія отримала назву SolarWinds на честь американської компанії-розробника програмного забезпечення, чий продукт був використаний на першому етапі зараження цих зусиль. Москва неодноразово заперечувала відповідальність за злом.

Хоча кількість урядових установ і компаній США, зламаних SVR, цього року була меншою, ніж минулого, коли було зламано близько 100 організацій, оцінити збиток важко, сказав Чарльз Кармакал, головний технічний директор Mandiant.

Кармакал сказав, що «не всі розкривають інциденти, тому що вони не завжди повинні розкривати це на законних підставах», що ускладнює процес оцінки збитків. Але загальний ефект досить серйозний. «Компанії, які зазнають зламу, вони також втрачають інформацію», – сказав він.

Mandiant не ідентифікував окремих цілей і не описав, яку конкретну інформацію, можливо, було вкрадено, але сказав, що серед цілей були невизначені «дипломатичні особи», які отримували шкідливі фішингові електронні листи…» ***(Hackers increasingly target Canada key infrastructure: Spy agency // Al Jazeera Media Network (https://www.aljazeera.com/news/2021/12/6/hackers-increasingly-target-canada-key-infrastructure-spy-agency). 06.12.2021).***

***

«Морська транспортна система (MTS) продовжує залишатися мішенню все більш складних шкідливих методів спуфінгу електронної пошти. У вересні 2020 року берегова охорона опублікувала Інформаційний бюлетень з безпеки на морі 19-20, у якому висвітлювалися зловмисні події підробки електронної пошти, спрямовані на MTC. Спираючись на ці методи атаки, досвідчені кіберзлочинці реєструють домени з навмисно неправильно написаними назвами веб-сайтів компаній і використовують їх для запуску фішингових атак. Ці події були проаналізовані та досліджені, а також рекомендації для зацікавлених сторін MTC:

Технічний контроль

Звіти про автентифікацію повідомлень на основі домену та відповідність (DMARC) – організаціям настійно рекомендуємо впроваджувати DMARC, щоб забезпечити, щоб усі електронні листи, які надходять з офіційних джерел, проходили перевірку Sender Policy Framework/Domain Keys Identified Mail (SPF/DKIM) для підтвердження. походження. DMARC розроблено, щоб вписатися в існуючий процес аутентифікації вхідної електронної пошти організації та захистити від прямого підроблення домену. Він дозволяє відправнику вказувати, що його повідомлення захищені SPF та/або DKIM, і повідомляє одержувачу, що робити, якщо жоден із цих методів аутентифікації не проходить. Для отримання додаткової інформації про DMARC відвідайте https://DMARC.org.

Сірий список електронної пошти – організації повинні впровадити сірий список електронної пошти як метод зменшення потенційно шкідливого спаму. Сірий список спочатку блокує будь-яку електронну пошту від невідомого відправника і повертає тимчасовий код помилки SMTP, який повідомляє серверу-відправнику, що електронна пошта була тимчасово відхилена. Законний сервер SMTP спробує повторно надіслати електронний лист через певний період часу, тоді як звичайний сервер розсилки спаму не намагатиметься надіслати повторно. Якщо сервер-відправник повторно надішле електронний лист протягом зазначеного терміну, воно буде вважатися законним і прийнятим.

Обізнаність та навчання користувачів. Обізнаність та залучення працівників є ключем до ефективного захисту кібербезпеки. Організаціям настійно рекомендуємо впроваджувати навчальні програми з підвищення обізнаності в галузі інформаційних технологій (IT) відповідно до спеціальної публікації Національного інституту стандартів і технологій 800-50, ISO 27001 або подібних стандартів, а також відповідно до вказівок, викладених у Циркулярі з інспекції навігації та суден (NVIC).) 01-20: Керівництво щодо подолання кіберризиків на об'єктах, що регулюються Законом про безпеку морського транспорту (MTSA), для досягнення цієї мети.

Як завжди, слід серйозно ставитися до будь-якої потенційної загрози кібербезпеці вашого підрозділу, судна чи об’єкта». ***(USCG Maritime Cyber Readiness Branch Recommendations for Fending Off Malicious Email Attacks // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/uscg-maritime-cyber-readiness-branch-recommendations-for-fending-off-malicious-email-attacks/). 02.12.2021).***

***

«Масова експлуатація веб-сайтів WordPress триває, і протягом 36 годин 1,6 мільйона доменів зазнали близько 13,7 мільйонів кібератак. У масштабній атаці взяли участь щонайменше 16 000 IP-адрес, згідно з повідомленням, опублікованим 9 грудня, у звіті компанії WordFence з безпеки WordPress.

WordFence каже, що хакери націлені на кілька вразливих плагінів і тем WordPress, при цьому один шаблон не має виправок безпеки.

Мотив зловмисників – отримати адміністративні привілеї та повністю заволодіти вразливими веб-сайтами.

Зловмисники активують реєстрацію та ролі адміністратора за замовчуванням на веб-сайтах WordPress

Дослідники помітили, що зловмисники змінили параметр «users_can_register» на «увімкнений», перш ніж встановити параметр «default_role» на «administrator».

Щоб пом'якшити вплив потенційного компромісу, власники сайтів повинні відвідати http://examplesite[.]com/wp-admin/options-general.php і переконатися, що для «членства» не встановлено значення «будь-який може зареєструватися» та «Новий користувач». Роль за замовчуванням» не була встановлена на роль «адміністратора».

Крім того, власники веб-сайтів повинні перевірити, чи немає незаконних доповнень до плагінів, облікових записів користувачів і ролей користувачів. Вони повинні негайно оновити свої сайти, теми та плагіни та видалити тему NatureMag Lite. На даний момент тема WordPress не має виправленої версії. WordFence також надає повний посібник із очищення для захисту зламаних веб-сайтів WordPress.

Однак серверна частина WordPress дозволяє адміністраторам редагувати файли вихідного коду. Таким чином, зловмисники можуть запровадити інші лазівки на зламаних веб-сайтах.

Кібератака спрямована на чотири вразливі плагіни WordPress і 15 тем Epsilon

WordFence каже, що хвиля атак почалася 8 грудня після того, як 6 грудня розробники виправили вразливості PublishPress Capabilities.

У компанії зазначили, що масштабні кібератаки WordPress були спрямовані на «неавтентифіковані вразливості довільного оновлення параметрів» у плагінах Kiwi Social Share (2018), WordPress Automatic, Pinterest Automatic і PublishPress Capabilities.

Дослідники також виявили, що версії плагіна WordPress Kiwi Social Sharing старші 2.0.11 дозволяють зловмисникам змінювати таблицю wp_options для створення облікових записів адміністратора або перенаправлення блогу на інший сайт.

Зловмисники також націлені на вразливість впровадження функцій у темах Epsilon Framework, що дозволяє віддалено виконувати код (RCE). За оцінками WordFence, щонайменше 150 000 веб-сайтів використовують фреймворк…». ***(Alicia Hope. 13.7 Million Cyber Attacks From 16,000 IP Addresses Target Four Vulnerable WordPress Plugins and 15 Themes Striking 1.6 Million Websites // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/13-7-million-cyber-attacks-from-16000-***

ip-addresses-target-four-vulnerable-wordpress-plugins-and-15-themes-striking-1-6-million-websites/). 20.12.2021).

***

«Электронные угрозы постоянно развиваются. Интернет-преступники настойчивы и постоянно развивают свое мастерство, применяя все более изощренные методы и приемы для обмана пользователей и обхода средств защиты кибербезопасности.

Компании должны знать о тактике, применяемой злонамеренными онлайн-преступниками, а те, кто не может приспособиться к современным цифровым угрозам, могут подвергнуть риску свои активы. Важность безопасности электронной почты нельзя недооценивать в 2021 году, и предприятиям, а также частным лицам необходимо делать все возможное, чтобы быть в курсе последних событий в области кибербезопасности.

Каковы самые большие угрозы безопасности электронной почты для предприятий?

По оценкам, около девяти из каждых десяти кибербезопасностей инициируются электронной почтой, и неудивительно, что работа из домашней культуры, принятая после пандемии Covid-19, создала бесчисленные возможности для киберпреступников. С увеличением числа людей, работающих удаленно и совместно с помощью таких инструментов, как Office 365, предприятия подвергаются большему риску. К наиболее распространенным онлайн-угрозам для бизнеса относятся следующие:

1) Социальная инженерия / спуфинг

Социальная инженерия - это термин, используемый для описания онлайн-преступника, завоевавшего доверие пользователя для кражи денег или данных. Спуфинг включает в себя создание ложных данных (таких как поддельная ссылка или форма входа для того, что кажется законным сервисом) для получения учетных данных, которые могут использоваться для доступа к конфиденциальным данным.

2) Спам

Спам, возможно, является самой старой преступной тактикой в отношении электронной почты. Он включает в себя бомбардировку адреса электронной почты несколькими нежелательными сообщениями, которые вынуждают вас открыть письмо или щелкнуть ссылку с броским заголовком или обязательной к просмотру рекламой.

3) Фишинг

Фишинговые атаки включают использование мошеннических сообщений для кражи денег и / или ценных данных. Как и спуфинг, он может включать в себя запрос информации для входа в систему, которая затем используется для получения доступа к учетным записям пользователя на других сайтах / службах.

К другим популярным атакам относятся программы-вымогатели (блокировка компьютера до тех пор, пока пользователь или компания не заплатит «выкуп»), DDoS (когда несколько запросов на загрузку сайта приводят к сбою сервера, на котором размещен сайт) и троянов (вредоносное программное обеспечение, которое блокирует файлы или операционные системы).

Какую роль играет осведомленность пользователей в адаптации бизнеса к киберугрозам?

В сегодняшнем ландшафте сетевых угроз сотрудники должны нести ответственность за кибербезопасность. Это потому, что многие из сегодняшних атак зависят от человеческого поведения для их успеха. Одним щелчком по электронной почте сотрудники рискуют поставить под угрозу весь бизнес.

Обучение осведомленности пользователей может помочь сотрудникам на всех уровнях организации распознавать, сообщать и избегать угроз безопасности электронной почты. Пользователи могут быть обучены с помощью имитационных фишинговых атак и других имитаций, которые полезны как для тестирования, так и для усиления разумных методов при открытии или принятии соответствующих ответов на подозрительные электронные письма.

Как бизнесу адаптироваться к современным угрозам безопасности?

Лучший способ адаптации бизнеса - это понимать постоянно меняющиеся риски и новые тенденции кибератак. Подготовка к кибератакам начинается с того, что все сотрудники понимают, как уязвимости потенциально могут повлиять на организацию.

В дополнение к этому, лица, ответственные за ИТ-инфраструктуру в рамках бизнеса, должны обеспечить наличие политики безопасности. Это может включать установку брандмауэра, регулярное обновление программного обеспечения для защиты от вредоносных программ, обеспечение установки обновлений и исправлений программного обеспечения Office 365, как только они становятся доступными, а также обеспечение безопасности сетей на рабочих местах.

Также важно убедиться, что все коллеги, работающие за пределами офиса, вошли в систему с помощью безопасного соединения и что системы контролируются для обнаружения любых потенциальных проблем с новейшим антивирусным программным обеспечением.

Как неспособность адаптироваться к киберугрозам может нанести вред бизнесу?

Сложные, постоянно развивающиеся методы кибератак могут нанести ущерб компаниям любого размера. Такие атаки предназначены для обмана сотрудников и предоставления доступа к конфиденциальным данным. Это может подвергнуть предприятия риску финансового мошенничества, потери данных, нарушений защиты данных, потери доверия клиентов и раскрытия информации частной компании, которая может быть полезна конкурентам.

Сбои в работе из-за кибератаки также могут привести к огромным потерям доходов, поскольку во время такой атаки или сразу после нее предприятиям зачастую невозможно вести нормальную работу. Проще говоря, все предприятия во всех отраслях будут подвержены риску угроз кибербезопасности в 2021 году, и важность обеспечения водонепроницаемой политики онлайн-безопасности нельзя недооценивать». ***(Nathan Hill-Haimes. How To Adapt a Business to Modern Email Security Threats // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/how-to-adapt-a-business-to-modern-email-security-threats/). 15.12.2021).***

***

«Кибератаки, которые могут вынудить предприятия прекратить свое существование или защитить себя от дальнейших атак, быстро распространяются. Вот почему эксперты теперь называют эти атаки «цифровой пандемией».

Ведущий европейский поставщик услуг безопасности Orange Cyberdefense недавно опубликовал свой отчет по Security Navigator за 2022 год. В этом отчете представлены результаты исследований, а также некоторые сведения о системе и мнения некоторых ведущих экспертов, основанные на глобальных киберугрозах.

Согласно отчету, в текущем году произошло почти 95 000 кибератак. Количество атак увеличилось на 45 398 по сравнению с предыдущим годом. Точно так же, по сравнению с тридцатью семью атаками в месяц в 2020 году, в текущем году происходит почти сорок две атаки. Такие атаки, о которых чаще всего сообщали жертвы, были основаны на системном вредоносном ПО, сетевых аномалиях (например, туннелирование), сбоях в учетных записях и получении фишинга с помощью атак с социальной инженерией.

Согласно статистическому анализу, у малых предприятий самый низкий уровень атак - всего семнадцать процентов. При дальнейшем анализе типов атак было замечено, что почти тридцать пять процентов были связаны с системным вредоносным ПО, за ними следовали аномалии приложений и сети с двадцатью девятью процентами, а наименьшим типом были нарушения в аккаунте всего с четырнадцатью. процентов. Хотя у малых платформ был самый низкий уровень атак, по сравнению с атаками, совершенными в 2020 году, сейчас их количество выросло почти на десять процентов. Более того, по данным Orange Cyberdefense, скорость атак постепенно увеличивается с ростом уровня бизнеса, но в случае малых платформ они подвергаются кибератакам на тридцать процентов больше, чем компании среднего класса. Одной из причин увеличения частоты атак может быть то, что эти типы предприятий обычно не вкладывают много средств в программное обеспечение для защиты от кибератак по сравнению со средними или крупными предприятиями. Вот почему эти платформы более уязвимы для кибер-хакеров и, как следствие, в этом году подверглись большему количеству атак.

С другой стороны, на предприятия среднего звена приходится почти треть всех зарегистрированных киберпреступлений. Основная часть этих атак происходила из-за сбоев в работе сети и приложений, за которыми следовали системные вредоносные программы и аномалии учетных записей с одинаковой скоростью. По сравнению с атаками, совершенными на малый бизнес, у них было меньше зарегистрированных случаев системного вредоносного ПО, очень мало случаев нарушения политики и меньше кибератак с социальной инженерией.

Несмотря на наличие программного обеспечения для защиты от таких злонамеренных атак, хорошо зарекомендовавшие себя крупные компании стали наиболее целевыми объектами атак, на которые приходится почти половина всех зарегистрированных атак. Однако частота кибератак через разные участки была разной. Системное вредоносное ПО занимало первое место в списке большинства зарегистрированных инцидентов, составляя до 43% случаев. Второй наиболее часто встречающейся категорией были аномалии приложений и сетей (почти 15%), а третьей по популярности категорией были аномалии учетных записей (почти 11%

случаев). Из отчета видно, что сбои в учетных записях и сети были ниже в крупных компаниях по сравнению с малыми предприятиями, но атаки системного вредоносного ПО компенсировали эти цифры удвоенным количеством случаев по сравнению с предыдущим годом. Платформы как для малого, так и для крупного бизнеса находились бок о бок из-за того, что злоумышленники обращались к своим данным с требованием выкупа.

Компании практически на всех уровнях подвергались таким атакам системного вредоносного ПО. В этом году количество кибератак увеличилось почти на 18%. Среди различных типов атак вредоносного ПО бэкдор-версия, обеспечивающая необнаруженную доступность, была на вершине таблицы с 37% случаев. Во-вторых, после Backdoor было загружено вредоносное ПО, в котором уже существующее закодированное вредоносное ПО начинает загрузку других файлов и инициирует свое действие. Третий тип - это вредоносные программы-черви, которые не только прикрепляются к одному устройству или системе, но и могут передаваться в другую систему.

В отчете также были выделены различные секторы бизнеса, пострадавшие от этих атак. Здравоохранение было наиболее частым сектором кибератак, на него приходилось 66% всех случаев сбоев в работе сетей и приложений, за которым следовала транспортная отрасль на втором месте, финансовый сектор на третьем и агентства недвижимости на четвертом.

В других отраслях, таких как производство, пищевая промышленность и трейдеры, атаки системного вредоносного ПО были наиболее распространенной средой для кибератак». ***(Arooj Ahmed. Security Navigator 2022 Report From Orange Cyberdefense Sheds Light On Digital Pandemic // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/security-navigator-2022-report-from.html). 21.12.2021).***

***

«Корпорации часто тратят много денег на кибербезопасность из-за того, что это то, что потенциально может защитить их от финансовых последствий, которые могут вызвать взломы и тому подобное. Однако, несмотря на все усилия и деньги, вложенные в это начинание, многие корпорации по-прежнему имеют относительно слабую безопасность, при этом все обстоятельства учтены и приняты во внимание.

Учитывая все вышесказанное, важно отметить, что недавний отчет, выпущенный Positive Technology, показал, что хакерам потребуется всего около двух дней работы, чтобы взломать даже самые защищенные корпоративные сети. Это действительно короткий период времени, особенно если учесть, насколько преданными своему делу злоумышленники склонны быть в этом отношении, а также количество попыток, которые они готовы осуществить, прежде чем сдадутся.

Исследование проводилось с середины 2020 до середины 2021 года. По-настоящему беспокоит то, что исследователи смогли получить полный доступ к корпоративным сетям и системам, так что практически ни один из методов, которые в настоящее время внедряются, не работает. все то эффективное, что

совсем не сулит ничего хорошего для будущего корпоративной безопасности. Фактически, это говорит о том, что взломать корпоративную сеть, возможно, проще, чем когда-либо прежде.

Эти исследователи также пытались смоделировать события, которые могут привести к значительным финансовым потерям или другим типам неприемлемых сценариев. Эти события происходили примерно в 71% случаев. Это указывает на то, что необходимо проделать еще много работы, прежде чем корпорации смогут с уверенностью сказать, что они защищены от всех форм финансовых атак. Такие атаки могут стоить больших денег и затруднять ведение бизнеса этим компаниям». ***(Zia Muhammad. Research Reveals How Easy It Is to Breach Corporate Networks // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/research-reveals-how-easy-it-is-to.html). 26.12.2021).***

***

«Кіберзлочинці завжди націлені на програмне забезпечення або веб-сайти, якими користується багато людей. Використовуючи виявлені вразливості або не обізнаність людей про належні методи кібербезпеки, суб'єкти загрози запускають різні кібератаки, які вплинуть на велику аудиторію та принесуть найбільшу користь.

Згідно з даними, представленими командою Atlas VPN, 73 відсотки фішингових сайтів видають себе за сторінки, пов'язані з продуктами Microsoft. Крім того, до 50 відсотків зламаних облікових записів хакери отримують доступ за 12 годин, а за тиждень 9 з 10 облікових записів повністю захоплюються зловмисниками.

Дані базуються на звіті Agari Anatomy of a Compromised Account про те, як учасники BEC використовують фішинг облікових даних та експлуатують зламані облікові записи. За шість місяців з жовтня 2020 року по березень 2021 року Agari надав облікові дані понад 8000 унікальних фішингових сайтів.

Кіберзлочинці видавали себе за сторінки входу в обліковий запис Microsoft на 60% фішингових сайтів. Оскільки продукти Microsoft широко використовуються в усьому світі, учасники загроз вважають їх найкращою мішенню для пошуку вразливостей. Хакери можуть використовувати зламаний обліковий запис, щоб запустити більше фішингових або інших кібератак із соціальною інженерією.

Зловмисники імітували сторінки входу в Adobe Document Cloud на 26% фішингових веб-сайтів. Маючи доступ до хмари, кіберзлочинці можуть вставляти шкідливі файли в такі документи, як зловмисне програмне забезпечення або програми-вимагачі. Крім того, якщо зламаний хмарний обліковий запис містить конфіденційну корпоративну чи особисту інформацію, хакери можуть використовувати її для шантажу або продажу даних у темній мережі.

Кіберзлочинці використовували підроблені сторінки входу в Microsoft SharePoint на 8% своїх фішингових сайтів. Отримавши контроль над обліковим записом, зловмисник завантажує шкідливий файл, а потім змінює дозвіл на доступ до файлу на «загальнодоступний», дозволяючи будь-кому поширювати посилання

далі. Зловмисник надсилає посилання на контакти користувача або інші цільові облікові записи через соціальні мережі або електронну пошту.

Сторінки входу в Microsoft Office 365 і OneDrive імітувалися кіберзлочинцями на 3% і 2% фішингових сайтів відповідно.

Пішла за тиждень

Отримавши облікові дані, кіберзлочинці не чекають довго, щоб вжити заходів і отримати те, що хочуть. У той час як деякі використовують автоматизовані інструменти для перевірки облікових даних, інші зловмисники вручну перевіряють дійсність вашої інформації для входу.

Зловмисники отримали доступ до 23 відсотків усіх облікових записів одразу після компромісу. Зловмисники, ймовірно, захопили облікові записи за допомогою автоматичного сценарію для перевірки легітимності облікових даних. Через годину злодія сталася, кіберзлочинці вручну захопили 18 відсотків облікових записів.

Після 6 годин пройшли, 2 з 5 (40 відсотків) рахунків були вручну доступні хакерами. За 12 годин половину акаунтів (50%) захопили кіберзлочинці. Значна кількість акаунтів, зламаних за 12 годин, означає, що більшість компаній навіть не помітять компромісу до того, як суб'єкти загроз вже отримають інформацію.

Після того, як в день, 64 відсотків рахунків були прийняті вручну зловмисниками. Нарешті, майже всі облікові записи, 91 відсоток, отримали доступ протягом тижня після компромісу. Зловмисникам знадобився лише тиждень, щоб отримати доступ до більшості акаунтів, що насправді може призвести до величезних грошових втрат для компанії чи особи.

Однією з найпоширеніших проблем безпеки електронної пошти є компроміс ділової електронної пошти (BEC). Маючи доступ до облікових записів Microsoft, кіберзлочинці можуть доставляти електронні листи, розміщувати шкідливі сторінки або створювати шкідливі документи, що дозволяє їм ефективніше поширювати атаку. Багатофакторна аутентифікація в облікових записах, пов'язаних із роботою, має бути обов'язковою для зменшення ризику». ***(Study: 73 Percent Of Phishing Sites Impersonate Microsoft Product-Related Login Pages // MITechNews.com (https://mitechnews.com/featured/study-73-percent-of-phishing-sites-impersonate-microsoft-product-related-login-pages/). 13.12.2021).***

***

«Европейский центр киберпреступности снова выступил против мошенничества с кредитными картами и готов продемонстрировать успех в том же масштабе, что и его кампания 2020 года, которая предотвратила убытки в размере 40 миллионов евро.

Хорхе Розал Косано, руководитель группы Европейского центра киберпреступности (EC3), сегодня сообщил CyberCrimeCon 21 - мероприятию, организованному компанией Group-IB, занимающейся поиском угроз и программным обеспечением безопасности, - что в 2021 году увеличится количество атак типа «отказ в обслуживании». по требованию выкупа. Еще одна атака 2021 года - это фишинг, который подделывает сообщения от компаний по доставке посылок.

Мошенничество с кредитными картами также сохраняется, преступники проводят постоянные кампании по получению номеров карт и использованию их для совершения несанкционированных покупок. Косано рассказал, как EC3 решила уменьшить влияние кардинга, пытаясь найти номера карт до их использования, чтобы Центр мог как можно скорее проинформировать банки и жертв.

Кардеры знают, что им необходимо защищать передачу номеров карт, полученных в интернет-магазинах, с помощью некачественной защиты, поэтому большая часть хранимых ими данных замаскирована, чтобы скрыть тот факт, что они записывают номера кредитных карт. Косано сказал, что Group-IB помогла найти замаскированные данные.

Поиск точки взлома карт - еще одно направление ежегодной «кардочесальной акции» EC3. Косано сказал, что этого можно достичь, позволив анализаторам JavaScript и другим инструментам позволить провайдерам электронной коммерции обнаруживать тех, чьи системы открыты для атак.

Иногда в открывшемся магазине все еще есть немаскированные данные, доступные для просмотра EC3.

Однако данные получены, по словам Косано, кампания этого года снова принесла хорошие результаты. В рамках усилий 2020 года было проанализировано 90 000 единиц карточных данных и предотвращено 40 миллионов евро убытков, и Косано предсказал: «Мы надеемся получить аналогичные результаты в ближайшие дни».

Group IB уже заявила, что помогла трехмесячной кампании, которая позволила европейским банкам избежать убытков в размере 14 миллионов евро». ***(Simon Sharwood. European Cybercrime Centre confident it's kicked credit card crims – again // The Register (https://www.theregister.com/2021/12/02/european_cybercrime_centre_carding_action_2021/). 02.12.2021).***

***

«Никогда ранее не замеченный противник целевого вторжения из Китая, получивший название Aquatic Panda, использовал критические недостатки в библиотеке журналов Apache Log4j в качестве вектора доступа для выполнения различных постэксплуатационных операций, включая разведку и сбор учетных данных в целевых системах.

Фирма по кибербезопасности CrowdStrike заявила, что проникновение, которое в конечном итоге было пресечено, было направлено против неназванного «большого академического учреждения». Предполагается, что спонсируемая государством группа работает с середины 2020 года в целях сбора разведывательной информации и промышленного шпионажа, причем ее атаки в основном направлены против компаний в телекоммуникационном, технологическом и государственном секторах.

Попытка вторжения использовала недавно обнаруженную уязвимость Log4Shell (CVE-2021-44228, оценка CVSS: 10,0) для получения доступа к уязвимому экземпляру продукта виртуализации рабочих столов и приложений VMware Horizon с последующим запуском серии вредоносных команд,

организованных для извлечения угрозы. полезные данные актора, размещенные на удаленном сервере.

«Модифицированная версия эксплойта Log4j, вероятно, использовалась в ходе операций злоумышленника», - отметили исследователи, добавив, что в ней использовался эксплойт, опубликованный на GitHub 13 декабря 2021 года.

Вредоносное поведение Aquatic Panda выходило за рамки разведки скомпрометированного хоста, начиная с попытки остановить стороннюю службу обнаружения и ответа конечных точек (EDR), а затем переходить к извлечению полезных нагрузок следующего этапа, предназначенных для получения обратной оболочки и сбора учетных данных.

Но после того, как организация-жертва была предупреждена об инциденте, организация «смогла быстро реализовать свой протокол реагирования на инциденты, в конечном итоге исправив уязвимое приложение и предотвратив дальнейшую активность злоумышленников на хосте». В свете успешного срыва атаки точное намерение остается неизвестным». ***(Ravie Lakshmanan. Chinese APT Hackers Used Log4Shell Exploit to Target Academic Institution // The Hacker News (https://thehackernews.com/2021/12/chinese-apt-hackers-used-log4shell.html). 30.12.2021).***

***

«Если и есть что-то, что процветает во время пандемии, так это киберпреступность. Тенденция работы на дому создала привлекательную цель для хакеров, поскольку сотрудники часто получают доступ к защищенным корпоративным сетям с устройств, которые могут не иметь такой же защиты, как в офисе.

В первой половине 2021 года в общей сложности 1097 организаций по всему миру подверглись атакам программ-вымогателей, при этом киберпреступники захватили сети и важные данные с целью получения платежей от своих жертв. Для сравнения, за весь 2020 год от этих атак пострадали 1112 организаций.

Компании, занимающиеся кибербезопасностью, извлекли выгоду из этого всплеска преступности, а инвесторы нашли убежище для своих портфелей, в частности, в некоторых акциях кибербезопасности. Два из них, в частности, все же стоит покупать в новом году.

1. Tenable

По мере развития киберпреступников, безопасность, которую мы используем, должна развиваться впереди них. Крупные организации обнаруживают, что одной только жесткой защиты недостаточно - им также необходимо проявлять инициативу в поиске угроз. Это привело к стремительному росту компаний по обнаружению угроз и управлению уязвимостями, таких как Tenable (NASDAQ: TENB), которая в настоящее время является лидером отрасли.

Tenable владеет платформой Nessus, которая является наиболее распространенным инструментом управления уязвимостями в мире, обслуживающим 30 000 организаций с более чем 2 миллионами индивидуальных загрузок. База данных правительства США об общих уязвимостях и уязвимостях (CVE) выросла до более чем 177 000 угроз, и Nessus покрывает 67 000 из них, что

делает его № 1. Поскольку платформа настраивается, компании могут адаптировать ее к своим конкретным потребностям и, следовательно, это очевидный выбор для предприятий любого размера.

Но, судя по разбивке по клиентам, Tenable показывает, что сегмент организаций с самыми высокими расходами растет быстрее всего, что говорит о том, что более крупные компании стали более осознавать угрозы, с которыми они сталкиваются. В 2016 году у Tenable было 124 клиента с шестизначными цифрами - тех, кто тратит 100 000 долларов и более в год, - а сейчас у компании 995 из них. Это представляет собой совокупный годовой рост на 51%, опережая общий рост выручки за тот же период.

Tenable находится на пороге своего второго прибыльного года подряд после того, как в предыдущие годы стабильно приносила убытки. Аналитики ожидают, что после того, как в 2020 году прибыль на акцию составит 0,19 доллара на акцию, к концу 2021 года компания принесет 0,31 доллара. фокус в корпоративном мире.

Если эти тенденции сохранятся, 2022 год может стать просто началом прекрасных долгосрочных возможностей для инвесторов, приобретающих эти акции прямо сейчас.

2. Zscaler

Zscaler (NASDAQ: ZS) использует облачный подход к кибербезопасности, поэтому для использования его продуктов обычно не требуется установка в локальных сетях или на отдельных устройствах. На корпоративном уровне он в первую очередь действует как уровень защиты между компьютером (или устройством) сотрудника и онлайн-активами компании, к которым они получают доступ. Это делает Zscaler идеальным решением для организаций с удаленным персоналом.

По мере того как все больше операций в корпоративном мире переводятся в онлайн, количество приложений, необходимых для выполнения повседневных задач, стремительно растет. Zscaler предлагает услугу частного доступа, которая создает защитный периметр вокруг этих приложений с доступом с нулевым доверием, что означает, что каждый пользователь должен соответствовать строгим требованиям идентификации, независимо от того, является он внутренним сотрудником или нет. Zscaler Private Access (ZPA) может эффективно сделать приложения организации невидимыми для посторонних и, следовательно, защищенными от атак.

Одним из самых популярных программных приложений для совместной работы является Microsoft Office 365, а Zscaler является авторизованным сетевым партнером. Более 4500 компаний развернули Office 365 с помощью Zscaler, защищая критически важную информацию и данные, созданные в процессе работы.

Zscaler набирает обороты с финансовой точки зрения, обеспечивая прибыль не по GAAP, начиная с 2019 финансового года. Аналитики ожидают, что в текущем 2022 финансовом году выручка компании впервые превысит 1 миллиард долларов.

Будущее выглядит еще ярче. В последнем первом квартале 2022 финансового года компания объявила, что она стала первым и единственным решением Zero Trust Network Access, получившим от Министерства обороны разрешение на работу на уровне воздействия 5, втором по величине уровне безопасности.

Несмотря на то, что у Zscaler ожидается лучший год, долгосрочная перспектива выглядит еще лучше, и это привлекательное предложение для инвесторов…» ***(Anthony Di Pizio. 2 Cybersecurity Stocks Worth Buying in 2022 // The Motley Fool (https://www.fool.com/investing/2021/12/30/2-cybersecurity-stocks-worth-buying-in-2022/). 30.12.3021).***

***

«Согласно новому отчету, неназванная компания недавно была взломана после того, как сотрудник сохранил пароль своей корпоративной учетной записи в своем веб-браузере.

Согласно исследованию охранной компании AhnLab, сотрудник работал из дома на устройстве, используемом совместно с другими членами семьи, которое уже было заражено Redline Stealer, вредоносной программой для кражи информации.

Хотя компьютер был оснащен антивирусным программным обеспечением, вредоносная программа смогла избежать обнаружения, прежде чем украсть пароли, хранящиеся в браузере жертвы.

Пароль snafu

Стремясь защитить свою корпоративную сеть от удаленных сотрудников с зараженными устройствами, рассматриваемая компания предоставила сотрудникам VPN, чтобы они могли безопасно получить доступ к своим рабочим файлам.

Однако этот конкретный сотрудник сохранил учетные данные для входа в VPN в своем браузере, который позже был заражен вредоносной программой. Три месяца спустя компания была взломана с использованием этих учетных данных.

Учитывая, что вредоносное ПО Redline Stealer продается в Интернете (примерно по цене от 150 до 200 долларов), очень сложно сказать, кто стоит за этой конкретной атакой.

Эксперты по кибербезопасности из AhnLab предупредили пользователей, чтобы они воздерживались от хранения паролей в браузере, несмотря на удобство. Менеджер паролей является гораздо лучшим вариантом, они говорят, особенно когда в пару с ключом защиты или другой формой многофакторной аутентификации». ***(Sead Fadilpašić. This nightmare incident shows why you really shouldn't store passwords in your browser // Future US, Inc. (https://www.techradar.com/news/this-simple-malware-shows-why-you-really-shouldnt-store-passwords-in-your-browser). 29.12.2021).***

***

«Специалисты по информационной безопасности компании Cisco представили список наиболее значительных, по их мнению, кибератак уходящего года. Никому не дано в точности предсказать каким в этом плане станет 2022 г. Очевидно, что на фоне растущей доступности средств для взлома, цели злоумышленников и киберинциденты будут становятся все масштабнее. Поэтому, чтобы наступающий год не застал врасплох, стоит оглянуться и вспомнить ключевые события года уходящего.

Январь

Хотя первая атака на цепочку поставок SolarWinds произошла в декабре 2020 г., ее последствия ощущались еще долго после этого.

Объектами атак стали специалисты по кибербезопасности. В числе получателей вредоносных ссылок и запросов в соцсетях от фальшивых аккаунтов оказались и аналитики Cisco Talos.

Февраль

Оператор платформы Lockbit, которая предлагает программы-вымогатели в качестве услуги, предоставил ряд ценных сведений о положении дел в этой сфере и о том, как атакующие выбирают свои жертвы.

С появлением трояна Masslogger набирает популярность безфайловое вредоносное ПО. Этот троян ориентирован на кражу учетных данных из веб-браузеров.

В 2021 г. злоумышленники предпочитали работать на тех, кто больше заплатит. Первым признаком этого тренда стала деятельность группы Gamaredon.

Март

Пока подразделение Cisco Talos продолжало разбираться с SolarWinds, на первый план вышла группировка Hafnium, атаковавшая уязвимости нулевого дня сервера Microsoft Exchange. Самой опасной из брешей, выявленных в ходе этой кампании, оказалась ProxyLogon. Через нее атакующие могли пройти по цепочке и взять под свой контроль весь сервер.

Апрель

Несмотря на то, что вакцина от Covid-19 уже была широко доступна, признаков возвращения в офисы не наблюдалось. Общаясь между собой, некоторые сотрудники продолжали пользоваться такими приложениями для совместной работы, как Slack и Discord, но злоумышленники не дремали: доверенные серверы попадали под их контроль и распространяли вредоносное ПО.

Май

Вирус LemonDuck, впервые обнаруженный в 2020 г., получил дальнейшее развитие. Теперь он нацелился на серверы Exchange с упомянутыми выше уязвимостями и взял на вооружение фреймворк Cobalt Strike.

Выяснилось, что Gamaredon – лишь одна из группировок, старающихся оставаться в тени. Они стали именоваться каперами (Privateers).

Атаке вымогателя DarkSide подвергся крупнейший на восточном побережье США трубопровод Colonial Pipeline. В ряде штатов насосные станции на несколько дней остались без газа, остальные подняли цены.

Июнь

Через несколько недель после атаки на трубопровод Colonial Pipeline группировка DarkSide ушла в тень, отключив свой платежный портал и сообщив о прекращении деятельности. Со временем она всплывет под именем BlackMatter.

JBS, крупный мировой производитель мясной продукции, подвергся кибератаке вымогателей и выплатил 11 млн. долл. Хотя деятельность компании не прекращалась, это привело к панике среди американских потребителей и росту закупок мяса впрок.

Июль

Новый месяц вскрыл новые уязвимости Microsoft нулевого дня. В этот раз под прицелом атакующих оказалась брешь в диспетчере печати Windows, получившая название PrintNightmare.

Национальный праздник США 4 июля стал выходным днем для всех, кроме специалистов по кибербезопасности, которым пришлось сразиться с очередной атакой на цепочку поставок. В этот раз целью злоумышленников стал провайдер управляемых услуг Kaseya, который инфицировал жертв вымогателем REvil.

Август

Снова обнаружена уязвимость PrintNightmare. В этот раз ею воспользовалась группировка вымогателей Vice Society. Специалисты Cisco Talos выявили множество организаций, пострадавших от этой атаки.

Выросла популярность приложений для совместного доступа в Интернет, и атакующие не преминули этим воспользоваться. Эти приложения дают возможность заработать небольшие деньги, «сдавая в аренду» часть своего канала, но, как обнаружили специалисты, немалую долю таких арендаторов составили злоумышленники.

Сентябрь

В результате атаки веб-сайт Amnesty International стал распространителем антивирусного ПО, якобы предназначенного для удаления с мобильных устройств шпиона Pegasus. Вместо этого происходила рассылка вредоносного ПО и кража информации.

Утечка данных группировки Conti стала продолжением истории о программах-вымогателях как услуге. Это позволило многое узнать о ее активности в частности и о таких группировках вообще.

Октябрь

Новый крупный игрок на поле спама – вредоносное ПО Squirrelwaffle. Это одно из самых изощренных и опасных изобретений уходящего года.

Ноябрь

Очередной набор необнаруженных уязвимостей: Microsoft предупреждает об атаках на установщик Windows Installer, в результате которых атакующий может получить привилегии администратора. Тем временем, уязвимости сервера Exchange продолжают эксплуатироваться, на этот раз вымогателем Babuk.

Американская полиция арестовала двух человек, предъявив обвинение в участии в атаке на цепочку поставок Kaseya в составе хакерской группировки REvil. За информацию, которая будет способствовать аресту лидера REvil, объявлена награда 10 млн. долл.

На время притихший, после проведенного в начале года международного полицейского рейда на распространителей Emotet, ботнет снова подает признаки жизни.

Декабрь

Специалисты Talos выявили серию кампаний, проводимых группировкой, которую назвали Magnat. В ее арсенал входит фейковое расширение браузера Google Chrome». ***(Евгений Куликов. Ключевые киберинциденты 2021 по версии Cisco // Компьютерное Обозрение***

(https://ko.com.ua/klyuchevye_kiberincidenty_2021_po_versii_cisco_139772). 21.12.2021).

***

«Эксперты по информационной безопасности из компании, недавно образованной путем слияния McAfee Enterprise и FireEye, представили свое видение ландшафта угроз в 2022 г., а также потенциального влияния этих новых или развивающихся угроз на предприятия, государства и простых граждан.

За последний год кибепреступники научились быстрее и эффективнее адаптировать свои тактики для новых схем нападений, в том числе с использованием программ-вымогателей и привлечением хакеров спецслужбами. Ожидается, что в будущем году эти тенденции сохранятся, а методы злоумышленников станут еще более изощренными. В связи с развитием ландшафта угроз и продолжающейся пандемией компаниям крайне важно отслеживать тренды кибербезопасности, чтобы своевременно принимать меры по защите своих данных.

Итак, каких киберугроз следует опасаться в 2022 г.?

1. Атаки с использованием социальных сетей

В ходе атак, санкционированных властями государств (NSN, nation state notification), будут активнее использоваться социальные сети. Для многих людей последние являются важной частью профессиональной деятельности и личной жизни. Со своей стороны киберпреступники активно используют распространенную привычку принимать приглашения в друзья от совершенно незнакомых людей, чтобы увеличить количество подписчиков.

В результате группы хакеров все чаще обращаются к сотрудникам компаний с предложениями трудоустройства, к примеру. Для них это эффективный способ обойти традиционные средства безопасности и напрямую пообщаться с потенциальными сообщниками или жертвами, работающими в компаниях, которые злоумышленники выбрали в качестве мишеней. Кроме того, кибергруппы могут использовать личные сообщения для захвата учетных записей инфлюенсеров и публикации своих постов в аккаунтах жертв.

Хотя данный подход не новый, он применяется почти так же широко, как альтернативные каналы. Конечно, киберпреступнику потребуется найти и изучить дополнительную информацию, чтобы начать беседу с жертвой, да и создание фиктивной учетной записи может отнять немало времени. Тем не менее, целевые атаки на конкретных лиц доказали свою эффективность, поэтому масштабы применения этого вектора будут только увеличиваться – к нему будут обращаться не только группы, занимающиеся шпионажем, но и другие злоумышленники, которые стремятся получить доступ к какой-либо организации с преступной целью.

2. Спецслужбы участят нападения на другие страны за счет привлечения кибепреступников

Одной из обнаруженных специалистами тенденций является увеличение доли совместных операций киберпреступников и спецслужб иностранных государств.

Во многих случаях для этого создается стартап, а затем появляется целая сеть подставных или действующих «технологических» компаний, которые работают

под руководством министерств национальной безопасности и государственных служб разведки.

Так, в мае правительство США предъявило обвинения четырем гражданам КНР, которые работали на подставные государственные компании. Эти компании оказывали поддержку хакерам в разработке вредоносного ПО и атаках с целью получения деловой информации, коммерческих тайн и конфиденциальных технологических сведений.

И если в прошлом у конкретного семейства программ-вымогателей всегда был автор – группа хакеров из определенного государства, то сейчас, когда их нанимают для написания кода и проведения атак, эти четкие границы постепенно стираются.

При первом проникновении в систему могут использоваться тактики и инструменты, характерные для «обычных» киберпреступников. Однако важно наблюдать за развитием событий и своевременно принимать меры. В 2022 г. различие между обычными киберпреступниками и хакерами, работающими на спецслужбы, продолжит стираться, поэтому компаниям необходимо проанализировать свое положение в отрасли и изучить тактики действующих в ней злоумышленников.

3. Материально независимые группы киберпреступников разделят власть в экосистеме RaaS

Уже несколько лет атаки с использованием программ-вымогателей широко освещаются в СМИ как имеющие наиболее серьезные последствия. В свое время модель «программа-вымогатель как услуга» (Ransomware-as-a-Service, RaaS) позволила начать карьеру множеству начинающих киберпреступников, что вызвало рост числа взломов и получения незаконной прибыли.

Администраторы и разработчики RaaS долгое время считались главными виновниками проблемы. Правоохранительные органы практически не обращали внимания на их сообщников, не обладающих значительными навыками. На фоне отсутствия технологических прорывов в экосистеме RaaS эта ситуация позволила тем самым «менее способным сообщникам» успешно развиться и стать очень компетентными киберпреступниками с собственными целями и задачами.

После атаки на трубопроводную систему Colonial Pipeline популярные среди киберпреступников форумы запретили рекламу программ-вымогателей. Теперь у групп RaaS нет независимой платформы для активного набора сотрудников, демонстрации своих возможностей, поиска посредников для хранения средств, тестирования бинарного кода модераторами или разрешения споров. Им труднее доказывать свою состоятельность, а разработчикам RaaS – удерживать лидирующие позиции в сообществе киберпреступников.

За последние годы программы-вымогатели принесли их создателям прибыль, исчисляемую миллиардами долларов. Рано или поздно найдутся люди, которые посчитают, что они непременно должны получить свою долю.

В 2022 г. ожидается появление новых материально независимых групп киберпреступников, после чего ведущее положение в экосистеме RaaS перейдет от тех, кто контролирует ПО, к тем, кто контролирует сети компании-жертвы.

4. После упомянутого передела власти в сфере RaaS менее квалифицированные операторы получат больше свободы

Экосистема Ransomware-as-a-Service развивалась благодаря появлению сообщников и посредников, сотрудничавших с разработчиками за долю прибыли. Эта организационная структура приобрела оптимальный вид в эпоху GandCrab, однако сегодня мы наблюдаем первый раскол в этом союзе.

Первоначально вся власть в этом альянсе принадлежала разработчикам, которые самостоятельно выбирали сообщников и даже проводили собеседования, чтобы определить уровень их технической подготовки. Чем больше игроков появлялось на рынке программ-вымогателей, тем выгоднее сообщники могли продать свои услуги. При этом они договаривались не только о повышенной доли прибыли, но и об учете их мнения при принятии решений. Например, функция составления списков Active Directory в программе-вымогателе DarkSide, возможно, ставила задачу нивелировать необходимость в высоком уровне технической грамотности сообщников. Эти перемены – признак возможного возврата к более ранним этапам становления программ-вымогателей, когда спрос на менее квалифицированных операторов, полностью полагающихся на опыт разработчиков ПО, был особенно высок.

5. Передача 5G- и IoT-трафика между сервисами API и приложениями делает их особенно привлекательными мишенями

Злоумышленники отслеживают корпоративную статистику и тренды, чтобы выявить сервисы и приложения с повышенным риском. Все типы облачных приложений (SaaS, PaaS и IaaS) стали источником качественной трансформации API на уровне планирования, потребления и применения разработчиками ПО в любых сценариях – B2B или B2C. Охват и популярность ряда облачных приложений, бесчисленные «сокровища» в виде критически важных для бизнеса данных, а также возможности указанных API делают их очень привлекательной мишенью для киберпреступников. Наличие API изначально предполагает связь с другими системами, что создает дополнительные риски для бизнеса. Эти интерфейсы часто становятся вектором для более обширных атак на цепочки поставок.

Судя по последним данным, более 80% всего интернет-трафика приходится на сервисы на базе API. Такая вездесущесть привлекает разработчиков вредоносного ПО, которые планируют атаки на API для получения максимальной прибыли.

Многофункциональные API давно эволюционировали из простого связующего ПО в полноценные приложения, на которых основана работа большинства современных потребительских приложений. Приведем несколько примеров:

Мобильные приложения 5G. Связь 5G и развертывание конечных устройств IoT обслуживают растущую потребность в дополнительных возможностях подключения;

Интернет вещей. По прогнозам, к 2025 г. в мире будут работать более 30,9 млрд. устройств IoT. В 2021 г. объем рынка промышленного IoT увеличится до 124 млрд. долл.;

Пакеты динамических офисных программ онлайн-формата. К 2026 г. объем глобального рынка облачного офисного ПО достигнет 50,7 млрд. долл.

В большинстве случаев атаки на API остаются незамеченными, поскольку эти интерфейсы считаются доверенными каналами, к которым не применяются средства управления и обеспечения безопасности достаточного высокого уровня.

По прогнозам экспертов, особую актуальность в будущем приобретут следующие ключевые риски:

нежелательное раскрытие информации из-за неправильной настройки API;

эксплуатация современных механизмов аутентификации, например, Oauth/Golden SAML для доступа к API и устойчивого нахождения в атакуемых средах;

развитие традиционных атак с использованием вредоносного ПО для проникновения в систему и распространение в ней через облачные API, например, Microsoft Graph API. Примеры такого применения – недавние атаки SolarWinds и APT40/Gadolinium;

потенциальное незаконное использование API для захвата корпоративных данных, например, за счет внедрения программы-вымогателя в облачное хранилище типа OneDrive и т.д.;

использование API в программно-определяемой инфраструктуре также создает опасность ее полного захвата или создания теневой инфраструктуры с незаконными целями.

Видимость использования приложений и работы API должна стать приоритетом для организаций. Конечная цель – инвентаризация всех используемых API с учетом рисков и действенная политика контроля доступа к этим сервисам. Не менее важно обеспечить видимость элементов инфраструктуры, не связанных с пользователями, например, учетных записей служб и принципов работы приложений, которые интегрируют API в более широкую корпоративную экосистему.

Разработчикам API необходимо создать эффективную модель предупреждения угроз и внедрить механизм контроля доступа с нулевым доверием. Другие важные моменты – организация безопасного входа в систему и применение телеметрии для более эффективного реагирования на инциденты и обнаружение несанкционированного использования.

6. Дальнейшая эксплуатация контейнеров с приложениями приведет к захвату ресурсов конечных устройств хакерами

Фактически, контейнеры являются платформой для современных облачных приложений. Такие преимущества, как портативность, эффективность и высокая скорость, помогают организациям быстрее внедрять приложения и использовать инновационные способы управления бизнесом. Однако расширение использования контейнеров также увеличивает поверхность атаки. Какие методы могут применять хакеры, и какие группы рисков связаны с контейнерами? Эксплуатация общедоступных приложений (MITRE T1190) – метод, популярный среди киберпреступников, использующих APT и программы-вымогатели.

Организация Cloud Security Alliance (CSA) определила несколько групп рисков, связанных с образами, оркестраторами, реестрами, контейнерами как

таковыми, хостовыми операционными системами и аппаратным обеспечением. Ниже представлены некоторые ключевые риски, которые, по прогнозам специалистов, будут активнее эксплуатироваться в будущем:

Риски оркестратора. Увеличение числа атак на уровне оркестрации – Kubernetes и связанных API, главным образом за счет ошибок в конфигурациях;

Риски образов или реестров. Увеличение случаев использования вредоносных или тайно внедренных образов за счет неэффективных проверок уязвимости;

Риски контейнеров. Увеличение числа атак на уязвимые приложения.

Более частая эксплуатация указанных уязвимостей в 2022 г. может повлечь за собой незаконное использование ресурсов с помощью вредоносного ПО для криптомайнинга, хищение данных, поддержку устойчивых атак и проникновение в хост-систему с помощью контейнеров.

Как можно защититься? В качестве мер по снижению рисков рекомендуется «встроить» безопасность в процесс DevOps за счет непрерывного контроля отсутствия ошибок в конфигурации, целостности образов и привилегий администратора. Используйте матрицу Mitre ATT&CK Matrix для контейнеров, чтобы выявить недостатки в архитектуре облачной безопасности.

7. Разработка эксплойтов для уязвимостей теперь занимает несколько часов, и с этим уже ничего не поделать… Единственное решение – экстренные патчи

Когда в 2020 г. были похищены данные 17 тыс. клиентов SolarWinds, после чего примерно 40 из них подверглись нападению хакеров, многие были шокированы масштабом взлома. К сожалению, в 2021 г. общее число скомпрометированных пользователей заметно увеличилось – на фоне крайне медленной реакции компаний на действия киберпреступников. Наглядный пример – спустя две недели после выпуска патча для ProxyLogon компанией Microsoft на 30 тыс. серверах Exchange уязвимость все еще не была устранена (по другим оценкам число серверов составило 60 тыс.).

В этом же году в Exchange обнаружилась вторая серьезная проблема – ProxyShell. В августе на следующий день после презентации Blackhat об уязвимостях Exchange Server был выпущен проверочный эксплойт (POC-эксплойт) для всех «дыр», закрытых патчами Microsoft в апреле и мае. По данным отчета Shodan, спустя неделю после появления этого эксплойта более 30 тыс. серверов Exchange оставались незащищенными – причем эти данные не давали полной картины происходящего (у специалистов Shodan не было времени, чтобы полностью просканировать Интернет). Говоря кратко, патчи были выпущены весной, но соответствующими уязвимостями еще можно было воспользоваться осенью.

Какой вывод можно сделать из всего вышесказанного? В следующем году и хакеры, и специалисты по безопасности продолжат совершенствовать свои навыки, чтобы создавать вредоносные и проверочные эксплойты в течение нескольких часов после раскрытия уязвимости. Вместе с тем, главным образом в связи с возрастанием серьезности последствий взлома, компании должны усилить бдительность и оптимизировать управление ресурсами и патчами. Им необходимо выявить общедоступные активы и внедрять «заплаты» в кратчайшие сроки,

невзирая на возможные неудобства для работы бизнеса. Оперативное применение патчей должно стать одной из приоритетных задач. Хотя полностью исключить эксплуатацию уязвимостей с серьезными последствиями нельзя. Следует понимать, что чем больше организаций будут неукоснительно выполнять базовые правила, тем меньше будет масштаб кибератак». ***(Евгений Куликов. McAfee: тренды кибербезопасности 2022 // Компьютерное Обозрение (https://ko.com.ua/mcafee_trendy_kiberbezopasnosti_2022_139807). 28.12.2021).***

***

«Эксперты по кибербезопасности, отслеживающие деньги, выплачиваемые американскими компаниями российским бандам кибервымогателей, обнаружили, что они вели по одному из самых престижных адресов Москвы.

Когда организации по кибербезопсаности отследили миллионы долларов, которые американские компании, больницы и городские власти заплатили онлайн-вымогателям в виде выкупа, они сделали убедительное открытие: по крайней мере, часть этих денег прошла через один из самых престижных деловых адресов в Москве.

Администрация Байдена также сосредоточила внимание на здании Башня Федерация Восток, самом высоком небоскребе в российской столице. Соединенные Штаты нацелены на несколько компаний в башне, поскольку они стремятся наказать российские группы кибер-вымогателей, которые шифруют цифровые данные своих жертв, а затем требуют оплаты за их расшифровку.

Эти платежи обычно производятся в криптовалютах, виртуальных валютах, таких как биткойны, которые затем злоумышленники конвертируют в стандартные валюты, такие как доллары, евро или рубли.

То, что это высотное здание в финансовом районе Москвы стало очевидным центром такого отмывания денег, убедило многих экспертов по безопасности в том, что российские власти терпимо относятся к операторам программ-вымогателей. Они отмечают, что цели находятся почти исключительно за пределами России, и по крайней мере в одном случае, задокументированном в объявлении о санкциях США, подозреваемый помогал российскому агентству внешней разведки.

«Это говорит о многом», - сказал Дмитрий Смилянец, эксперт по анализу угроз из компании Recorded Future, занимающейся кибербезопасностью из Массачусетса. «У российских правоохранительных органов обычно есть ответ: «В российской юрисдикции нет открытых дел. Жертв нет. Как вы ожидаете, что мы будем преследовать этих уважаемых людей?»

Recorded Future насчитала около 50 криптовалютных бирж в столичном финансовом районе Москва-Сити, которые, по его оценке, занимаются незаконной деятельностью. Другие биржи в этом районе не подозреваются в приеме криптовалюты, связанной с преступностью.

Киберпреступность - лишь одна из многих проблем, разжигающих напряженность между Россией и США, наряду с наращиванием российской

военной мощи на границах с Украиной и недавним миграционным кризисом на белорусско-польской границе.

По оценкам министерства финансов, с 2011 года американцы заплатили выкуп кибрепреступникам на общую сумму 1,6 миллиарда долларов. Согласно оценкам, один российский штамм-вымогатель, Ryuk, заработал в прошлом году около 162 миллионов долларов, шифруя компьютерные системы американских больниц во время пандемии и требуя плату за разглашение данных, об этом сообщила компания Chainalysis, отслеживающая транзакции с криптовалютой.

Атаки на больницы привлекли внимание к быстрорастущей преступной индустрии программ-вымогателей, базирующейся в основном в России. Преступные синдикаты стали более эффективными и наглыми в том, что превратилось в конвейерный процесс взлома, шифрования, а затем переговоров о выкупе в криптовалютах, которыми можно владеть анонимно.

На июньской встрече на высшем уровне президент США Джозеф Байден призвал путина принять меры по борьбе с программами-вымогателями после того, как российская банда DarkSide атаковала крупный нефтепровод на восточном побережье - Colonial Pipeline, прервав поставки и создав очереди на заправочных станциях.

Американские официальные лица указывают на таких людей, как Максим Якубец, худощавый 34-летний парень со стрижкой в стиле помпадур, которого США определили как одного из организаторов, участвовашего в крупной киберпреступной операции, банды, называющей себя Evil Corp. Аналитики по кибербезопасности связали его группу с серией атак программ-вымогателей, в том числе одно прошлогоднюю атаку на Национальную стрелковую ассоциацию. В объявлении о введении санкций США Якубец обвиняется в том, что он также помогает ФСБ РФ.

Но после того, как Госдепартамент объявил награду в размере 5 миллионов долларов за информацию, ведущую к его аресту, Якубец, казалось, только щеголял своей безнаказанностью в России: его сфотографировали за рулем Lamborghini в Москве, частично окрашенном флуоресцентно-желтым цветом.

Группа подозреваемых в отмывании преступных денег бирж по обмену криптовалютой прячется в Башне Федерации Восток, о которой впервые сообщили в прошлом месяце Bloomberg News, что еще раз демонстрирует, как российская индустрия кибервымогателей находится под протекторатом властей.

97-этажное здание из стекла и стали, стоящее на берегу Москвы-реки, находится в пределах видимости нескольких правительственных министерств финансового района, в том числе Министерства цифрового развития, связи и массовых коммуникаций России.

Два из самых решительных на сегодняшний день действий администрации Байдена по борьбе с программами-вымогателями связаны с башней. В сентябре министерство финансов ввело санкции в отношении криптовалютной биржи Suex, офисы которой расположены на 31 этаже. Компанию обвинили в отмывании незаконных средств на сумму 160 миллионов долларов.

В то же время в интервью основатель Suex Василий Жабыкин отрицал какую-либо незаконную деятельность.

А в прошлом месяце российские СМИ сообщили, что голландская полиция, используя ордер на экстрадицию в США, задержала владельца, Дениса Дубникова, другой фирмы под названием EggChange, офис которой находится на 22-м этаже. В заявлении одной из своих компаний Дубников отрицал какие-либо нарушения с его стороны.

По словам экспертов по кибербезопасности, программы-вымогатели привлекательны для преступников, поскольку атаки происходят в основном анонимно в Интернете, что сводит к минимуму шансы быть пойманным. Он превратился в разросшуюся, сильно разрозненную отрасль в России, известную исследователям кибербезопасности как «программа-вымогатель как услуга».

Организационная структура имитирует франшизы, такие как McDonald's или Hertz, что снижает барьеры для входа, позволяя менее искушенным хакерам использовать устоявшиеся методы ведения бизнеса для входа в бизнес. Несколько высокопоставленных группировок разрабатывают программное обеспечение и продвигают устрашающие бренды, такие как DarkSide или Maze, для запугивания предприятий и других организаций, являющихся жертвами. Другие группы, которые по сути являются исполнителями, взламывают компьютерные системы, используя бренд и франчайзинговое программное обеспечение.

Росту отрасли способствует рост криптовалют. Это сделало олдскульных денежных мулов, которым иногда приходилось переправлять наличные через границу, практически устаревшими.

Отмывание денге через криптовалютные биржи является последним и наиболее уязвимым шагом, поскольку преступники должны покинуть анонимный онлайн-мир, чтобы появиться в физическом месте, где они обменивают биткойны на наличные или кладут их в банк.

Обменные пункты - это «конец радуги биткойнов и программ-вымогателей», - говорит Гурвейс Григг, бывший агент ФБР, который является исследователем в Chainalysis, компании по отслеживанию криптовалют.

Компьютерные коды в виртуальных валютах позволяют отслеживать транзакции от одного пользователя к другому, даже если личности владельцев анонимны, до тех пор, пока криптовалюта не попадет на биржу. Теоретически записи должны связывать криптовалюту с реальным человеком или компанией.

«Они действительно являются одним из ключевых моментов во всем штамме программ-вымогателей», - говорит Григг об обменниках. По его словам, банды вымогателей «хотят зарабатывать деньги. Но пока вы не обналичите их и не получите через обмен в пункте выдачи наличных, то не сможете их потратить».

Именно здесь, по мнению экспертов кибербезопасности, следует выявлять и задерживать преступников. Но российское правительство позволило таким биржам процветать, заявив, что расследует киберпреступления только в случае нарушения российских законов. Регулирование - это серая зона в России, как и везде, в зарождающейся индустрии торговли криптовалютой.

Российские трейдеры криптовалюты заявляют, что Соединенные Штаты возлагают на их компании несправедливое бремя должной осмотрительности, учитывая быстро меняющийся характер правил.

«Люди, которые являются настоящими преступниками, которые создают программы-вымогатели, и люди, работающие в Москва-Сити, - совершенно разные люди», - сказал в интервью Garantex Сергей Менделеев, основатель одного из трейдеров, базирующегося в Federation Tower East, Garantex. По его словам, российские криптобиржи обвиняют в преступлениях, о которых они не подозревают.

Менделеев, который больше не работает в компании, сказал, что американские службы отслеживания криптовалюты предоставляют данные нероссийским биржам, чтобы помочь им избежать незаконных транзакций, но отказались работать с российскими трейдерами - отчасти потому, что они подозревают, что трейдеры могут использовать эту информацию. чтобы предупредить преступников. Это затрудняет попытки российских компаний искоренить незаконную деятельность.

Он признал, что не все российские биржи старались. По его словам, некоторые из них, находящиеся в финансовом районе Москвы, представляли собой не более чем офис, сейф с наличными деньгами и компьютер.

Согласно списку предприятий в здании, составленному российской картографической службой Яндекс, в Башне Федерации Восток базируется не менее 15 криптовалютных бирж.

Помимо Suex и EggChange, компании, на которые нацелена администрация Байдена, кибер-исследователи и международная компания по обмену криптовалют, отметили еще двух арендаторов зданий, которых они подозревают в незаконной деятельности, связанной с биткойнами.

Управляющий зданием, Aeon Corp, не ответила на вопросы о криптовалютных биржах в своих офисах.

«Подобно банкам и страховым компаниям, с которыми они делят помещения, эти фирмы, вероятно, выбрали это место из-за его статуса и строгой безопасности зданий», - сказал Смилянец, исследователь из Recorded Future.

«Небоскребы Москва-Сити очень красивы, - сказал он. «Они могут размещать в Instagram фото красивых видов из окон небоскреба. Это повышает их легитимность». ***(Романов Роман. Компании, причастные к атакам программ-вымогателей, находятся в центре Москвы // Internetua (http://internetua.com/kompanii-prichastnye-k-atakam-program-vymogateley-nahodyatsya-v-tsentre-moskvy). 06.12.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Google заявила у вівторок, що вирішила закрити мережу з близько мільйона викрадених електронних пристроїв, які використовуються в усьому світі для вчинення онлайн-злочинів, а також подала до суду на російських хакерів, відповідальними за яких стверджував технологічний гігант.

Так званий ботнет заражених пристроїв, який також використовувався для таємного майнінгу біткойнів, принаймні наразі був відрізаний від людей, які користуються ним в Інтернеті.

«Оператори Glupteba, імовірно, спробують відновити контроль над ботнетом, використовуючи механізм резервного копіювання, — пишуть Шейн Хантлі та Лука Наді з групи аналізу загроз Google.

Великі технологічні компанії, такі як Google і Microsoft, все більше втягуються в боротьбу з кіберзлочинністю, яка ведеться через їхні продукти, що дає їм унікальне розуміння загроз і доступ до них.

Google заявила, що мережа включає близько мільйона пристроїв, які використовують Windows у всьому світі для злочинів, які включають крадіжку облікових даних користувачів, і націлена на жертв зі Сполучених Штатів, Індії, Бразилії та Південно-Східної Азії.

Компанія також подала позов до федерального суду Нью-Йорка проти Дмитра Старовікова та Олександра Філіппова, вимагаючи заборони на їх порушення на своїх платформах.

Експерти з кібербезпеки вперше помітили Glupteba у 2011 році, яка поширюється, маскуючись під безкоштовне програмне забезпечення, яке можна завантажити, відео чи фільми, які люди мимоволі завантажують на свої пристрої.

Однак, на відміну від звичайних ботнетів, які покладаються на заздалегідь визначені канали, щоб забезпечити своє виживання, Glupteba запрограмовано знайти замінний сервер, щоб продовжувати працювати навіть після атаки, йдеться у позові Google.

Оскільки мережа ботнетів поєднує в собі потужність приблизно одного мільйона пристроїв, вона має незвичайну потужність, яку можна використовувати для великомасштабних програм-вимагачів або інших атак.

Щоб підтримувати цю мережу, організація «використовує рекламу Google для розміщення вакансій для веб-сайтів», які здійснюють незаконну роботу.

Хакери також використовували власні служби Google для розповсюдження шкідливого програмного забезпечення – інтернет-гігант видалив близько 63 мільйонів документів Google і заблокував понад 1100 облікових записів Google, які використовувалися для поширення Glupteba.

Ботнети можуть «швидше відновлюватися після збоїв, що значно ускладнює їх закриття. Ми тісно співпрацюємо з промисловістю та урядом, оскільки боремося з цією поведінкою», - йдеться в повідомленні Google». ***(Google Disrupts Cybercrime Web Infecting 1 Mn Devices // IBTimes LLC. (https://www.ibtimes.com/google-disrupts-cybercrime-web-infecting-1-mn-devices-3353161). 07.12.2021).***

***

«Згубний ботнет, який використовується для криптоджекінгу, зазнав серйозного удару завдяки Google, чиї безкоштовні хмарні послуги він розповсюджував. Компанія виявила та видалила тисячі облікових записів, розміщених файлів і рекламних облікових записів, які використовувалися для поширення шкідливих файлів.

Ботнет Glupteba функціонує вже кілька місяців, і вважалося, що на його піку щодня ставить під загрозу тисячі людей. Ботнет для криптоджекінга безшумно встановлює майнери монет на ПК з Windows і намагається вкрасти облікові дані для входу та файли cookie для аутентифікації. Він поширювався через рекламу Google, яка обіцяла злам програмного забезпечення та фішингові електронні листи з посиланнями на шкідливі файли, розміщені в Google Docs.

Сумнозвісний криптомайн і викрадення облікових даних ботнет пошкодили

Google попереджає, що, хоча робота ботнету Glupteba була порушена, він не вийшов з ладу. Компанія самостійно вжила заходів, щоб видалити елементи, які використовували ресурси Google для атаки нових жертв, але знадобляться зусилля правоохоронних органів, щоб «зламати» та вилучити апаратні ресурси ботнету. Google почала своє оголошення попередженням, що оператори, ймовірно, перегрупуються та розроблять альтернативні механізми розповсюдження.

Але, принаймні на даний момент, ботнет для криптоджекінгу слід принаймні значно уповільнити. Glupteba спостерігається, як компрометує машини в усьому світі, і вважається, що з 2020 року він заразив близько мільйона пристроїв.

Потрапляючи на цільовий пристрій, зловмисне програмне забезпечення Glupteba ховається у фоновому режимі і намагається вкрасти облікові дані, а також використовувати системні ресурси для криптомайнінгу. Ботнет в основному живиться через шкідливі веб-сайти, які обіцяють завантаження зламаного комерційного програмного забезпечення, але замість цього встановлюють Glupteba, коли користувач натискає посилання для завантаження.

Дослідники Google відстежили Glupteba до сховища git, яке вказує, що ним керує досвідчена група кіберзлочинців; Підозрювані також були пов’язані з продажем номерів кредитних карток і вкраденими обліковими даними, включаючи незаконний доступ до проксі-серверів. Як повідомляється, деякі номери кредитних карток використовувалися для покупки шкідливих рекламних кампаній через сотні облікових записів Google Ads.

Команда криптоджекінга також, очевидно, була завзятими користувачами безкоштовних хмарних послуг Google. Компанія заявила, що виявила 1183 облікові записи Google і 908 хмарних проектів, у яких розміщено шкідливі файли, пов’язані з групою, а також вражаюче близько 63 мільйонів документів Google із шкідливими елементами, пов’язаними зі зловмисним програмним забезпеченням Glupteba.

Окрім видалення цих внутрішніх файлів, Google повідомила, що звернулася до веб-хостів (наприклад, Cloudflare) і повідомила їм про шкідливі сайти, що містять шкідливе програмне забезпечення. Повідомляється, що ці постачальники послуг почали видаляти деякі з цих сайтів і серверів і розміщувати міжсторінкові сторінки з попередженнями перед деякими, які вказують на те, що вони можуть бути шкідливими.

Незважаючи на те, що Google не може «зламати» шкідливі сервери і досяг юридичного рівня зв’язку з провайдерами та хостами, він провів деяке дослідження системи командування та контролю Glupteba і виявив, що у неї є резервна система резервного копіювання біткойн-блокчейну, призначена для маршрутизації. трафік на альтернативні сервери, якщо основні з них видалені. З огляду на те, як довго

циркулювало зловмисне програмне забезпечення для криптоджекінгу та рівень успіху зловмисників, цілком розумно очікувати, що вони врешті перегрупуються з новою системою магістральних серверів, які підтримують ботнет.

Видалення назавжди тепер переходить до рук офіційних розслідувань правоохоронних органів, але Google також повідомляє про подання позову проти двох осіб у Росії, які, як вважають, пов'язані з ботнетом. Двоє налаштували електронні адреси Google за допомогою сервера, який також був ідентифікований як частина інфраструктури Glupteba. Google також зв'язала двох чоловіків з діловими адресами в вежі Російської Федерації, яка в минулому була пов'язана з іншими операціями з кіберзлочинності.

Дуже успішне зловмисне програмне забезпечення для криптоджекінгу, ймовірно, залишиться загрозою

Якщо припустити, що зловмисники справді перебувають у Росії та достатньо досконалі, щоб мати надійні системи резервного копіювання, цілком імовірно, що Glupteba врешті-решт повернеться до своєї діяльності з криптоджекінгу. Дії правоохоронних органів проти окремих осіб у Росії завжди складні та мають низьку ймовірність успіху, оскільки уряд Путіна не видаватиме цих злочинців і не виглядає особливо мотивованим переслідувати їх.

Однак цей крок показує, що основні технологічні платформи вживають суттєвих заходів, щоб контролювати власні служби за неправомірне використання їхніх ресурсів, а також обмінюються зібраними розвідувальними даними з іншими організаціями. Нещодавно Microsoft зробила щось подібне, видаливши хакерську групу, яка, як вважають, базується в Китаї, зі своїх служб, передаючи інформацію, яку вона зібрала про зловмисників, провайдерам і державним установам.

У той час як Glupteba досі використовувалася лише для криптоджекінгу та крадіжки облікових даних, деякі аналітики з безпеки стурбовані тим, що, якщо вона виросте достатньо великим, вона може перетворитися на розподілену відмову в обслуговуванні (DDoS) або ботнет-вимагач». ***(Scott Ikeda. Google Disrupts Glupteba Cryptojacking Botnet With Removal of Hosted Ads, Documents and Accounts, & Notifications to Web Hosts // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/google-disrupts-glupteba-cryptojacking-botnet-with-removal-of-hosted-ads-documents-and-accounts-notifications-to-web-hosts/). 15.12.2021).***

***

«Координаційний центр кібербезпеки сектору охорони здоров'я (HC3) опублікував попередження для сектору охорони здоров'я щодо шкідливого програмного забезпечення Tardigrade, складного штаму зловмисного програмного забезпечення, яке використовувалося для атаки на завод із виробництва вакцин.

Нове дослідження некомерційної організації Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) з кібербезпеки показало, що група Advanced Persistent Threat (APT) використовує зловмисне програмне забезпечення через його «безпрецедентну складність і скритність».

За даними BIO-ISAC, навесні 2021 року в кібератаку було залучено велике підприємство з виробництва вакцин.

«У зв’язку з розвиненими характеристиками та постійним поширенням цієї активної загрози, BIO-ISAC прийняла рішення пришвидшити консультацію щодо цієї загрози в інтересах суспільства», – заявила некомерційна організація.

«Наразі сайти біовиробників та їхні партнери заохочуються вважати, що вони є мішенями, і вживати необхідних заходів для перегляду своєї кібербезпеки та позицій реагування».

Tardigrade — це метаморфічна версія сімейства шкідливих програм SmokeLoader, яка в основному здійснює атаки через заражене програмне забезпечення електронної пошти, рекламу, плагіни, USB та заражені мережі.

Основна мета Tardigrade — завантажувати файли та маніпулювати ними, а потім розгортати інші модулі, залишаючись прихованими. Він сумісний з іншими корисними навантаженнями APT, включаючи Conti, Ryuk і Cobalt Strike.

«Хоча багато шкідливих систем є поліморфними, ця система, здається, здатна перекомпілювати завантажувач з пам’яті, не залишаючи узгодженого підпису», – виявив BIO-ISAC. «Повторна компіляція відбувається після мережевого підключення в дикій природі, яке може бути викликом до сервера командування та керування (CnC) для завантаження та виконання компілятора».

Ця стратегія забезпечує несподіваний рівень автономності порівняно з іншими шкідливими програмами.

«HC3 рекомендує біотехнологічним компаніям, а також сектору охорони здоров’я та громадського здоров’я (HPH) загалом переглянути цей звіт і вжити відповідних заходів для захисту своєї інформаційної інфраструктури від поширення Tardigrade», – йдеться у повідомленні HC3.

BIO-ISAC рекомендував підприємствам переглянути сегментацію своєї біовиробничої мережі та провести тести, щоб перевірити правильну сегментацію між корпоративною, гостьовою та операційною мережами. Біовиробники також повинні тестувати та виконувати автономне резервне копіювання ключової біологічної інфраструктури та планувати можливі наслідки непрацездатності певних машин.

BIO-ISAC також запропонував організаціям дізнаватися про терміни виконання ключових компонентів біоінфраструктури, таких як системи хроматографії та системи забруднення ендотоксинами та мікробами.

Належна кібергігієна — найкращий спосіб захистити організації від кібератак. Оскільки фішинг є поширеним вектором атаки для цього конкретного роду шкідливих програм, організаціям слід навчити персонал біовиробничих установ шукати цілеспрямовані атаки та переглядати повідомлення в соціальних мережах, щоб визначити ймовірні цілі.

Дослідники також відзначили, що багато машин у цьому секторі є застарілими або застарілими системами, які неможливо виправити чи оновити. Якщо це так, організації повинні агресивно сегментувати їх і намагатися перейти на інші системи.

«Сектори біоекономіки та біовиробництва зазнають узгодженої, витонченої атаки. Ви – мішень», – підсумував BIO-ISAC. «Це шкідливе програмне забезпечення надзвичайно важко виявити через метаморфічну поведінку. Важлива пильність на корпоративних комп’ютерах ключового персоналу». ***(Jill McKeon.***

Tardigrade Malware Poses Unprecedented Threat to Biomanufacturers // TechTarget, Inc. (https://healthitsecurity.com/news/tardigrade-malware-poses-unprecedented-threat-to-biomanufacturers). 03.12.2021).

***

«Дослідники NetLab виявили штам зловмисного програмного забезпечення, націлений на вразливість на пристроях AT&T, що вражає 5700 VoIP-серверів, які спрямовують трафік від корпоративних клієнтів до постачальників мобільного зв'язку.

Модульне зловмисне програмне забезпечення, назване ботнетом EwDoor, націлено на мережеві пристрої Edgewater, пізніше визначені як прикордонні контролери сеансів EdgeMarc від AT&T.

За словами дослідників, зловмисник скористався невиправленою вразливістю CVE-2017-6079 на серверах EdgeMarc для встановлення зловмисного програмного забезпечення.

Дослідники почали відстежувати ботнет у жовтні 2021 року і стверджують, що він націлений на жертв, «географічно розташованих у США».

Ботнет EwDoor дозволяє виконувати довільні команди на серверах VoIP

Згідно зі звітом, опублікованим NetLab, підрозділом мережевої безпеки китайської фірми Qihoo 360, ботнет використовує недолік на прихованій сторінці EdgeMarc, що дозволяє користувачам встановлювати власні команди.

Зловмисники використовують сторінку як веб-оболонку для виконання довільних команд. Однак повідомляється, що на інтерфейс не вплине недолік.

Крім того, вони виявили, що ботнет використовує стратегію резервування C2, завантажуючи кінцеві точки сервера командно-управління за допомогою трекера BT. Він розшифровує трекер, щоб отримати сервери C2, перш ніж повідомляти інформацію про пристрій і виконувати відповідні команди. Ботнет також використовує шифрування TLS, щоб уникнути перехоплення дослідниками його трафіку та визначення його характеристик.

Дослідники NetLab опублікували список індикаторів компромісу та хешів файлів, щоб допомогти іншим виявити потенційний компроміс.

Ботнет зосереджений на DDoS та вилучення інформації

За словами дослідників, мотивом ботнету є виконання розподілених атак відмови в обслуговуванні (DDoS) і вилучення інформації зі зламаних серверів VoIP.

«Виходячи з того факту, що атакувані пристрої пов'язані з телефонним зв'язком, ми припускаємо, що основною метою [EwDoor] є DDoS-атаки та збір конфіденційної інформації, наприклад журналів викликів», – припустили вони.

Хоча ботнет EwDoor зазнав кількох оновлень, його основними функціями залишаються DDoS-атаки та функція Backdoor. Його остання версія також включала інші функції, такі як механізми самооновлення, сканування портів, керування файлами та зворотну оболонку.

AT&T визнала результати дослідження та заявила, що вживає заходів, щоб пом'якшити ризики, з якими стикаються VoIP-сервери, що піддаються Інтернету.

Телекомунікаційний гігант також заявив, що не було доступу до даних клієнтів, і недолік не був використаний.

Цікаво, що за словами засновника та технічного директора Bugcrowd Кейсі Елліса, використана уразливість – це вразливість чотирирічної давності, виправлення якої було випущено через 18 місяців.

Муралі Паланісамі, директор з рішень AppViewX, скептично поставився до запевнень AT&T.

«Хоча я радий бачити, що AT&T бере на себе цю відповідальність, щоб вивчити ботнет, який інфікував понад 5700 VoIP-серверів, розташованих всередині її мережі, мені неприємно бачити, що сканування в Інтернеті свідчать про те, що більше 100 000 пристроїв використовують те саме Сертифікат SSL, який використовується на VoIP-серверах EdgeMarc», – сказав Паланісамі.

Ботнетом EwDoor може бути заражено до 100 000 VoIP-серверів

Дослідники NetLab спостерігали лише за запитами, зробленими зараженими серверами VoIP, перш ніж зловмисне програмне забезпечення перейшло на інший сервер C2. Вони виявили 5700 скомпрометованих серверів VoIP всього за три години. Проте, розширене сканування Інтернету виявило, що понад 100 000 VoIP-серверів використовують той самий сертифікат SSL, що використовується на подібних VoIP-серверах EdgeMarc.

«Перевіривши сертифікати SSL, які використовуються цими пристроями, ми виявили, що близько 100 тисяч IP-адрес використовували той самий сертифікат SSL», — пишуть дослідники. «Ми не впевнені, скільки пристроїв, що відповідають цим IP-адресам, можуть бути заражені, але ми можемо припустити, що оскільки вони належать до одного класу пристроїв, можливий вплив є реальним».

«Сертифікати SSL – це ідентифікатори пристроїв, які використовуються для перевірки того, хто підключається та чи підключається до правильної системи», – пояснив Паланісамі. «Використання одного сертифіката SSL для кількох пристроїв приблизно схоже на те, що люди роблять копії паспорта, у якому є лише прізвище та вся велика сім’я, використовуючи той самий паспорт».

Він зазначив, що повторне використання SSL передбачає, що сертифікат за замовчуванням копіюється разом із програмою, що вказує, що програма мала облікові дані за замовчуванням і є небезпечною.

«Ці сертифікати, які отримали назву Wildcard Certificates, надають на ці пристрої дії протоколів прикладного рівня, що дозволяють міжпротокольні атаки (ALPACA), як нещодавно повідомило АНБ».

Паланісамі запропонував AT&T захистити тисячі інших пристроїв, які вже могли бути скомпрометовані.

«AT&T має терміново вжити заходів — прикордонні контролери сеансів (SBC) обробляють телефонні дзвінки з сучасних телефонів. Організації також доведеться переоформити і захистити тисячі пристроїв, а також подивитися на доступність, яку вони мають, і задні двері, які вони налаштували або отримали доступ». ***(Alicia Hope. Chinese Researchers Discover EwDoor Botnet Affecting up to 100,000 AT&T VoIP Servers // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/chinese-researchers-discover-ewdoor-botnet-affecting-up-to-100000-att-voip-servers/). 13.12.2021).***

***

«З січня по листопад 2021 року експерти Kaspersky виявили нову шкідливу програму, яка націлена на понад 35 000 комп'ютерів у 195 країнах. Названий «PseudoManuscrypt» через схожість із шкідливим програмним забезпеченням Manuscrypt групи Lazarus, це нове зловмисне програмне забезпечення містить розширені можливості шпигунства і було помічено націленим як на державні організації, так і на системи промислового контролю (ICS) у багатьох галузях.

Промислові організації є одними з найбажаніших цілей для кіберзлочинців як для отримання фінансової вигоди, так і для збору розвідувальних даних. Фактично, у 2021 році спостерігався значний інтерес до промислових організацій з боку відомих груп APT, таких як Lazarus і APT41. Досліджуючи чергову серію атак, експерти Kaspersky виявили нову частину шкідливого програмного забезпечення, яке має певну схожість із «Manuscrypt» від Lazarus, користувацьким шкідливим програмним забезпеченням, яке використовувалося в кампанії ThreatNeedle проти оборонної промисловості, і назвали його PseudoManuscrypt.

З 20 січня по 10 листопада 2021 року продукти Kaspersky заблокували PseudoManuscrypt на понад 35 000 комп'ютерах у 195 країнах. Багато з них були промислові та державні організації, включаючи військово-промислові підприємства та науково-дослідні лабораторії. 7,2% атакованих комп'ютерів були частиною промислових систем управління (ICS), причому інженерна і будівельна автоматизація представляла найбільш постраждалі галузі.

PseudoManuscrypt спочатку завантажується в системи цілей через підроблені архіви піратського програмного забезпечення, деякі з яких призначені для піратського програмного забезпечення, специфічного для ICS. Цілком імовірно, що ці підроблені інсталятори пропонуються через платформу Malware-as-a-Service (MaaS). Цікаво, що в деяких випадках PseudoManuscrypt був встановлений через сумнозвісний ботнет Glupteba. Після початкового зараження запускається складний ланцюжок зараження, який зрештою завантажує основний шкідливий модуль. Експерти Kaspersky виділили два варіанти цього модуля. Обидва мають розширені можливості шпигунського програмного забезпечення, включаючи реєстрацію натискань клавіш, копіювання даних з буфера обміну, крадіжку облікових даних автентифікації VPN (і, можливо, RDP), даних підключення, копіювання знімків екрана тощо.

Атаки не показують переваги певним галузям, однак велика кількість атакованих інженерних комп'ютерів, включаючи системи, що використовуються для 3D і фізичного моделювання та цифрових близнюків, припускають, що промислове шпигунство може бути однією з цілей.

Як не дивно, деякі з жертв поділяють зв'язки з жертвами кампанії Lazarus, про яку раніше повідомляв ICS CERT, і дані надсилаються на сервер зловмисників за рідкісним протоколом за допомогою бібліотеки, яка раніше використовувалася лише зі зловмисним програмним забезпеченням APT41. Тим не менш, враховуючи велику кількість жертв і відсутність чіткого фокусування, Касперський не пов'язує кампанію з Lazarus або будь-яким відомим загрозою APT…» ***(Mike Brennan. Mass***

Spyware Campaign Targets Thousands Of ICS Computers Worldwide // MITechNews.com (https://mitechnews.com/featured/mass-spyware-campaign-targets-thousands-of-ics-computers-worldwide/). 16.12.2021).

***

«Аналіз даних статистики Dr.Web за жовтень показав збільшення загальної кількості виявлених загроз на 34.87% порівняно з вереснем. Кількість унікальних загроз зросла на 39.75%. Більшість детектувань, як і раніше, припадає на частку рекламних і небажаних програм. У поштовому трафіку найчастіше поширювалися PDF-документи, що використовуються у фішингових розсиланнях.

Кількість звернень користувачів за розшифруванням файлів збільшилася на 7.9% порівняно з вереснем. Найпоширенішим шифрувальником місяця став Trojan.Encoder.26996, на частку якого припало 44.02% всіх інцидентів.

Adware.SweetLabs.5 – Альтернативний каталог програм та надбудова до графічного інтерфейсу Windows від авторів Adware.Opencandy.

Adware.Downware.19998 – Рекламне ПЗ, що виступає в ролі проміжного інсталятора піратських програм.

Adware.Elemental.17 – Сімейство рекламних програм, які потрапляють на пристрої шляхом заміни посилань на файлообмінних сервісах. Замість очікуваних файлів жертви отримують програми з рекламою, а також встановлюють непотрібне ПЗ.

Adware.OpenCandy.247, Adware.OpenCandy.248 – Сімейство програм, призначених для встановлення на комп'ютер різного додаткового рекламного ПЗ.

PDF.Phisher.313, PDF.Phisher.311, PDF.Phisher.314, PDF.Phisher.312, PDF.Phisher.321 – PDF-документ, що використовується у фішинговому розсиланні». ***(У жовтні кількість унікальних загроз збільшилась майже на 40% // Компьютерное Обозрение (https://ko.com.ua/u_zhovtni_kilkist_unikalnih_zagroz_zbilshilas_majzhe_na_40_139599). 06.12.2021).***

***

«…Исследование нескольких вредоносных фреймворков для вывода данных из изолированных систем показали, что за последние полтора десятка лет во всех случаях злоумышленникам приходится полагаться на съемные USB-приводы (флешки) в качестве основного инструмента доставки вредоносов.

Изолированные системы, как можно понять из их названия, отсоединены от интернета, чтобы исключить возможность удаленных манипуляций. Тем не менее, их киберзащита также может являться довольно проблемной сферой.

Эксперты компании ESET исследовали 17 вредоносных фреймворков, которые различные хакеры использовали на протяжении последнего десятилетия для атак на изолированные системы.

Единственным способом доставить на них вредоносное ПО и вывести данные во всех случаях оказываются съемные приводы.

Наиболее известным случаем использования flash-приводов для кибератак на изолированные системы остается инцидент со Stuxnet — вредоносной программой, назначением которой было выведение из строя иранского завода по обогащению урана в Натанце. Именно съемный накопитель, подключенный к нужному компьютеру, обеспечил Stuxnet возможность проникнуть в целевые системы и частично вывести из строя центрифуги завода (впрочем, считается, что Stuxnet нанес куда меньший ущерб, чем должен был).

Помимо Stuxnet, однако, существует множество других вредоносных комплексов, нацеленных на изолированные системы. В их числе Ramsay, разработанный южнокорейской APT-группой DarkHotel, PlugX, разработанный китайской APT-группой Goblin Panda, а также Fanny, принадлежащий EquationGroup, вероятному детищу АНБ США. Также были исследованы фреймворки ProjectSauron и agent.btz, происхождение которых остается загадкой, и многие другие.

Исследователи сосредоточились на таких аспектах как механизмы запуска и функциональность вредоносов внутри целевых изолированных систем, обеспечение скрытности и постоянства, а также пути вывода данных.

Слабое место

Во всех случаях использовались USB-накопители. Все вредоносы были разработаны для шпионажа и нацелены на системы Windows. 75% вредоносов использовали файлы LNK или средства автозапуска в USB-приводах для изначальной компрометации изолированных систем, дальнейшего перемещения по их сетям и сбора данных. Вывод собранной информации также осуществляется через инфицированный накопитель — предполагается, что рано или поздно он будет подключен к системе, имеющей выход в интернет.

Как отмечают эксперты ESET, основное внимание необходимо направить именно на те физические накопители, которые используются для доставки и установки ПО на изолированные системы.

«И накопители для переноса данных на изолированные системы, и машины с выходом в интернет, к которым эти накопители подключаются, нуждаются в самой тщательной проверке перед каждой операцией, — говорит Анастасия Мельникова, директор по информационной безопасности компании SEQ. — Злоумышленники могут через Всемирную сеть установить на нужную систему вредонос, который автоматически будет заражать любые внешние накопители в надежде попасть в итоге внутрь изолированного периметра. Соответственно, данные на накопитель должны попадать только с максимально защищенной машины. Не помешает и установка антивирусных средств и внутрь изолированных систем». ***(Найден лучший за последние 15 лет способ взломать защищенную сеть // CNews (https://www.cnews.ru/news/top/2021-12-07_nazvan_luchshij_za_poslednie). 07.12.2021).***

***

«…Аналитики по безопасности Darktrace обнаружили на 30% увеличение среднего числа попыток атак программ-вымогателей во всем мире в период праздников каждый год подряд с 2018 по 2020 год. Также наблюдалось увеличение на 70% для этого типа атак. атаки во время сезона праздничных покупок (ноябрь и декабрь) по сравнению с месяцами сразу после него (январь и февраль).

Согласно недавнему отчету, средняя стоимость выкупа после единственной успешной атаки с помощью программы-вымогателя составляет около 170 000 долларов, а восстановление может стоить пострадавшим компаниям до 1,85 миллиона долларов. Таким образом, независимо от того, решит ли организация заплатить выкуп, атака всегда будет иметь огромные затраты.

Эти высокие затраты показывают, насколько разрушительной может быть одна атака. В этот период для злоумышленников привлекательны как крупные ритейлеры, так и малый бизнес. Небольшие компании, такие как стартапы, часто становятся еще большей целью из-за их ограниченных человеческих ресурсов, посвященных кибербезопасности, и отсутствия средств для инвестирования в надежную киберзащиту и обучение. Злоумышленники хорошо осведомлены об этих ограничениях, и злоумышленники масштабно автоматизируют свои атаки. Сегодня целью являются все организации, независимо от их размера и отрасли.

Организации также особенно уязвимы в этот период, потому что службы безопасности находятся вдали от своих компьютеров, наслаждаясь столь необходимым и заслуженным отдыхом с близкими. По мере того, как приближаются праздники и службы безопасности теряют свое внимание, цифровая инфраструктура организаций становится благоприятной для атак. Таким образом, компании, особенно розничные торговцы, которые хотят получить максимальную отдачу от сезона праздничных покупок, должны вкладывать средства в инструменты, которые могут обнаруживать угрозы и реагировать на них, когда люди не могут.

Компании, которые побеждают в битве с кибератаками, вовсе не пытаются их предотвратить. Скорее, это компании, которые осознают реальность того, что неосторожные, злонамеренные или скомпрометированные инсайдеры или злоумышленники неизбежно атакуют и сосредоточатся на смягчении любого потенциального нанесенного ущерба. Такие технологии, как самообучающийся искусственный интеллект и автономное реагирование, могут отражать попытки атак на цифровую инфраструктуру организации в течение нескольких секунд после обнаружения, даже если поблизости нет людей, действуя как пара глаз 24 часа в сутки. чтобы сотрудники службы безопасности могли сохранять спокойствие и наслаждаться отдыхом». ***(Eloy Бvila. Christmas shopping has arrived, and so are cyber threats: Main trends to understand // Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/402283). 13.12.2021).***

***

«Немногие банды вымогателей существуют дольше 18 месяцев. Это не потому, что преступники распускаются. Вместо этого набирает силу тенденция к ребрендингу картелей-вымогателей.

Быть позорным преступником - это палка о двух концах. Хотя известность свидетельствует об успехе темной стороны, в то же время она вызывает беспокойство.

Элвин Карпис, последний американский общественный враг №1 и мозг, стоящий за грабителями банков, бандой Карписа-Баркера, остро осознавал, что это бремя несет бремя славы.

«Чтобы стать знаменитостью, вы должны быть известны. И вы не можете заниматься таким бизнесом, не попав в тюрьму», - сказал Карпис в интервью, проведя 33 года в тюрьме за похищение бизнесменов и последующее вымогательство денег. аналог версии вымогателя.

Похоже, киберпреступники, похитители данных, усвоили этот урок. Например, исследователи «Лаборатории Касперского» недавно отметили, что продолжительность жизни банды вымогателей сократилась до менее чем 18 месяцев.

Однако большинство киберпреступников просто так не исчезают. Те же люди, которые используют одни и те же инструменты, выполняют одну и ту же работу, хотя и под разными именами. Введите: ребрендинг вымогателей. Проверенная временем практика сокрытия на виду.

Плащ невидимости

Кибератака на объект Colonial Pipeline в Алабаме стала одной из самых громких кибер-историй в этом году. Из-за атаки программы-вымогателя хакеры вынудили перекрыть трубопровод, покрывающий 45 процентов поставок топлива на Восточном побережье, что вызвало нехватку топлива на юго-востоке Америки.

Несколько дней спустя ФБР подтвердило, что за атакой стояла банда вымогателей Darkside. Группа работает с августа 2020 года, но на сегодняшний день это самый большой результат банды. Фактически, такая большая, что группа объявила о закрытии всего через неделю после нападения.

По данным Агентства кибербезопасности и инфраструктуры (CISA), остановка была кратковременной. Два месяца спустя появилась еще одна группа, BlackMatter, которую многие считали переименованной версией Darkside.

Похожая история происходит с другой печально известной группой вымогателей REvil, также известной как Sodinokibi. Несмотря на то, что группа работает с 2019 года, в 2021 году она попала в заголовки новостей благодаря атакам на поставщика мяса JBS и компанию по разработке программного обеспечения Kaseya. Он тоже пытался проглотить больше, чем мог, и отключился после атаки.

Это будет не первый раз для REvil. Широко распространено мнение, что эта группа является ответвлением программы-вымогателя GrandCrab, которая закрылась после выплаты выкупа в размере 2 миллиардов долларов с января 2018 года по май 2019 года.

Эти два случая не единичные, поскольку недавно Avaddon стал Haron, DoppelPaymer теперь Grief, а SynAck изменился на El Cometa.

У воров нет чести

Люди обычно сами используют вредоносное ПО для вымогательства. Это означает, что это не автоматизировано, и всегда есть кто-то на другом конце цифровой записки о выкупе.

Как бы киберпреступники ни хотели, чтобы ребрендинг остался незамеченным, у исследователей безопасности есть инструменты, позволяющие определить связь между старыми и новыми группами.

«У разработчиков, как и у писателей, есть стили, которые сохраняются во всех их продуктах. Не окончательные, но показательные», - сказал CyberNews Брайан Чаппелл, главный стратег по безопасности в странах Европы, Ближнего Востока, Африки и Азиатско-Тихоокеанского региона в BeyondTrust.

В конце концов, по своей сути вредоносное ПО - это просто текст, написанный человеком. И люди оставляют следы. Подробный анализ кода позволяет выявить функциональные сходства и экстраполировать, остается ли ядро группы прежним.

«Вы можете относительно легко изменить свое имя, но успешную стратегию вашего бизнеса изменить гораздо сложнее, - пояснил Чаппелл.

Однако эта стратегия не является надежной. Как заметил Джеймс Мод, ведущий исследователь кибербезопасности в BeyondTrust, это потому, что среди воров нет чести.

«Авторы вредоносных программ воруют код и идеи друг друга, поэтому часто бывает трудно отличить подражателя от ребрендинга. От внутренних разногласий до взлома конкурентов - существует множество способов появления этих ребрендированных версий», - сказала Мод.

Пространство для дыхания

Наиболее очевидная причина ребрендинга - избежать обнаружения. Например, русскоязычные хакеры из Darkside и REvil привлекли столько внимания, что президент США Джо Байден обсудил программы-вымогатели со своим коллегой в Москве Владимиром Путиным.

Ребрендинг, как предполагает опытный эксперт по кибербезопасности Чарльз Денайер, призван снять напряжение с преступников, оказавшихся именно в такой ситуации. Теоретически молчание должно позволить бандам вымогателей скрыть свое цифровое и реальное присутствие.

«Стратегия скрытия темноты довольно эффективна, заставляя власти работать еще усерднее, чтобы соединить точки, узнать, кто они и откуда пришли», - сказал Денайер CyberNews.

Интересно, что одного из участников REvil могло не хватить, так как один из его членов, 22-летний гражданин Украины Ярослав Васинский, был арестован в Польше. Другой хакер, связанный с REvil, Евгений Полянин, оказался в розыске ФБР.

Стремление к известности редко выдерживает испытание вниманием правоохранительных органов и исследователей безопасности. Крейг Глатт, ведущий аналитик по кибербезопасности в AGIO, считает, что смена имени может просто отвлекать от выживания группы.

«Они думают, что, если они смогут заново изобрести свою личность, они смогут сбить аналитиков со следа и снова стать печально известными», - сказал Глатт CyberNews.

Обслуживание клиентов

Связь имени вашей банды с наиболее разыскиваемыми ФБР серьезным препятствием для продолжения работы картелей вымогателей по бизнес-модели.

Люди, стоящие за вредоносными программами-вымогателями, редко являются теми, кто проводит атаки. При использовании модели «программа-вымогатель как услуга» (RaaS) «мозг» операции предоставляет доступ к инструментам для получения части выкупа, обычно около 20–30% от суммы вымогательства, выплачиваемого жертвами вымогательства.

Наличие агентов международных правоохранительных служб, борющихся с определенным видом вредоносного ПО, будет препятствовать аффилированным компаниям прикасаться к «горячим» вредоносным программам, что делает ребрендинг прибыльным способом начать все с нуля.

«Ребрендинг может включать перемещение местоположения, новые каналы связи и новые учетные записи для получения платежей - чистый старт в грязном мире или настолько чистый, насколько это возможно. Я подозреваю, что он также более распространен среди банд, которые имеют финансовую мотивацию, меньше эгоизма, больше зарабатывая, - объяснил Чаппелл.

По словам Матье Горджа, эксперта по ИТ-безопасности, основателя и генерального директора VigiTrust, довольные партнеры, вероятно, являются главной причиной ребрендинга банд программ-вымогателей.

«Власти не дураки; они знают, что хакеры проводят ребрендинг. Они также могут распознавать характерные признаки хакерских групп, даже если они меняют свое название. Таким образом, ребрендинг предназначен для аффилированных лиц и, как ни странно, для их клиентов», - сказал Гордж. CyberNews.

Спасение лица

Эксперты, с которыми мы разговаривали, предложили несколько неожиданную причину, по которой банды вымогателей могут начать искать новое название - этика. Подобно законному бизнесу, желающему дистанцироваться от сомнительной практики прошлого, киберпреступники идут тем же путем.

«Хотя вы можете подумать, что злоумышленникам наплевать, у многих есть кодексы поведения и даже условия, на которые соглашаются партнеры преступников, например отсутствие больниц или школ», - пояснила Мод.

Репутация имеет значение, потому что связь с причинением смерти может иметь множество неприятных последствий. Филиалы могут искать более безопасную ставку, в то время как жертвы могут отказаться платить из принципа, независимо от последствий.

«Группы должны решить, что важнее: деньги или репутация. Деньги, которые они могут получить обратно в другом взломе, но если они будут продолжать возиться с последствиями жизни или смерти, жертвы в конечном итоге разозлятся и откажутся платить», - Гордж сказал.

Переступление «красной черты» может вызвать ярость не только в правоохранительных органах, но и в сообществе хакеров. По словам Горджа,

хорошим примером является кибератака, парализовавшая ирландскую систему здравоохранения.

Банда программ-вымогателей Conti сначала потребовала выкуп в размере 20 миллионов долларов, но решила предложить программное обеспечение для расшифровки данных после последствий атаки на систему здравоохранения во время пандемии.

«Хакеры из больниц решили, что они не могут позволить себе вести гражданскую войну между хакерами, поэтому они предоставили ключи дешифрования до того, как жертвы заплатили, даже когда жертвы были готовы заплатить», - сказал Гордж.

Независимо от причины ребрендинга, Гордж считает, что бандам вымогателей лучше провести ребрендинг, чем расколоться.

«В греческой мифологии, если кто-то отрубит одну из голов Гидры, на ее месте вырастут две. […] Мы предпочитаем ребрендинг группы, а не змею, у которой отрубается больше голов после того, как вы отрезаете одну-единственную голову. легче управлять», - сказал он». ***(Vilius Petkauskas. Why ransomware gangs love rebranding // Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/404356). 16.12.2021).***

***

«В последние годы программы-вымогатели нанесли такой ущерб, что многие упускают из виду другие риски кибербезопасности. Для некоторых отсутствие личной информации делает их невосприимчивыми к хакерам и киберинцидентам. По мнению других, пока их компьютеры работают, вредоносных программ на них нет. К сожалению, в действительности все иначе.

Возникает новая тенденция, когда вредоносное ПО используется для перехвата конфиденциальной информации, включая коммерческие секреты, с последующей ее продажей третьим сторонам или раскрытием ее общественности.

СМИ широко обсуждали программное обеспечение Pegasus, используемое для слежки за журналистами и политическими оппонентами по всему миру, до такой степени, что власти США решили включить его в свой список запретов. Но использование шпионского ПО не ограничивается политической сферой.

Недавно суд Калифорнии обязал американскую компанию 24 [7].ai выплатить 30 миллионов долларов одному из своих конкурентов, Liveperson3. Это связано с тем, что программное обеспечение 24 [7].ai было установлено одновременно с программным обеспечением Liveperson на общих клиентских системах. Liveperson утверждал в своем иске, что 24 [7].ai установили шпионское ПО, которое собирало конфиденциальную информацию из приложения Liveperson. Кроме того, программное обеспечение, которое якобы установил 24 [7].ai, удалило некоторые функции приложения Liveperson, в том числе кнопку для активации функции чата. Поступив таким образом, 24 [7].ai вмешался бы в отношения между Liveperson и его клиентами. Более того, эта юридическая эпопея продолжается еще одним судебным разбирательством, касающимся коммерческой тайны клиента Liveperson.

Этот судебный процесс показывает, что кибербезопасность касается не только личной информации, но и коммерческих секретов и даже правильного функционирования программного обеспечения для бизнеса.

Чтобы снизить риск инцидентов, связанных с кибербезопасностью, можно предпринять несколько мер предосторожности. Надежная внутренняя политика на всех уровнях внутри компании помогает поддерживать безопасную среду для бизнес-операций. В сочетании с осведомленностью сотрудников о юридических и деловых вопросах кибербезопасности эти политики могут стать важным дополнением к передовым методам ИТ. Кроме того, обучение сотрудников способствует внедрению передового опыта, включая систематическое расследование неисправностей и использование методов программирования, защищающих коммерческую тайну компании. Кроме того, может быть целесообразно обеспечить, чтобы контракты с клиентами предоставляли поставщикам ИТ доступ к необходимым последующим действиям для обеспечения безопасности обеих сторон.

Наконец, необходимо помнить, что совет директоров должен проявлять осторожность, усердие и навыки, обеспечивая при этом наилучшие интересы компании. Директора могут нести личную ответственность, если они не выполнят свои обязательства по обеспечению принятия адекватных мер для предотвращения киберинцидентов или если они игнорируют риски и демонстрируют умышленную слепоту. Таким образом, члены совета директоров должны проявлять бдительность и быть обученными и осведомленными о кибербезопасности, чтобы иметь возможность интегрировать ее в свое управление рисками…» ***(Eric Lavallŭe, Selena Lu. Un faux sentiment de cybersŭcuritŭ? // Lavery de Billy, S.E.N.C.R.L. (https://www.lavery.ca/fr/publications/nos-publications/4287-un-faux-sentiment-de-cybersecurite-.html). 08.12.2021).***

***

«Французька компанія, що надає IT-послуги, Inetum Group підтвердила, що минулого тижня вона стала предметом атаки програмного забезпечення-вимагача, яка порушила певні операції.

Inetum Group стверджує, що атака програмного забезпечення-вимагача сталася 19 грудня і вплинула на її діяльність у Франції, але вона виключила будь-які зв’язки з уразливістю Log4j.

У компанії заявили, що жодна з її інфраструктур, комунікацій, інструментів співпраці чи операцій доставки для своїх клієнтів не постраждала.

«У межах постраждалого периметра всі сервери були ізольовані, а клієнтські VPN були вимкнені. Після цих початкових заходів і в якості запобіжного заходу спеціальний кризовий підрозділ у Групі негайно звернувся до оперативних груп Inetum з проханням деактивувати певні клієнтські з'єднання, які на той момент вважалися чутливими», – кажуть у компанії.

Компанія також стверджує, що ідентифікувала підпис неназваної групи програм-вимагачів, яку, за її словами, повідомила владі Національного агентства безпеки інформаційних систем Франції - головного агентства з кібербезпеки країни.

«Inetum вже сповістила органи прокуратури та тісно співпрацює з їхніми спеціалізованими підрозділами з боротьби з кіберзлочинністю. Група Inetum також вирішила залучити службу реагування на інциденти безпеки, щоб скористатися підтримкою третьої сторони, яка довіряє», - повідомляє компанія.

Inetum Group працює в більш ніж 26 країнах, налічує майже 27 000 співробітників і в 2020 році отримала дохід у розмірі 1,966 мільярда євро (2,2 мільярда доларів), згідно з її веб-сайтом.

Компанія надає цифрові послуги клієнтам у різних секторах, включаючи аерокосмічний та оборонний, хімічну та медико-санітарну, банківську, автомобільну, енергетичну та комунальні послуги, охорону здоров'я, страхування, роздрібну торгівлю, державний сектор, логістику, телекомунікації та інші.

Інформаційна безпека Media Group не змогла зв'язатися з представником Inetum Group для коментарів у суботу.

BlackCat Ransomware

Компанія не розкриває назви групи програм-вимагачів, але Валері Pic-Мархів, головний редактор французького видання LeMagIt, каже, що за атакою на адресу стояла нова програма-вимагач BlackCat, також відома як ALPHV і Ransom.Noberus. Група «Інетум».

Symantec, підрозділ Broadcom Software, який 18 листопада виявив програму-вимагач у організації-жертві, побачив три варіанти Noberus, розгорнуті зловмисниками під час цієї атаки.

«Noberus — це цікаве програмне забезпечення-вимагач, оскільки воно закодовано на Rust, і це перший раз, коли ми бачимо професійний штам програм-вимагачів, який використовувався в реальних атаках, закодованих цією мовою програмування», — повідомляє команда Threat Hunter у Symantec.

Оператори, які стоять за програмним забезпеченням-вимагачем, здійснюють типові подвійні атаки з вимаганням, під час яких вони спочатку крадуть інформацію з мереж жертв, а потім шифрують файли. Noberus додає розширення.sykffle до зашифрованих файлів.

Symantec також повідомила, що розробники, що стоять за цим програмним забезпеченням-вимагачем, шукають партнерів на російськомовних хакерських форумах, що, на їхню думку, означає, що кількість зловмисників, які розгортають це програмне забезпечення-вимагач, швидше за все, зростатиме…». ***(Prajeet Nair. French IT Services Firm Hit by Ransomware Attack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/french-services-firm-hit-by-ransomware-attack-a-18202). 25.12.2021).***

***

«Північноамериканський постачальник пропану Superior Plus, який надає продукти та послуги, пов’язані з пропаном і дистилятами, більш ніж 780 000 клієнтів у США та Канаді, каже, що він став жертвою атаки програмного забезпечення-вимагача в неділю.

Компанія тимчасово взяла комп'ютерні системи та додаток відсутній в якості запобіжного заходу, в відповідно до компанією заяву. У заяві йдеться, що компанія

розслідує справу разом із нерозкритими експертами з кібербезпеки, щоб зрозуміти масштаб атаки.

«Дізнавшись про інцидент, Superior вжив заходів, щоб захистити свої системи та пом'якшити вплив на дані та операції Корпорації. Незалежні експерти з кібербезпеки були залучені, щоб допомогти Корпорації у боротьбі з цим питанням відповідно до найкращих практик галузі», – каже Superior.

Згідно з первинним розслідуванням компанії, немає доказів будь-якого компромісу в безпеці або безпеці будь-яких персональних даних своїх клієнтів.

Superior Plus ще не відповів на запит Information Security Media Group щодо інформації про масштаби атаки.

«Масштаб цієї атаки поки невідомий, і лише Superior може надати більше деталей, але той факт, що Superior перевів певні системи в автономний режим, свідчить про те, що зловмисники досягли успіху, і тепер настав час зробити більше, ніж мінімум», — каже Сем Каррі, керівник служби безпеки в компанії з кібербезпеки Cybereason.

Своєчасна атака

Еріх Крон, адвокат з питань безпеки в KnowBe4, називає це своєчасною атакою напередодні святкового сезону. «Ця атака та пов'язані з ними порушення можуть стати важливою проблемою як для споживачів, так і для організацій у ці святкові сезони», – говорить Крон ISMG.

Багато споживачів покладаються на газ пропан для обігріву своїх будинків і приготування святкових страв, каже він. «Комерційні організації часто покладаються на пропан для заправки свого парку обладнання, такого як вилкові навантажувачі, щоб допомогти переміщати продукт на свій склад і з нього, а також завантажувати вантажівки для доставки товарів. Без пропану і без того напружений ланцюг поставок може бути ще більше напруженим, в результаті у повільному переміщенні товарів прямо в час піку покупок у році».

Крон радить організаціям і окремим особам бути особливо пильними протягом наступних тижнів, оскільки підприємства часто стикаються з нестачею персоналу під час свят, що уповільнює виявлення атак і реагування на них.

Відповідь та відновлення

Невідомо, чи Superior вже розгорнув системи резервного копіювання, але протидія такій атаці на критично важливу інфраструктуру вимагає попереднього моделювання та готовності, за словами Тіма Маккі, головного стратега з питань безпеки дослідницького центру кібербезпеки Synopsys.

«Зрештою, якщо ви з'ясовуєте, як реагувати, намагаючись відновити операції, є більша ймовірність того, що щось піде не так або проскочить через тріщини. Під час такого планування важливо, щоб усе програмне забезпечення, системи та процеси були оцінені на потенційний компроміс, а потім за ним активно відслідковуються», – каже Маккі.

«Активна оцінка та моніторинг можуть привести лише до двох сценаріїв: «У гіршому випадку, ви покращуєте свій бізнес. У кращому випадку ви виявите атаку досить рано, щоб обмежити її шкоду».

Критичні закони про інфраструктуру

У травні атака програм-вимагачів на Colonial Pipeline спонукала законодавців у політичному спектрі США внести два законопроекти, призначені для усунення недоліків кібербезпеки в критичній інфраструктурі країни – особливо газопроводах і нафтопроводах.

Перший з двох, двопартійний Закон про безпеку трубопроводів, був введений для закріплення в законі ролей, які відіграють Адміністрація безпеки транспорту та Агентство кібербезпеки та безпеки інфраструктури у забезпеченні безпеки газо- та нафтопроводів. Законопроект також вимагає від TSA оновити інструкції з безпеки трубопроводів протягом року та розширити контроль Конгресу за роллю агентства, особливо коли йдеться про кібербезпеку.

Інша двопартійна пропозиція в Палаті представників, Закон CISA Cyber Exercise Act, була внесена для того, щоб CISA вимагала створити «національну програму кібертренінгів», у якій уряд і компанії перевірятимуть свою IT-інфраструктуру на кіберзагрози, включаючи програмне забезпечення-вимагання.

Обидва законопроекти ще очікують на затвердження через запропоновані поправки». ***(Mihir Bagwe. Superior Plus is Latest Fuel Supplier Hit by Ransomware // Information Security Media Group, Corp. (https://www.govinfosecurity.com/superior-plus-latest-fuel-supplier-hit-by-ransomware-a-18128). 15.12.2021).***

***

«Для тих, хто сподівається відсвяткувати занепад і падіння програм-вимагачів до кінця року, подумайте ще раз. Дослідники з питань безпеки кажуть, що мильна опера з програмами-вымогами продовжує існувати: деякі групи програм-вимагачів вийшли, інші просто пройшли ребрендинг, приплив нових гравців залишається постійним, а висококваліфіковані філії, а також брокери початкового доступу продовжують займатися своєю торгівлею.

Багато груп програм-вимагачів продовжують використовувати модель програм-вимагачів як послуги. У цій моделі розробник або адміністратор RaaS зазвичай підтримує програмне забезпечення-вимагач і платіжний портал для жертв і може самостійно запускати деякі атаки. Але, як правило, вони покладаються на ділових партнерів – також афілійованих осіб – які отримують налаштовану версію програм-вимагачів і використовують її для зараження жертв. За кожну жертву, яка платить, афілійована особа отримує скорочення.

Провайдери послуг RaaS продовжують змінюватися. Тим часом філії також можуть змінювати, з ким вони працюють, а іноді працюють з кількома групами одночасно. Усе це може ускладнити передбачити, які групи можуть бути націлені на які типи жертв, виходячи з їх сектору, географії чи розміру, кажуть деякі експерти.

Домінують 4 групи

Які операції-вимагачі є найактивнішими? З липня по вересень компанія Intel 471 з розвідки загроз повідомляє, що відстежила 612 атак, пов'язаних із 35 різними варіантами програм-вимагачів. Але лише чотири варіанти разом склали більшість відстежених атак:

- LockBit 2.0: 33%
- Conti: 15.2%

- BlackMatter: 6.9%
- Hive: 6%

Примітно, що три з цих чотирьох груп були відносними новачками. Наприклад, Hive був вперше помічений 26 червня. У серпні ФБР опублікувало миттєву тривогу щодо Hive, після того як група вразила Memorial Health System в Огайо, серед інших жертв.

Серед інших свіжих операцій- вимагачів на той час були LockBit 2.0 і DarkSide, а також ALTDOS, AvosLocker, HelloKitty і OnePercent Group.

Тим часом, такі групи, як Sodinokibi - aka REvil - а також Avaddon і DarkSide в останні місяці вийшли, що підкреслює, що групи приходять і зникають, принаймні за назвою.

«Через правоохоронні органи, боротьбу між групами або люди, які взагалі відмовляються від варіантів, групи RaaS, які домінують в екосистемі на даний момент часу, зовсім інші, ніж лише кілька місяців тому», — говорить Intel 471. «Втім, навіть зі зміною варіантів кількість випадків використання програм-вимагачів у цілому все ще зростає».

Висновки Intel 471 можуть відрізнятися від результатів інших дослідників. Наприклад, фірма Coveware, що реагує на інциденти з програмами-вимагателями, каже, що на основі фактичних інцидентів із програмним забезпеченням-вимагачем, які вона розслідувала, найбільше в третьому кварталі вона спостерігала типи Conti, Mespinoza, Sodinokibi, LockBit 2.0 і HelloKitty.

Сплески LockBit 2.0

Виходячи з усіх атак, які були відкриті в третьому кварталі, Intel 471 стверджує, що LockBit 2.0 припадає на одну третину з них, і це частково примітно, оскільки операція вперше з'явилася лише в червні. Це вже було пов'язано з деякими помітними хітами, зокрема проти консалтингової компанії Accenture.

У ході подвійного вимагання в хіті Accenture зловмисники вимагали 50 мільйонів доларів, погрожуючи в іншому випадку витоку більше 6 терабайт даних, які вони, як стверджували, вкрали. Intel 471 стверджує, що LockBit 2.0 також націлений на консалтингову компанію за допомогою розподіленої атаки відмови в обслуговуванні - яку іноді називають потрійним вимаганням, коли це частина перевірки програм-вимагачів, - щоб зробити інцидент більш публічним і спробувати збільшити тиск на оплату.

Після того, як Accenture відмовився платити, зловмисники виконали свою загрозу і вилили принаймні деякі вкрадені дані через свій сайт витоку даних.

Conti досліджує Log4j

Серед усіх активних операцій із програмним забезпеченням-вимагачем, зокрема, Conti здобула репутацію безжального, зокрема вразила національну службу охорони здоров'я Ірландії в травні, що призвело до місяців збоїв у секторі охорони здоров'я країни. Експерти кажуть, що Conti також часто не надає дешифратор, якщо жертва платить викуп.

Хоча група продовжує залишатися великим гравцем, кількість атак, пов'язаних з нею, зменшилася на 64% з 2 по 3 квартал цього року, повідомляє Intel 471. «Це може бути частково через те, що оператори не регулярно оновлюють і не

публікують дані жертв у своєму загальнодоступному блозі», - йдеться в повідомленні.

Незвично, що Conti використовує інший підхід до моделі RaaS. «Імовірно, що розробники Conti платять розробникам програм-вимагачів заробітну плату, а не відсоток від надходжень», – повідомило у вересні Агентство з кібербезпеки та безпеки інфраструктури США. Однак такий підхід, схоже, призвів до певної ворожнечі з боку розгортачів, причому один з них оприлюднив підручник атаки групи в помсту за, за його словами, недостатню заробітну плату.

Попереду можуть бути подальші зриви. У листопаді швейцарська фірма Prodaft Threat Intelligence повідомила, що скористалася недоліком в інфраструктурі Conti, дозволивши їй зламати системи групи та отримати уявлення про її діяльність. У звіті Prodaft стверджує, що він ідентифікував фактичні IP-адреси, які використовуються Conti, журнали чату з жертвами та 113 біткойн-адрес для отримання платежів викупу, з яких 100 були пов'язані «з однією атакою програмного забезпечення-вимагача, під час якої жертва просила заплатити Conti у 100». окремі операції з метою приховування платежу від податкових та аудиторських органів».

Prodaft також повідомляє, що Конті, схоже, якимось чином пов'язаний з групою Рюк. Відомі викупи, сплачені Рюку в 2020 році, склали майже 100 мільйонів доларів, повідомила аналітична компанія Chainalysis.

«На основі аналізу зразків програм-вимагачів та порівняння біткойн-гаманців, які використовуються для отримання викупу, існує безсумнівний зв'язок між командами з викупу Conti та Ryuk», – повідомляє Prodaft. «Це може бути та сама команда, або різні команди, які поділяють членів і ресурси один з одним».

Тим часом Conti продовжує розвиватися. Компанія Active Intelligence, що займається розвідкою загроз, каже, що операція, схоже, прагне використати нещодавно виявлений недолік Apache Log4j і активно сканує на наявність уразливості. У середу йдеться, що Conti, схоже, почав використовувати кінцеві точки, які вже заражені Cobalt Strike, для використання програмного забезпечення для керування сервером VMware vCenter, в яке вбудовано Log4j. За даними Advanced Intelligence, експлуатація vCenter може дати зловмисникам можливість переміщатися збоку в мережі жертви.

Сила ребрендингу

У той час як операції з програмним забезпеченням-вимагачем приходять і зникають, іноді це відбувається лише в імені. Наприклад, операція BlackMatter, яка дебютувала минулого літа, була просто ребрендингом DarkSide, після того, як її потрапляння на Colonial Pipeline в США викликало у споживачів паніку, купуючи паливо, що викликало політичну бурю. Справді, ФБР пропонує винагороду в розмірі до 5 мільйонів доларів за інформацію, пов'язану з усіма, хто працює з DarkSide та її додатковим продуктом BlackMatter, включаючи будь-яких філій.

Тому команда DarkSide, схоже, змінила назву та перезавантажилася як BlackMatter. Але будь-яка спроба зробити чистий розрив була недовгою, оскільки експерти з безпеки швидко помітили схожість не лише в коді, але й у гаманцях криптовалюти, які використовуються для отримання викупу.

Однак для злочинних угруповань, які діють з Росії чи інших країн, які не видають своїх громадян, неясно, чи самі подібні розкриття порушить їхню діяльність, хоча західні уряди заявляють, що вони більш активно намагаються зламати та зірвати операції з програмним забезпеченням-вимагачем». інфраструктури.

Незважаючи на це, «розробники все ще легко закривають популярні варіанти, припиняють роботу й повертаються з точно налаштованим шкідливим програмним забезпеченням, яке використовується як ними самими, так і філіями», — говорить Intel 471. «Поки розробники можуть залишатися в країнах, де їм надано безпечну гавань, атаки триватимуть, хоча й з різними варіантами». ***(Mathew J. Schwartz. As Ransomware Variants Shift, Incidents 'Still on the Rise' // Information Security Media Group, Corp. (https://www.govinfosecurity.com/as-ransomware-variants-shift-incidents-still-on-rise-a-18157). 20.12.2021).***

***

«ФБР попереджає, що вимагачі група «Куба» вдалася викачати млн $ 43,9 у виплатах викупу від потерпілих після збитку, по крайней мере 49 об'єктів в п'яти найважливіших секторах інфраструктури.

У п’ятничному сповіщенні бюро повідомляється, що з початку листопада група програм-вимагачів націлена на критично важливі організації національної інфраструктури, включаючи фінансовий, урядовий, медичний, виробничий та IT-сектор.

«Кубинські учасники програм-викупів вимагали щонайменше 74 мільйони доларів і отримали щонайменше 43,9 мільйона доларів у вигляді викупу», - йдеться у повідомленні. Вважається, що операція не має жодних зв’язків з однойменною країною чи її урядом.

Зловмисне програмне забезпечення Hancitor

ФБР стверджує, що Cuba розповсюджується через шкідливе програмне забезпечення Hancitor, завантажувач, відомий тим, що скидає або виконує злодіїв, таких як трояни віддаленого доступу та інші типи програм-вимагачів, у мережі жертв.

У травні охоронна фірма Group-IB виявила випадки, коли зловмисники використовували завантажувач зловмисного програмного забезпечення Hancitor для доставки на Кубу програм-вимагачів у рамках спам-кампанії електронної пошти для вилучення даних і вимагання викупу.

Group-IB каже, що банда програм-вимагачів використовувала Hancitor для отримання доступу до цільових мереж, поширюючи шкідливе програмне забезпечення у шкідливих вкладеннях електронної пошти, замаскованих як сповіщення DocuSign. Після того, як пристрій жертви було скомпрометовано, оператори кампанії використовували спеціальний сайт для витоку даних Cuba ransomware, щоб опублікувати вилучені дані, якщо вимоги щодо викупу не були виконані.

Незрозуміло, коли почалася кампанія і хто є жертвами. Але станом на кінець квітня дослідники Group-IB повідомили, що на сайті були перераховані дані

дев’яти компаній, головним чином з авіації, фінансів, освіти та виробництва в США та Європі.

В останньому сповіщенні ФБР зазначено, що зловмисники Hancitor використовують фішингові електронні листи, уразливості Microsoft Exchange, скомпрометовані облікові дані або законні інструменти протоколу віддаленого робочого столу, щоб отримати початковий доступ до мережі жертви.

«Кубинські учасники програм-вимагачів використовують законні служби Windows, такі як PowerShell, PsExec та інші невизначені служби, а потім використовують права адміністратора Windows для віддаленого виконання своїх програм-вимагачів та інших процесів», – йдеться в повідомленні ФБР.

У попередженні також зазначено, що учасники програм-вимагачів Cuba скомпрометують мережу жертви через шифрування цільових файлів із розширенням «.cuba».

Технічні деталі

У ФБР стверджують, що як тільки система жертви скомпрометована, оператори програм-вимагачів встановлюють і запускають «Маяк CobaltStrike як послугу в мережі жертви через PowerShell».

Після успішної інсталяції програма-вимагач завантажує два виконувані файли, які включають «pones.exe» для отримання пароля та «krots.exe», що дає змогу операторам програм-вимагачів Куби записувати у тимчасовий файл.tmp зламаної системи.

«Після завантаження файлу TMP файл «krots.exe» видаляється, а файл TMP виконується в зламаній мережі. Файл TMP містить виклики програмного інтерфейсу, пов'язані з ін'єкцією пам'яті, яка після виконання видаляється з системи «Після видалення файлу TMP скомпрометована мережа починає зв’язуватися зі сховищем шкідливих програм, розташованим на базі Чорногорії Uniform Resource Locator (URL) teoresp.com», – додає ФБР.

Зловмисники кубинських програм-вимагачів також використовують програмне забезпечення для крадіжки облікових даних Mimikatz разом із RDP для входу на зламані хости мережі, повідомляє ФБР. Після встановлення успішного RDP-з’єднання зловмисники іноді також використовують інструменти тестування на проникнення CobaltStrike, щоб отримати більш глибокий доступ до мережі жертви, що підтримується сценаріями PowerShell для кращої автоматизації атаки.

«Одна з початкових функцій сценарію PowerShell виділяє місце в пам'яті для запуску корисного навантаження, закодованого base64. Після того, як це корисне навантаження буде завантажено в пам'ять, його можна використовувати для доступу до сервера віддаленого командування та керування - C2, а потім розгортання наступного етапу файлів для програм-вимагачів», - зазначає ФБР. "Віддалений сервер C2 розташований за шкідливою URL-адресою kurvalarva.com."

Заходи пом'якшення

У сповіщенні ФБР перераховано кілька рекомендованих кроків для запобігання і відновлення інцидентів із програмним забезпеченням-вимагачем. Серед них — регулярне резервне копіювання даних, впровадження багатофакторної аутентифікації та підтримка автономного резервного копіювання даних.

Крім того, організації повинні переконатися, що всі операційні системи та програмне забезпечення оновлені, і вони повинні видалити непотрібний доступ до адміністративних спільних ресурсів.

Інші важливі засоби захисту включають реалізацію сегментації мережі, наявність плану відновлення для підтримки та збереження кількох копій конфіденційних або приватних даних, а також розміщення серверів у фізично окремому, сегментованому та безпечному місці.

За словами ФБР, організації також повинні встановлювати оновлення та виправляти операційні системи, програмне забезпечення та мікропрограми, щойно вийдуть оновлення.

ФБР заохочує організації ділитися інформаційними журналами кордонів, які показують зв'язок з іноземними IP-адресами та з них, інформацією біткойн-гаманця, файлом дешифратора та будь-якими небезпечними зразками зашифрованих файлів.

ФБР повторило у своєму попередженні, що рекомендує організаціям не платити викуп, оскільки оплата не гарантує відновлення файлів, а також надихає кіберзлочинців здійснювати подальші атаки або заохочувати інших злочинців до участі в незаконній діяльності.

«Однак ФБР розуміє, що коли жертви стикаються з нездатністю функціонувати, всі варіанти оцінюються для захисту акціонерів, співробітників і клієнтів», - стверджують у бюро. «Незалежно від того, чи вирішили ви або ваша організація сплатити викуп, ФБР закликає вас негайно повідомляти про інциденти з використанням програм-викупів у місцевий офіс»…» ***(Prajeet Nair. Alert: 'Cuba' Ransomware Slams Critical Sector Organizations // Information Security Media Group, Corp. (https://www.govinfosecurity.com/alert-cuba-ransomware-slams-critical-sector-organizations-a-18058). 04.12.2021).***

***

«Оскільки організації сектору охорони здоров'я в усьому світі продовжують боротися з інцидентами з програмним забезпеченням-вимагачем, новий звіт з аналізом атаки програм-вимагачів Conti на керівника служб охорони здоров'я Ірландії надає уявлення про фактори, які вплинули на вплив атаки, і пропонує список рекомендацій щодо того, як HSE, а також інші організації, можна краще підготуватися до таких інцидентів.

У 157-сторінковому звіті PricewaterhouseCoopers, створеному на замовлення HSE та оприлюдненому 3 грудня, йдеться про те, що травнева атака використала низку вразливостей, які не є унікальними для національної системи охорони здоров'я Ірландії, включаючи проблеми, з якими стикаються інші організації.

Ці проблеми включали HSE, який має «дуже низький рівень зрілості кібербезпеки», як оцінено у порівнянні з Рамками кібербезпеки Національного інституту стандартів і технологій, йдеться у звіті.

Приклади відсутності засобів контролю кібербезпеки в HSE під час інциденту включають:

IT-середовище не має великої кількості засобів контролю безпеки, які є найбільш ефективними для виявлення та запобігання атак програм-вимагачів, керованих людьми;

Відсутність можливостей моніторингу безпеки, які могли б ефективно виявляти, досліджувати та реагувати на попередження безпеки в IT-середовищі HSE або ширшій Національній мережі охорони здоров'я;

Відсутність ефективного виправлення, включаючи оновлення та виправлення помилок, у IT-середовищі, підключеному до NHN;

Залежність на єдиному продукті захисту від шкідливих програм, який не контролювався чи ефективно не підтримувався за допомогою оновлень у всьому середовищі.

Наприклад, робоча станція, на якій зловмисник спочатку закріпився, не оновлювала антивірусні сигнатури понад рік, йдеться у звіті.

«Низький рівень зрілості кібербезпеки в поєднанні зі слабкістю IT-статей дозволили зловмиснику в цьому інциденті з відносною легкістю досягти своїх цілей», – йдеться у звіті. «Зловмисник зміг використати добре відомі та прості методи атаки, щоб переміщатися по NHN, витягувати дані та розгортати програмне забезпечення-вимагач на великих частинах маєтку без виявлення».

Хронологія атаки

Атака HSE розпочалася 18 березня із зараження шкідливим програмним забезпеченням на робочій станції HSE, яка отримала назву «Patient Zero Workstation» - в результаті клацання користувачем та відкриття шкідливого файлу Microsoft Excel, який був вкладений до фішингового листа, надісланого користувачеві в березні. 16

«Отримавши несанкціонований доступ до IT-середовища HSE 18 березня, зловмисник продовжував діяти в середовищі протягом восьми тижнів до детонації вимагача Conti 14 травня», – йдеться у повідомленні.

«Це включало скомпрометацію та зловживання значною кількістю облікових записів із високими рівнями привілеїв, скомпрометацію значної кількості серверів, вилучення даних та переміщення збоку до державних та добровільних лікарень».

Інцидент не був ідентифікований та локалізований лише після детонації вимагача Conti 14 травня, що спричинило масові збої в IT.

«До 14 травня було кілька випадків виявлення активності зловмисника, але це не призвело до інциденту кібербезпеки та розслідування, ініційованого HSE, і, як наслідок, були упущені можливості запобігти успішній детонації вимагача».

Поширене порушення

Після виявлення детонації програмного забезпечення-вимагача HSE запустив свій процес критичного інциденту, «який розпочав послідовність подій, що призвели до рішення вимкнути всі IT-системи HSE та відключити Національну мережу охорони здоров'я від Інтернету, щоб спробувати стримати та оцінити вплив кібератаки», – йдеться у повідомленні.

Ці дії позбавили зловмисника доступу до середовища HSE. Але вони також негайно призвели до того, що медичні працівники втратили доступ до всіх IT-систем HSE, включаючи інформаційні системи пацієнтів, системи клінічної допомоги та лабораторні системи, йдеться у звіті. Також було втрачено

використання доклінічних систем, таких як фінансові системи, системи оплати праці та закупівлі.

Багатьом клініцистам довелося повернутися до ручки та паперу, щоб продовжити догляд за пацієнтами, йдеться у звіті. «Послуги охорони здоров'я по всій країні були серйозно порушені з реальними і негайними наслідками для тисяч людей, які потребують медичних послуг щодня».

Втрачені лінії зв'язку

Звичайні канали зв'язку, як у національному центрі ВШЕ, так і в його оперативних службах, також були негайно втрачені, включаючи електронну пошту та мережеві телефонні лінії.

«Метою зловмисника було порушити роботу служб охорони здоров'я та IT-систем, викрасти дані та вимагати викуп за неопублікування вкрадених даних та надання інструменту для відновлення доступу до даних, які вони зашифрували», – йдеться у повідомленні.

Спочатку HSE звернувся за допомогою до Національного бюро боротьби з кіберзлочинністю Garda, Інтерполу та Національного центру кібербезпеки для підтримки відповіді.

Програма-вимагач створила нотатки про викуп з інструкціями, як зв'язатися зі зловмисником.

«Зловмисник також опублікував повідомлення в інтернет-чаті в темній мережі з посиланням на кілька зразків даних, які, як повідомляється, викрадено з HSE. HSE та уряд Ірландії підтвердили в день атаки, що вони не будуть платити викуп», – йдеться у повідомленні.

У ньому зазначається, що інцидент мав "набагато більший і триваліший вплив на HSE, ніж очікувалося спочатку", і зусилля з відновлення тривають більше чотирьох місяців.

Інші фактори - у тому числі відсутність CISO

Серед деяких інших факторів, які сприяли ризику атаки HSE, були питання керівництва IT-безпекою та кадрові проблеми. Зокрема, не було CISO, йдеться у звіті.

«HSE не має жодного відповідального власника за кібербезпеку на рівні вищої виконавчої влади чи керівництва, який би забезпечував керівництво та керівництво», – йдеться у звіті та додає, що такий упущення «дуже незвичайний для організації HSE розміром і складністю з покладатися на технології для виконання важливих операцій і обробки великих обсягів конфіденційних даних». У результаті, йдеться у звіті, не було кому забезпечити визнання ризиків, з якими зіткнулася організація через свою позицію кібербезпеки та зростаюче середовище загроз».

У HSE також було лише близько 1519 штатних співробітників на посадах кібербезпеки, і вони не володіли знаннями та досвідом для виконання завдань, які очікуються від них, йдеться у звіті.

Могло бути навіть гірше

Незважаючи на ці недоліки, у звіті йдеться про те, що персонал HSE, включаючи IT та операційний персонал центру HSE та лікарень, а також медичні працівники, доклав значних зусиль, щоб реагувати на інцидент і відновлюватися

після інциденту, продовжуючи надавати догляд пацієнтам протягом усього випробування.

«Якби ці значні зусилля не були зроблені цими людьми, вплив інциденту на ірландську систему охорони здоров'я, безумовно, був би набагато гіршим», – йдеться у звіті.

«HSE працює на слабкому IT-майданчику, якому протягом багатьох років не вистачало інвестицій, необхідних для підтримки безпечної, стійкої, сучасної IT-інфраструктури. Він не володіє необхідними можливостями кібербезпеки для захисту роботи медичних служб та даних, які вони мають. процесу, від кібератак, з якими сьогодні стикаються всі організації».

Планування на випадок надзвичайних ситуацій і криз у HSE раніше зосереджувалося на таких сценаріях, як несприятлива погода, пандемія, серйозні аварії та терористичні атаки, які викликають тимчасовий сплеск попиту на екстрені послуги, йдеться у звіті.

«Як і багато інших організацій, HSE не проводив планування на випадок кібератаки чи будь-якого іншого сценарію, пов'язаного з повною втратою інфраструктури, людей чи об'єктів».

Основні рекомендації

У звіті PwC виклав ряд стратегічних і тактичних рекомендацій для HSE.

Стратегічні рекомендації включають зосередженість та покращення в кількох ключових сферах, зокрема:

Управління IT та кібербезпекою;

Лідерство та трансформація IT-фундаменту, від якого залежить надання медичних послуг;

Лідерство та трансформація можливостей кібербезпеки;

Розвиток безперервності клінічних послуг і послуг, а також можливостей управління кризовими ситуаціями, щоб охопити події в масштабі служби, такі як тривале повне відключення.

Тактичні рекомендації, зокрема деякі, які, як сказано у звіті, вимагають негайної уваги HSE, включають:

Призначити тимчасового CISO, який відповідатиме за покращення кібербезпеки та керує третіми сторонами, які надають послуги кібербезпеки;

Переконайтеся, що керована служба захисту або еквівалент постачальника реагування на інциденти HSE підтримується для виявлення та реагування на інциденти на кінцевих точках;

Розробити, задокументувати та застосувати план управління та координації інциденту кібербезпеки, в якому беруть участь декілька організацій, підключених до NHN;

Встановіть пріоритети відновлення критично застарілих систем.

HSE має «максимізувати отримані знання» від інциденту, включаючи впровадження узгоджених можливостей оперативної стійкості, включаючи безперервність клінічних та сервісних послуг та кризове управління, у всій організації, йдеться у звіті.

«Зменшення ризику кібербезпеки вимагає як трансформації можливостей кібербезпеки, так і трансформації IT, щоб вирішити проблеми застарілих і складних IT-майданчиків і вбудувати кібербезпеку та стійкість в IT-архітектуру».

Згідно зі звітом, інвестиційні зобов'язання HSE, які HSE повинні взяти, щоб покращити свою позицію кібербезпеки, «ймовірно, будуть кратними поточних витрат HSE на технології та операційну стійкість». Але, зазначається у звіті, такі витрати необхідні для захисту HSE від потенційних майбутніх атак, які можуть завдати ще більшої шкоди.

Заява HSE

У заяві, наданій для Information Security Media Group, HSE стверджує, що вже вніс термінові зміни, щоб захистити організацію від подібної майбутньої атаки, включаючи «розпочати впровадження рекомендацій у звіті PwC та співпрацю з Міністерством охорони здоров'я Ірландії щодо програми трансформації кібербезпеки».

Голова HSE Сіаран Девен каже: «Ми замовили цей терміновий огляд після кримінальної атаки на наші IT-системи, яка спричинила величезні порушення в медичних та соціальних службах в Ірландії, і вплив якої все ще відчувається щодня. Зрозуміло, що наші IT-системи та Підготовка до кібербезпеки потребує серйозних змін. Цей звіт підкреслює швидкість, з якою зростала витонченість кіберзлочинців, і в цьому звіті є важливі уроки для організацій державного та приватного секторів в Ірландії та за її межами».

За його словами, HSE прийняла висновки та рекомендації звіту та перебуває у процесі створення відповідних та стійких структур та посилених заходів безпеки.

Пол Рід, генеральний директор HSE, каже: «Ми розпочали низку негайних дій, і тепер ми розробимо план впровадження та бізнес-обґрунтування для інвестицій, щоб зміцнити нашу стійкість та чутливість у цій сфері».

У заяві HSE йдеться, що вона вже впровадила низку рішень високого рівня безпеки, зокрема нові засоби контролю кібербезпеки, моніторингу та розвідки загроз на основі рекомендацій міжнародних експертів.

Подібні виклики

За словами Джона Мура, директора з питань конфіденційності та безпеки консалтингової компанії Clearwater, шкоди від атаки HSE та подібних атак програм-вимагачів на інші медичні організації, у тому числі в США, здебільшого можна було уникнути.

«Проблема полягає в тому, що для впровадження методів кібербезпеки, які мінімізують ризик, потрібні зобов'язання від рівня правління до організації», – говорить він.

Він каже, що це вимагає інвестування часу та ресурсів, і що керівники бізнесу повинні розуміти роль безпеки, допомагаючи організації досягти своєї місії, ризик для місії від таких загроз, як програми-вимагачі. Організації повинні «приймати обґрунтовані рішення про те, як найкраще розподілити свої обмежені ресурси», каже Мур.

«Це включає в себе належну структуру управління та людей, впровадження та вдосконалення практик кібербезпеки, заснованих на визнаних структурах, таких

як NIST… та ефективне використання технологій для виявлення, захисту, виявлення, реагування та відновлення від атак», – говорить він.

«На жаль, це не відбувається за одну ніч». ***(Marianne Kolbasuk McGee. Report Dissects Conti Ransomware Attack on Ireland's HSE // Information Security Media Group, Corp. (https://www.govinfosecurity.com/report-dissects-conti-ransomware-attack-on-irelands-hse-a-18102). 10.12.2021).***

***

«Програми-вимагачі мають на увазі фінансово мотивований злочин. Крадіжка мільйонів доларів за допомогою вимагання є сучасним виразом тактики, набагато старішої за цифрові системи, які так часто страждають. Але зосередившись на програмі-вимагачі, оскільки злочинна діяльність не враховує реальну стратегічну цінність, яку ці операції можуть надати своїм власникам. Програми-вимагачі можуть бути використані для руйнівного впливу без будь-якого вірогідного бажання отримати фінансову вигоду (Росія), залучити фінансову підтримку для програм стратегічної зброї (Північна Корея), а також для прикриття, якщо не безпосередньої операції, збору розвідданих.

Цей останній стратегічний ефект заслуговує на особливу увагу, оскільки уряд США та його союзники працюють над протидією операціям із програмним забезпеченням-вимагачем після нещодавнього сплеску інцидентів, про які часто повідомлялося. Багато з політичних інструментів для кращого зміцнення державних і приватних систем і переслідування злочинних угруповань програм-вимагачів можуть не впоратися з ризиками стратегічної розвідки, які можуть спричинити операції з викупом. Це створює ризик передачі цінної інформації супротивникам через групи програм-вимагачів, які діють від їх імені або за певною координацією. Надана інформація може надати супротивникам як оперативне розуміння, так і стратегічний вплив у боротьбі зі Сполученими Штатами та їх союзниками у кіберпросторі.

Програма-вимагач призначена для шифрування даних цілі, поки жертва не заплатить зловмиснику викуп, в обмін на розшифрування даних. Схоже, що публічно повідомлені операції з використанням програм-вимагачів здійснюються переважно фінансово мотивованими злочинними організаціями. Ці операції мають низький технічний бар’єр для входу, оскільки потенційним групам програм-вимагачів не потрібні великі технічні знання для розгортання програм-вимагачів, але замість цього вони можуть покладатися на ринок постачальників програм-вимагачів, що розвивається, для надання інструментів та операційної підтримка. Цей ринок стимулює розвиток ряду програм-вимагачів, оскільки успіх однієї групи породжує імітацію, еволюцію та подальший успіх інших.

Однією з таких еволюцій за останні роки є поширення подвійного вимагання. Ця тактика загрожує не лише шифруванням даних, а й крадіжкою та/або витоком інформації. Відомо, що принаймні 16 груп програм -вимагачів використовували тактику подвійного вимагання у 2020 році, порівняно з однією такою групою у 2019 році. А згідно з одним звітом за 2021 рік, кількість випадків подвійного вимагання зросла на 935 відсотків у порівнянні з попереднім роком. Деякі іноземні розвідувальні служби прагнуть розвивати окремі партнерські відносини з групами

програм-вимагачів, які можуть надавати цінну інформацію, зібрану в процесі їх злочинних операцій. Дослідження вказало що Федеральна служба безпеки Росії (ФСБ) і Служба зовнішньої розвідки (СВР) отримують переваги від тісних робочих відносин з кількома російськими групами програм-вимагачів.

Іноземні розвідувальні служби можуть витягувати велику кількість інформації з операцій-вимагачів, які мають оперативну та стратегічну цінність. Ці операції можуть не дозволяти прямого стягнення коштів зі зрілого державного органу, але забезпечують легкий доступ до менш захищених організацій, які мають відчутну особисту цінність, як-от лікарні, психіатри, банки, дослідницькі лабораторії та державні підрядники. Атака програм- вимагачів у жовтні 2021 рокупро Planned Parenthood в Лос-Анджелесі та подальший витік інформації продемонстрував величезну кількість конфіденційних даних, які операції-вимагачі можуть вилучити з потрібних цілей — була оприлюднена особиста інформація 400 000 пацієнтів, включаючи подробиці про діагнози, процедури та рецепти.

Оперативно ця інформація може підтримувати майбутні операції кібер- або людської розвідки. Наприклад, отримуючи інформацію про звички та розпорядок об’єкта, зміст і стиль спілкування, фінансову стабільність та потенційно компрометуючий матеріал, іноземна розвідувальна служба могла б краще зрозуміти доступ особи, сприйнятливість та придатність для потенційного вербування як розвідувальний актив. На стратегічному рівні держави можуть використовувати цю інформацію для формування власної поведінки, участі в кампаніях впливу та отримання інтелектуальної власності для стимулювання інновацій.

Хоча це не є прикладом програмного забезпечення -вимагача, кампанія кібершпигунства Sunburst продемонструвала активне пошук Росією оперативної та стратегічної інформації через кібероперації в державному та приватному секторах. Широко розголошений компроміс програмного забезпечення Orion від SolarWinds був одним із багатьох напрямків, використаних SVR, щоб отримати доступ до найголовнішої нагороди агентства — хмарного середовища Microsoft Office 365, що цікавить цілей. Серед скомпрометованих цілей були високопоставлені урядовці, лідери галузі та — принаймні в одному випадку — чиновник з кабінету міністрів США, чиї електронні листи, календарі та файли були очищені під час кампанії. У жовтні 2021 року вказано у звітіщо в рамках кампанії Sunburst СВР збирала оперативну та стратегічну інформацію про розслідування контррозвідки США та політику санкцій проти російських осіб відповідно.

Програми-вимагачі надають нові переваги в порівнянні зі стандартними кібероперaціями для такого типу збору даних, оскільки його інтелектуальна цінність втрачається в шумі для політиків, стурбованих порушеннями та економічними наслідками. Адміністрація Байден наголошує в своїх поточних зусиллях по боротьбі з вимагачами в «фінансовому приводиться характер цієї діяльності,» волають сотні мільйонів доларів, що підприємства розщедрюватися у виплатах викупу. Адміністрація публічно не посилається на загрозу ексфільтрації даних, її потенційну стратегічну цінність для супротивників або намагання протистояти їм. Серед інших переваг, які може надати зловмисникам програм-вимагач, продемонстрував російський напад NotPetya 2017 року, вимоги викупу

можуть служити хитрістю для приховування справжніх намірів операції, відволікання захисників і порушення судово-медичної експертизи. Особа, яка реагує на інциденти, зайнята операцією кібершпигунства, що маскується під програмне забезпечення-вимагач, може повільніше реалізувати справжню мету операції. Можливо, найважливіше те, що ці операції заплутують процес атрибуції, дозволяючи державам працювати через групи програм-вимагачів, а не ризикувати викриттям, безпосередньо беручи участь у операціях.

У відносинах між державними розвідувальними органами та програмним забезпеченням-вимагачем держави можуть надавати пасивну підтримку у вигляді оперативних безпечних притулок за умови, що групи не націлені на суб'єктів на території держави. Держави також можуть надавати активнішу допомогу групам програм-вимагачів під час їхньої діяльності, надаючи керівництво і навіть технічну підтримку, що ще більше стирає межу між фінансованими державою та недержавними операціями. Партнерство між розвідувальними службами та групами програм-вимагачів може забезпечити такі держави, як Росія, певну відокремленість — і правдоподібне заперечення — від операцій, які на поверхні можуть здатися злочинними.

Служба іноземної розвідки не обов'язково повинна розгортати програму-вимагач безпосередньо або співпрацювати з тими, хто це робить. За допомогою спостереження, подібного до «збирання з боку четвертої сторони», — коли розвідувальна служба може активно або пасивно збирати розвідувальні дані на серверах управління іншої іноземної розвідувальної служби, щоб шпигувати за діяльністю іноземних шпигунів — іноземні розвідувальні служби можуть підтримувати додатковий ступінь поділу. відвідавши колодязь нічого не підозрюючих груп програм-вимагачів. Там вони можуть стежити за пошуками груп програм-вимагачів, де ці групи знаходять потенційно цінні розвідувальні цілі, але мимоволі.

Політики, загалом, розглядали сплеск атак програм-вимагачів як здебільшого економічний виклик із руйнівними наслідками. Незважаючи на те, що багато операцій із програмним забезпеченням-вимагачем зумовлені фінансами та завдають беззаперечної шкоди малим і середнім підприємствам, уряд США та його союзники можуть вжити подальших дій, щоб пом'якшити стратегічну розвідувальну цінність програм-викупників для супротивників і супутній ризик відмови від важелів впливу у кіберпросторі. Як зазначено у звіті Atlantic Council «Протидія програмному забезпеченню-вимогачу: уроки викрадення літаків», пом'якшення наслідків мають полягати в пасивних та активних заходах безпеки, щоб визначити пріоритет безпеки в екосистемі, водночас накладаючи витрати та шукаючи корінь проблеми.

Низька вартість програм-вимагачів і помітні ефекти становлять коктейль проблем для політиків у сфері кібербезпеки. Розпізнавання та реагування на потенційну цінність стратегічної розвідки операцій-вимагачів для основних супротивників допоможе уникнути згубної загрози через надмірне наголошення на більш гучній. В результаті уряд США та його союзники будуть більш ефективно конкурувати в період загострення стратегічної конкуренції». ***(Simon Handler. The***

Strategic Intelligence Value of Ransomware // The Lawfare Institute (https://www.lawfareblog.com/strategic-intelligence-value-ransomware). 15.12.2021).

***

«Кількість глобальних атак програм-вимагачів зростає. За даними Threatpost, у першому півріччі 2021 року глобальний обсяг операцій із програмним забезпеченням-вимагачем досяг 304,7 мільйона атак. Це на 151% більше, ніж за рік. Більше того, це понад 100 тисяч спроб атаки більше, ніж те, що дослідники безпеки виявили за весь 2020 рік.

Деякі операції сприяли цьому сплеску активності програм-вимагачів більше, ніж інші. Одним із них був Рюк, група нападників, з якими ми добре знайомі. Ми відстежуємо Ryuk з тих пір, як він вперше почав заражати жертв у 2018 році. Відтоді ми спостерігали, як зловмисники, відповідальні за Ryuk, співпрацюють з іншими цифровими злочинними операціями — іноді в тій же спробі атаки.

Хто може забути час, коли ми бачили, як Emotet завантажує TrickBot, розгортаючи Ryuk? Кіберзлочинці, націлені на великі підприємства, використовували спам для доставки трояна Emotet з метою подальшого поширення шкідливого програмного забезпечення TrickBot. Після того, як цільова машина була заражена зловмисним програмним забезпеченням TrickBot, зловмисники почали красти конфіденційну інформацію та визначати, чи є організація високоцінною метою – якщо так, вони продовжили доставляти програму-вимагач Ryuk.

Програми-вимагачі: постійна проблема

Розглянутий вище приклад показує, наскільки програмне забезпечення-вимагач залишається однією з найпомітніших загроз серед шкідливих програм. Розглянемо, наприклад, висновки Звіту про розслідування порушень даних за 2021 рік (DBIR). У своїй публікації Verizon зазначив, що 13% інцидентів, які не передбачали атаки відмови в обслуговуванні (DoS), включали компонент програмного забезпечення-вимагача.

У звіті дослідники також відзначили, що програмне забезпечення-вимагач з'являлося в 10% випадків зловживання даними, що подвоїло їх частоту за рік і стало третьою за поширеністю атакою за кількістю порушень даних. Ця зміна відображає ступінь, до якого банди програм- вимагачів прийняли подвійне вимагання — акт вилучення конфіденційних даних на додаток до їх шифрування та погрози їх витоку або продажу, якщо вимога викупу не буде задоволена. Додатковий стимул ускладнює зусилля цільових організацій із відновлення та дає змогу зловмисникам вимагати більших виплат викупу.

Подвійне вимагання було не єдиною новою технікою, яка допомогла зловмисникам-вимагателям зайняти третє місце в рейтингу дій Verizon щодо атак. Зловмисники також намагалися використати вразливості програмного забезпечення — деяким з них на той час було аж сім років — як засіб заробітку на слабких методах управління вразливими місцями організації.

За словами CSO, групи програм-вимагачів виявили особливий інтерес до CVE-2019-19781. Операція з програмним забезпеченням-вимагачем Ragnarok використовувала цю вразливість Citrix, щоб отримати доступ до мереж вразливих

організацій та завантажити інструменти для атаки, маскуючись як частину служб Windows Certificate Services.

Потім вони виконали свій двійковий файл, перш ніж видалити URL-адресу з кешу сертифікатів користувача. Black Kingdom та інші зловмисники-вимагачі також намагалися використати недолік CVE-2019-11510 Pulse як спосіб пограбування невиправлених корпоративних активів.

Збільшення витрат на програми-вимагачі

У сукупності ці тактики допомогли підвищити витрати, пов'язані з атаками програм-вимагачів. IBM зазначила у своєму дослідженні Cost of a Data Breach Study 2021, що середня атака програмного забезпечення-вимагача зараз коштує 4,62 мільйона доларів для відновлення. Це дорожче, ніж ціна в 4,24 мільйона доларів США за середній злом даних, але вона навіть не включає витрати, пов'язані з виплатою викупу та інші наслідки атаки.

Отже, що включає вартість атаки програмного забезпечення-вимагача? Наше дослідження щодо програм-вимагачів, проведене на початку цього року, під назвою «Програми-вимагачі: справжня вартість бізнесу» дає деякі ознаки. Розглянемо наступну статистику:

Втрата доходу від бізнесу: дві третини організацій заявили, що втратили прибуток через атаку програм-вимагачів.

Шкода бренду та репутації: більше половини (53%) організацій сказали, що вони зазнали шкоди своєму бренду та репутації після атаки.

Втрата таланту C-Level: приблизно третина респондентів заявили, що втратили талант C-Level після того, як зазнали інциденту з програмним забезпеченням-вимагачем.

Звільнення співробітників: приблизно троє з 10 учасників опитування вказали, що вони були змушені звільнити співробітників через фінансовий тиск, викликаний атакою програмного забезпечення-вимагача.

Закриття бізнесу: чверть організацій тимчасово закрили свою діяльність після зараження програмним забезпеченням-вимагачем.

Наш подальший звіт під назвою «Організації під загрозою: зловмисники не ходять у відпустку» показав, що 60% респондентів сказали, що атака програмного забезпечення-вимагача у вихідні або свята призвела до більш тривалого періоду для оцінки масштабу атаки, 50% сказали, що їм потрібно більше. час для ефективної реакції, а 33% сказали, що їм потрібен більший період, щоб повністю відновитися після атаки. Що стосується людського боку рівняння, 86% респондентів вказали, що вони пропустили свято або вихідні через атаку програм-вимагачів, ситуацію, яка може вплинути на задоволеність роботою співробітників і потенційне вигорання.

Але, незважаючи на значний вплив атак програм-вимагачів на організації, більшість з них просто не готові належним чином захищатися від них, навіть якщо їх організація вже зазнала успішної атаки програмного забезпечення-вимагача. Це останнє дослідження показало, що 49% вважають, що атака програм-вимагачів на їхню організацію була успішною, оскільки вони не мали правильних рішень безпеки.

Насправді, лише 67% організацій мали рішення NextGen Antivirus (NGAV), розгорнуте під час атаки, лише 46% мали традиційний антивірус на основі сигнатур (AV), а лише 36% мали функцію виявлення та реагування кінцевої точки. (EDR) рішення на місці.

Захист від сучасних атак програм-вимагачів

Ці висновки підкреслюють необхідність для організацій захищатися від більш складних, малоповільних операцій-вимагачів або RansomOps. Ви не можете покладатися на індикатори компромісу (IOC) від відомих атак – сьогоднішні RanomOps значною мірою налаштовані для цільової організації.

Найкраща стратегія для організацій — запобігти успішній атаці програм-вимагачів. Для цього вам потрібно інвестувати в багаторівневе рішення, яке використовує індикатори поведінки (IOBs) для виявлення та запобігання атаці програм-вимагачів на самих ранніх етапах початкового проникнення, до вилучення конфіденційних даних для подвійного вимагання та тривалого до того, як буде доставлено фактичне корисне навантаження програмного забезпечення-вимагача.

Операційний підхід Cybereason надає можливість раніше виявляти атаки RansomOps, і саме тому Cybereason залишається непереможеним у боротьбі з програмним забезпеченням-вимагачем з найкращими на ринку можливостями запобігання, виявлення та реагування.

Cybereason присвячений об’єднанню захисників, щоб припинити атаки програм-вимагачів на кінцеву точку, по всьому підприємству, скрізь, де відбувається бій. Дізнайтеся більше про рішення Cybereason Predictive Ransomware Protection, перегляньте наші ресурси захисту від програм- вимагачів або заплануйте демонстрацію сьогодні, щоб дізнатися, як ваша організація може отримати вигоду від операційного підходу до безпеки». ***(Anthony M. Freed. Ransomware by the Numbers – An Impact Overview // Techstrong Group Inc. (https://securityboulevard.com/2021/12/ransomware-by-the-numbers-an-impact-overview/). 07.12.2021).***

***

«Під час опитування понад 1500 професіоналів у сфері безпеки 60 відсотків респондентів повідомили, що розглядають програмне забезпечення-вимагач і тероризм як рівні загрози. Sapio Research провела опитування від імені постачальника послуг керування ідентифікацією машин Venafi.

Висновки перегукували з настроями Міністерства юстиції (DOJ), яке оголосило в червні 2021 року, що визначатиме пріоритет атак програм-вимагачів на рівні, який раніше зарезервував лише для тероризму, повідомляє Reuters.

Промисловість охорони здоров’я та інші сектори критично важливої інфраструктури зазнали особливого впливу від програм-вимагачів протягом останніх років, і атаки не сповільнюються. Понад 500 організацій охорони здоров’я повідомили про порушення даних, пов’язаних із захищеною медичною інформацією (PHI), до Управління з громадянських прав (OCR) HHS у 2021 році.

Дві третини опитаних спеціалістів із безпеки повідомили, що їхня організація зазнала атаки програм-вимагачів протягом останніх 12 місяців. Як великі, так і малі компанії зазнали значного впливу програм-вимагачів у минулому році.

Незважаючи на збільшення атак, 77% респондентів все ще сказали, що вони впевнені, що їхні поточні засоби безпеки захистять їх від майбутніх атак програм-вимагачів.

«Однак ця впевненість залежить від назви посади, що вказує на дещо меншу впевненість керівників груп безпеки, ніж керівників рівня С, в ефективності їхніх поточних наборів інструментів», – зазначається в опитуванні.

Висновки підтвердили попередні дослідження (ISC)I, які показали розрив між керівниками з кібербезпеки та керівниками C-suite, коли справа доходить до повідомлення про ризики програм-вимагачів.

Більше третини респондентів сказали, що вони сплатять викуп, але 57% цих респондентів сказали, що скасували б це рішення, якщо б їм доведеться публічно повідомити про платіж. Закон про розкриття інформації про програму-вимагач потенційно може вимагати від компаній повідомляти про платежі програм-вимагачів протягом 48 годин. Що стосується охорони здоров'я, про порушення, які зачіпають понад 500 осіб, необхідно повідомляти HHS.

Опитування також показало, що більшість сучасних засобів захисту поглибленої безпеки не підходять для сучасних IT-інфраструктур.

«Організації використовують широкий спектр засобів контролю безпеки, призначених для захисту від або обмеження впливу атаки програмного забезпечення-вимагача», – пояснюється у звіті.

«Однак більшість із цих засобів управління безпекою не оптимізовані для роботи з мережами без периметра, не кажучи вже про зміни інфраструктури, спричинені цифровою трансформацією. Зокрема, методології DevOps та програмно-визначені мережі вимагають різних стратегій безпеки, щоб розірвати ланцюжок знищення програм-вимагачів».

Понад 40 відсотків респондентів повідомили про використання VPN, а багато інших повідомили про використання звичайного зашифрованого резервного копіювання, технології захисту від фішингу та сканування уразливостей. У дослідженні наголошується, що з усіх досліджених засобів контролю безпеки лише деякі призначені для того, щоб фактично зламати ланцюжок знищення програм-вимагачів.

Незважаючи на їхню впевненість у сучасній практиці безпеки, понад три чверті опитаних спеціалістів із безпеки повідомили, що їх організація планує збільшити бюджет на програму-вимагач на наступний рік.

«Ці цифри свідчать про те, що групи безпеки усвідомлюють, що їхні поточні стратегії не забезпечують достатнього захисту, а також ймовірність того, що загрози програм-вимагачів будуть продовжувати зростати у 2022 році», — підсумовується у звіті.

«Команди InfoSec можуть виправдати ці інвестиції, оскільки вартість атаки програм-викупів — незалежно від того, чи вона успішна — може швидко перевищити вартість самої ціни викупу». ***(Jill McKeon. Security Professionals View Ransomware and Terrorism as Equal Threats // TechTarget, Inc. (https://healthitsecurity.com/news/security-professionals-view-ransomware-and-terrorism-as-equal-threats). 29.12.2021).***

***

«Дослідники Mandiant попередили про партнерську програму програм-вимагачів Sabbath, оператора програм-вимагачів, яка націлена на критичну інфраструктуру, освіту та охорону здоров'я. Дослідники виявили, що ця група, ймовірно, пов’язана з діяльністю програм-вимагачів під іменами Arcane і Eruption.

У вересні 2021 року на exploit.in учасники загроз шукають партнерів для нової партнерської програми-вимагача, виявив Mandiant. У червні 2021 року UNC2190, що працював як Arcane і Sabbath, націлився на критичну інфраструктуру в США та Канаді. До 21 жовтня 2021 року Sabbath, іноді відомий як 54BB47h, створив сайт і блог для ганьби.

«На відміну від більшості інших партнерських програм, Mandiant спостерігав два випадки, коли оператор програм-вимагачів надавав своїм філіям попередньо налаштовані бекдорні корисні навантаження Cobalt Strike BEACON», – пояснюється у звіті Mandiant.

«Хоча використання BEACON є звичайною практикою під час вторгнень програм-вимагачів, використання оператора партнерської програми викупу за умови, що BEACON є незвичайним і створює проблеми для атрибуції, а також пропонує додаткові можливості для виявлення».

Багато суб’єктів загроз ухиляються від націлювання на критичну інфраструктуру, оскільки це привертає до їхньої роботи велику увагу громадськості та уряду. Проте групи програм-вимагачів все частіше націлені на охорону здоров’я, освіту та інші критично важливі організації, хоча міжнародні уряди присвятили свою увагу та ресурси, щоб зупинити їх.

«Субота вперше з’явилася у жовтні 2021 року, коли група публічно присоромила та вимагала шкільний округ США на Reddit та з тепер призупиненого облікового запису Twitter @54BB47h», – йдеться у звіті.

«Під час цього недавнього вимагання актор-загроза вимагав багатомільйонну виплату після розгортання програм-вимагачів. ЗМІ вказують на те, що група вжила надзвичайно агресивного кроку, надсилаючи електронні листи співробітникам, батькам і навіть учням безпосередньо, щоб посилити громадський тиск на шкільний округ».

Виявилося, що Sabbath не є винятком із все більш сміливих дій, які здійснюють великі групи програм-вимагачів. Органи охорони здоров’я повинні бути пильними та стежити за підозрілою мережевою активністю.

«UNC2190 продовжував працювати протягом останнього року, вносячи лише незначні зміни в свої стратегії та інструменти, включаючи впровадження комерційного пакувальника та ребрендинг їхньої пропозиції послуг», – йдеться у звіті.

«Це підкреслює, як добре відомі інструменти, такі як BEACON, можуть призвести до вражаючих і прибуткових інцидентів, навіть якщо їх використовують менш відомі групи».

У жовтні Mandiant опублікував звіт, у якому викладено походження та практики FIN12, варіанта програм-вимагачів, що спеціалізується на кібератаках у

сфері охорони здоров’я. Дослідники виявили, що майже 20 відсотків жертв групи програм-вимагачів FIN12 були в секторі охорони здоров’я.

Координаційний центр кібербезпеки сектору охорони здоров’я (HC3) у грудні опублікував запис про загрози, в якому викладалися ризики та тактики пом’якшення проти FIN12.

За словами Джеремі Кеннеллі, старшого менеджера та головного аналітика Mandiant, FIN12 небезпечний з трьох причин: вони працюють з надзвичайною швидкістю, вони непередбачувані та продовжують орієнтуватися на охорону здоров’я навіть у разі негативної реакції.

«FIN12 протягом своєї діяльності завжди націлювався на медичні організації. Ми не помітили жодних пропорційних змін, навіть перед обличчям пандемії або перед обличчям широкої реакції громадськості на операції з викупом», — пояснив Кеннеллі HealthITSecurity в попередньому інтерв’ю.

«Сам факт недоступності систем спричиняє величезні збої в роботі цих організацій. Таким чином, серед цих акторів, ймовірно, існує думка, що, незважаючи на поганий вигляд орієнтації на організацію охорони здоров’я, організація охорони здоров’я матиме вагоміші аргументи, щоб потенційно заплатити викуп, щоб запустити свою систему в Інтернет». ***(Jill McKeon. Sabbath Ransomware Targeting Healthcare, Mandiant Warns // TechTarget, Inc. (https://healthitsecurity.com/news/sabbath-ransomware-targeting-healthcare-mandiant-warns). 08.12.2021).***

***

«Принаймні, 39 груп вимагачів атакували сектор охорони здоров'я в 27 країнах протягом останніх 18 місяців, дані від кібер - інциденти Tracer в кіберсвіту інституту виявлені. Незважаючи на те, що вони не будуть орієнтуватися на охорону здоров’я, 12 груп виділили цей сектор.

Деякі медичні організації можуть бути просто побічною шкодою, пояснюється в супровідній публікації в блозі. Деякі оператори програм-вимагачів використовували розпливчасті терміни, наприклад «медичні організації», описуючи, які організації заборонені. Інші вважали фармацевтичні компанії чесною грою. Половина з 12 операторів програм-вимагачів були націлені на лікарні, незважаючи на те, що вони не будуть орієнтуватися на охорону здоров’я.

«Згідно з трьома операторами програм-вимагачів, такі атаки можуть статися помилково, і в цьому випадку ключ дешифрування буде наданий «безкоштовно», — пояснюється в блозі.

«Як би благородно вони не намагалися показати цей жест, намір не має значення для жертви (жертв). Щойно програму-вимагач розгорнуто, шкода завдано».

Інші групи орієнтуються на охорону здоров’я за своїм вибором. Філія групи FIN12 має репутацію йти після медичних організацій. Розвідувальна компанія Mandiant виявила, що майже 20 відсотків атак угруповання були спрямовані на медичні установи, а понад 70 відсотків були спрямовані на установи, що базуються в США.

Інколи медичні організації можуть бути націлені через байдужість. Зазвичай це означає, що медичні організації стають жертвами тактики «розпилюй і молись», коли оператори програм-вимагачів проводять фішингові кампанії або атаки грубої сили протоколу віддаленого робочого столу (RDP) з надією змусити деякі організації піддатися атаці.

«Незалежно від того, чи є націлення на організації охорони здоров'я помилковим, задумом чи байдужістю, оператори програм-вимагачів діють безкарно і де-факто визначають, які організації є законними об'єктами, а що заборонено», – йдеться у дописі в блозі.

«Однак їхні спрощені відмінності ігнорують складність та взаємозв'язок сектору охорони здоров'я, в якому атака на фармацевтику під час пандемії може мати такий же руйнівний вплив на людину, як і напад на лікарні».

Hive, Pysa, Conti, LockBit, Groove і REvil/Sodinokibi були одними з провідних операторів програм-вимагачів у 2021 році за кількістю атак. Кібератаки можуть зробити більше, ніж розкрити дані або вивести системи в автономний режим. У деяких випадках медичні організації змушені перенаправляти пацієнтів до інших лікарень або скасовувати прийоми.

Оскільки екосистема кіберзагроз продовжує розвиватися, групи програм-вимагачів продовжуватимуть знаходити нові та інноваційні способи атаки. Однак незмінним було те, що майже всі групи програм-вимагачів суворо фінансово мотивовані.

Злочинці переслідуватимуть організації, які, на їхню думку, є найбільш уразливими або з найбільшою ймовірністю платять викуп. Дані про здоров'я також надзвичайно цінні в темній мережі, що робить цей сектор ще більш прибутковою метою.

Незважаючи на те, що оператори програм-вимагачів здебільшого мотивовані фінансово, міністр внутрішньої безпеки США Алехандро Майоркас заявив USA Today у жовтні, що наступною серйозною загрозою кібербезпеки буде «кіберпрограмне забезпечення», на яке слід звернути увагу.

Майоркас вказав на напад у лютому 2021 року на водоочисну споруду у Флориді, під час якої суб'єкти загрози намагалися підняти рівень лугу в громадському водопроводі до небезпечного рівня.

Незважаючи на те, що Killware звучить як надзвичайно шкідлива та небезпечна загроза, малоймовірно, що Killware стане щоденною загрозою для медичних організацій, оскільки це приверне багато небажаної уваги до операторів програм-вимагачів, Браян Врозек, CISO в Optiv Security, раніше сказав HealthITSecurity.

«Вони продовжуватимуть націлюватися, використовуючи ті самі методи», – припустив Врожек. «Я не бачу, щоб вони дійсно адаптували свої методи або те, що вони намагаються атакувати, як намагання підвищити рівень тривоги жертв, щоб переконати їх платити і платити більше».

Фішинг, програми-вимагачі, зловживання застарілими системами та інші перевірені тактики й надалі використовуватимуться регулярно.

«Основною проблемою тут є і залишається відсутність відповідальності, що дозволило цим групам діяти майже безкарно і з позиції влади», – стверджується в блозі Інституту КіберМиру.

«Це частково пов’язано з тим, що аналіз таких акторів часто спирався на інформацію, яку самі ці групи готові показати під виглядом своїх брендів. Однак ці бренди є лише транспортним засобом, а програми-вимагачі — лише інструментом. Таким чином, щоб притягнути їхніх винних до відповідальності, потрібно дивитися не тільки на їх бренди-вимагачі, а на кібер-екосистему (злочинну)». ***(Jill McKeon. 39 Ransomware Groups Targeted Healthcare in the Past 18 Months // TechTarget, Inc. (https://healthitsecurity.com/news/39-ransomware-groups-targeted-healthcare-in-the-past-18-months). 17.12.2021).***

***

«AvosLocker, новичок на рынке программ-вымогателей, наращивает количество атак, используя при этом некоторые новые методы, чтобы попытаться уклониться от программ безопасности.

Фирма по безопасности Sophos предупреждает, что AvosLocker, банда программ-вымогателей, управляемая людьми, возникшая этим летом, ищет партнеров - таких как «брокеры доступа», которые продают доступ к уже взломанным машинам - в надежде заполнить пробел, оставленный REvil. вывод.

Одной из ключевых особенностей AvosLocker является использование инструмента удаленного ИТ-администрирования AnyDesk и запуск его в безопасном режиме Windows. Последний вариант использовался REvil, Snatch и BlackMatter как способ отключить предполагаемую безопасность цели и инструменты ИТ-администратора. Как указывает Sophos, многие продукты для обеспечения безопасности конечных точек не работают в безопасном режиме - специальной диагностической конфигурации, в которой Windows отключает большинство сторонних драйверов и программного обеспечения и может сделать защищенные машины небезопасными.

AnyDesk, законный инструмент удаленного администрирования, стал популярной среди злоумышленников альтернативой TeamViewer, предлагавшей те же функции. Запуск AnyDesk в безопасном режиме при подключении к сети позволяет злоумышленнику сохранять контроль над зараженными машинами.

В то время как AvosLocker просто переупаковывает методы других банд, Питер Маккензи, директор по реагированию на инциденты в Sophos, охарактеризовал их использование как «простое, но очень умное».

Маккензи говорит, что, хотя Avos скопировал технику безопасного режима, установка AnyDesk для управления машинами в безопасном режиме - первая.

Злоумышленники AvosLocker перезагружают машины в безопасном режиме на заключительных этапах атаки, но также изменяют конфигурацию загрузки в безопасном режиме, чтобы разрешить установку и запуск AnyDesk.

Sophos отмечает в своем блоге, что законные владельцы могут не иметь возможности удаленно управлять компьютером, если он настроен для запуска AnyDesk в безопасном режиме. Администратору может потребоваться физический

доступ к зараженному компьютеру для управления им, что может создать проблемы для большой сети компьютеров и серверов Windows.

Sophos обнаружил еще несколько любопытных приемов, используемых AvosLocker. Компонент Linux, например, нацелен на серверы гипервизора VMware ESXi, уничтожая любые виртуальные машины (ВМ), а затем шифруя файлы ВМ. Sophos исследует, как злоумышленники получили учетные данные администратора, необходимые для включения ESX Shell или доступа к серверу.

Злоумышленники также использовали инструмент управления ИТ PDQ Deploy, чтобы отправить несколько пакетных сценариев Windows на целевые машины, включая Love.bat, update.bat и lock.bat. Как объясняет Sophos, примерно за пять секунд эти скрипты отключают продукты безопасности, которые могут работать в безопасном режиме, отключают Защитник Windows и позволяют злоумышленнику AnyDesk работать в безопасном режиме. Они также создают новую учетную запись с автоматическими данными для входа, а затем подключаются к целевому контроллеру домена для удаленного доступа и запуска исполняемого файла вымогателя update.exe.

Sophos предупреждает: «Программы-вымогатели, особенно когда они были доставлены вручную (как это было в случае этих экземпляров Avos Locker), представляют собой сложную проблему, которую нужно решить, потому что нужно иметь дело не только с самой программой-вымогателем, но и с любыми механизмами, которые злоумышленники создали лазейку в целевой сети. Ни одно оповещение не должно рассматриваться как «низкий приоритет» в этих обстоятельствах, каким бы безобидным оно ни казалось». ***(Liam Tung. This new ransomware has simple but very clever tricks to evade PC defenses // ZDNet (https://www.zdnet.com/article/this-new-ransomware-has-simple-but-very-clever-tricks-to-evade-pc-defenses/). 23.12.2021).***

***

«Гигант фотографии и персонализированной фотографии Shutterfly подвергся атаке программы-вымогателя Conti, которая якобы зашифровала тысячи устройств и украла корпоративные данные.

Хотя многие ассоциируют Shutterfly со своим веб-сайтом, услуги компании, связанные с фотографией, ориентированы на потребителей, предприятий и образовательных учреждений через различные бренды, такие как GrooveBook, BorrowLenses, Shutterfly.com, Snapfish и Lifetouch.

Основной веб-сайт можно использовать для загрузки фотографий, создания фотокниг, персонализированных канцелярских принадлежностей, поздравительных открыток, открыток и т.д.

Shutterfly подвергся атаке программы-вымогателя Conti

В пятницу источник сообщил BleepingComputer, что примерно две недели назад на Shutterfly была совершена атака вымогателя со стороны банды Конти, которая утверждает, что зашифровала более 4000 устройств и 120 серверов VMware ESXi.

Хотя BleepingComputer не видел переговоров о нападении, нам говорят, что они ведутся в процессе и что вымогатели банда требуют миллионов долларов в качестве выкупа.

Прежде чем банды вымогателей зашифруют устройства в корпоративных сетях, они обычно прячутся внутри в течение нескольких дней, если не недель, крадут корпоративные данные и документы. Эти документы затем используются в качестве рычага давления, чтобы заставить жертву заплатить выкуп под угрозой того, что они будут опубликованы или проданы другим хакерам.

В рамках этой тактики «двойного вымогательства» Conti создал частную страницу утечки данных Shutterfly, содержащую скриншоты файлов, предположительно украденных во время атаки вымогателя. Злоумышленники угрожают сделать эту страницу общедоступной, если не будет уплачен выкуп.

BleepingComputer сообщили, что эти скриншоты включают в себя юридические соглашения, информацию о банках и торговых счетах, учетные данные для входа в корпоративные службы, электронные таблицы и, как представляется, информацию о клиентах, включая последние четыре цифры кредитных карт.

Conti также утверждает, что имеет исходный код для магазина Shutterfly, но неясно, имеет ли банда вымогателей Shutterfly.com или другой веб-сайт.

После того, как в пятницу BleepingCompuer связался с Shutterfly по поводу атаки, ему было отправлено заявление, подтверждающее атаку вымогателя поздно вечером в воскресенье.

В этом заявлении, которое полностью показано ниже, говорится, что сайты Shutterfly.com, Snapfish, TinyPrints или Spoonflower не пострадали от атаки. Однако их корпоративная сеть, Lifetouch, BorrowLeneses и Groovebook нарушила работу служб.

«Shutterfly, LLC недавно испытала атаку программы-вымогателя на части нашей сети. Этот инцидент не затронул наши сайты Shutterfly.com, Snapfish, TinyPrints или Spoonflower. Тем не менее, некоторые части нашего бизнеса Lifetouch и BorrowLenses, Groovebook, производства и некоторых корпоративных систем пострадали. были перебои. Мы привлекли сторонних экспертов по кибербезопасности, проинформировали правоохранительные органы и круглосуточно работали над устранением инцидента».

«В рамках нашего продолжающегося расследования мы также оцениваем полный объем любых данных, которые могли быть затронуты. Мы не храним информацию о кредитных картах, финансовых счетах или номера социального страхования наших Shutterfly.com, Snapfish, Lifetouch, TinyPrints., BorrowLenses или Spoonflower, и поэтому ни одна из этих сведений не была затронута в этом инциденте. Однако понимание характера данных, которые могли быть затронуты, является ключевым приоритетом, и это расследование продолжается. Мы продолжим предоставлять обновления по мере необходимости» - Shutterfly.

В то время как Shutterfly заявляет, что финансовая информация не разглашается, BleepingComputer сообщили, что на одном из снимков экрана указаны последние четыре цифры кредитных карт, поэтому неясно, была ли украдена дополнительная и более важная информация во время атаки.

Когда BleepingComputer обратилась к Shutterfly по поводу скриншота, они вернули нас к исходному заявлению.

Банда программ-вымогателей Conti

Conti - это операция по вымогательству, которой, как полагают, занимается российская хакерская группа, известная своими другими печально известными вредоносными программами, такими как Ryuk, TrickBot и BazarLoader.

Эта операция выполняется как программа-вымогатель как услуга, при которой основная группа разрабатывает программу-вымогатель, поддерживает сайты для платежей и утечки данных и ведет переговоры с жертвами. Затем они нанимают «партнеров», которые взламывают корпоративную сеть, крадут данные и шифруют устройства.

В рамках этой договоренности выплаты выкупа распределяются между основной группой и аффилированным лицом, при этом аффилированное лицо обычно получает 70-80% от общей суммы.

Conti обычно взламывает сеть после того, как корпоративное устройство заражается вредоносными программами BazarLoader или TrickBot, которые обеспечивают удаленный доступ к хакерской группе.

Получив доступ к внутренней системе, они распространяются по сети, собирают данные и развертывают программы-вымогатели.

Конти известен своими атаками на другие известные организации в прошлом, в том числе на Управление здравоохранения Ирландии (HSE) и Департамент здравоохранения (DoH), город Талса, государственные школы округа Бровард и Advantech.

В связи с возросшей активностью банды киберпреступников правительство США недавно выпустило рекомендацию по атакам программ-вымогателей Conti». ***(Lawrence Abrams. Shutterfly services disrupted by Conti ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomware-attack/?mid=1#cid=26444). 27.12.2021).***

***

«Относительно новая программа-вымогатель Pysa была доминирующей разновидностью атак с шифрованием файлов в ноябре, и согласно анализу, проведенному компанией по безопасности NCC Group, число атак на правительственные организации увеличилось на 400%.

Pysa - одна из банд программ-вымогателей, использующих двойное вымогательство, чтобы вынудить жертв заплатить вымогательство, и сбросила утечки от 50 ранее скомпрометированных организаций в прошлом месяце. В целом в ноябре количество атак Pysa увеличилось на 50%, что означает, что он обогнал Conti и присоединился к Lockbit в двух самых распространенных версиях вредоносного ПО. По данным NCC Group, с августа доминируют сорта Conti и Lockbit.

Необъяснимо, Pysa утекает данные от целей через несколько недель или месяцев после попытки вымогательства. Масштабная свалка данных последовала за совместными действиями правоохранительных органов США и ЕС против

некоторых членов банды вымогателей REvil, которые стояли за атакой на поставщика ИТ-услуг Касею.

Также известная как Меспиноза, банда Пизы ищет доказательства преступности среди целей, чтобы использовать их в качестве рычага во время обычно многомиллионных переговоров о вымогательстве.

ФБР начало отслеживать активность Pysa в марте 2020 года при атаках программ-вымогателей на правительство, учреждения, частный сектор и сектор здравоохранения. Группа часто использует методы фишинга для учетных данных, чтобы скомпрометировать подключения по протоколу удаленного рабочего стола (RDP).

Pysa нацелена на крупные финансовые, государственные и медицинские организации, отмечает NCC Group.

Во всех бандах вымогателей общее число жертв из Северной Америки достигло 154 в течение месяца, из которых 140 были организациями США, а число жертв из Европы в ноябре составило 96. Промышленный сектор был наиболее атакуемым, в то время как атаки на технологический сектор снизились на 38%.

NCC Group также обращает внимание на русскоязычную банду программ-вымогателей Everest Group, которая раздвигает новые границы двойного вымогательства, не только угрожая утечкой файлов, но и предоставляя своим клиентам доступ к ИТ-инфраструктуре жертв. Вместо того, чтобы добиваться выкупа, группа продает сторонний доступ к сети цели, создавая новый способ монетизации скомпрометированной цели. Группа NCC предупреждает, что если это окажется прибыльным, это может стать тенденцией в следующем году.

«В ноябре группа предложила своим жертвам платный доступ к ИТ-инфраструктуре, а также пригрозила раскрыть украденные данные, если жертва откажется платить выкуп», - отмечается в сообщении.

«Хотя продажи программ-вымогателей как услуги резко выросли за последний год, это редкий случай, когда группа отказывается от запроса выкупа и предлагает доступ к ИТ-инфраструктуре, но мы можем увидеть атаки подражателя в 2022 году и не только». ***(Liam Tung. This ransomware strain just started targeting lots more businesses // ZDNet (https://www.zdnet.com/article/this-ransomware-strain-just-started-targeting-lots-more-businesses/). 22.12.2021).***

***

«…Канадский центр кибербезопасности («CCCS») предложил несколько причин увеличения активности программ-вымогателей, включая переход к онлайн-операциям на протяжении всей пандемии и растущую изощренность киберпреступников. Возможно, наибольшую тревогу вызывает появление «программы-вымогателя как услуги», когда разработчики продают или сдают в аренду свои программы-вымогатели другим киберпреступникам, получая взамен процент от выкупа жертвы.

Тем не менее, как отмечает CCCS, организации могут предотвратить или смягчить подавляющее большинство атак с использованием программ-вымогателей, реализовав базовые меры кибербезопасности. Вот почему 30 ноября 2021 года CCCS выпустила учебник для программ-вымогателей («Пособие»),

чтобы помочь организациям подготовиться к атакам программ-вымогателей и отреагировать на них…

На какие компании нацелены киберпреступники?

Предприятия любого размера могут быть объектами атак программ-вымогателей. В то время как атаки на более крупные корпорации могут быть более прибыльными для киберпреступников, как отмечается в Playbook, киберпреступники часто считают, что малые и средние организации имеют более слабые меры защиты, что делает их более легкой мишенью. [5]

Следующие факторы делают компанию более вероятной целью атаки программ-вымогателей:

Компания имеет доступ к конфиденциальным данным, которые могут быть использованы напрямую, таким как номера социального страхования, номера кредитных карт или другая финансовая информация;

Компания имеет доступ к личной информации, которую люди не хотели бы раскрывать, например, к медицинской или религиозной информации;

Данные являются важным компонентом бизнеса компании, так что нарушение работы систем компании остановило бы весь их бизнес (увеличивая вероятность того, что компания заплатит выкуп);

Компания владеет ценными данными клиентов или интеллектуальной собственностью, например коммерческой тайной;

Компания участвует в критически важной инфраструктуре, например, в жизненно важных медицинских услугах; или

Компания связана с компанией, отвечающей одному из приведенных выше описаний.

Первая половина Пособия посвящена тому, как компания может защитить себя от программ-вымогателей. Он охватывает планирование киберзащиты и базовые меры кибербезопасности. Что касается планирования киберзащиты, Пособие предоставляет полезный обзор принципов, которые следует учитывать при разработке (i) плана резервного копирования, (ii) плана реагирования на инциденты и (iii) плана восстановления.

Что касается мер кибербезопасности, Playbook предоставляет список полезных мер безопасности данных, включая, помимо прочего:

Защита периметра, такая как межсетевые экраны, антифишинговое программное обеспечение и виртуальные частные сети;

Ведение журнала и оповещение для отслеживания активности в системе, что помогает установить контрольный журнал;

Тестирование на проникновение для оценки уязвимостей;

Сегментация сети для контроля и ограничения доступа к информации в вашей ИТ-системе; и

Управление паролями для обеспечения использования более надежных паролей в вашей организации.

Вторая половина пособия посвящена восстановлению после атак программ-вымогателей. Он охватывает действия по немедленному реагированию, которые компании должны предпринять в случае взлома, и действия, которые помогут компании как можно быстрее восстановить свой бизнес после атаки…» ***(Mitch***

Koczerginski, Robbie Grant. Canadian Centre for Cyber Security Releases Ransomware Playbook // McMillan LLP (https://mcmillan.ca/insights/canadian-centre-for-cyber-security-releases-ransomware-playbook/). 21.12.2021).

***

«…По данным IDC, в 2020 году объем данных, созданных или реплицированных по всему миру, достигнет 64,2ZB, и в ближайшие годы он будет продолжать расти со среднегодовым темпом роста 23%.

Итак, учитывая этот экспоненциальный рост объема данных, которые организации генерируют и хранят, можем ли мы немного расслабиться, заботясь о них? Конечно, нет. Если бы данные не были ценными, у нас не было бы бедствий программ-вымогателей, и технические руководители не беспокоились бы по этому поводу бессонными ночами.

По прогнозам Gartner, три четверти ИТ-организаций столкнутся с одной или несколькими угрозами вымогательства в период с настоящего момента до 2025 года. По оценкам Cybersecurity Ventures, атака вымогателя происходит каждые 11 секунд, и это приведет к предполагаемым финансовым потерям в размере более 20 миллиардов долларов в 2021 году.

В то же время «новые» модели программ-вымогателей вызывают наибольшую озабоченность ИТ-руководителей, как показывает отчет Emerging Risks Monitor от Gartner, поскольку организации, занимающиеся вымогательством, становятся «более специализированными и в остальном эффективными». По мнению Gartner, одними из наиболее тревожных событий являются «вирусы, которые задерживаются и заражают системы резервного копирования, не полагаются на фишинг как вектор, вирусы, которые труднее идентифицировать, такие как «бесфайловые» и «криптоджекинговые» атаки».

Как говорит Мэтт Шинкман из Gartner, последствия атаки с использованием программ-вымогателей могут быть серьезными и даже фатальными для любой организации: «Длительные задержки в работе, потеря и разглашение данных, а также последующий ущерб репутации представляют потенциальные риски для существования организации, которая руководители слишком хорошо осведомлены об этом, особенно если атаки происходят в результате неадекватного контроля кибербезопасности».

Итак, защита данных явно необходима. Но компаниям необходимо понимать, какие данные им нужно защищать.

Ваши данные вчера и сегодня

Архитектор решений Veeam Software Джон Вуд отмечает: «Данные, которыми вы располагаете сегодня, несомненно, являются наиболее ценными данными».

Но эти данные могут также использоваться в системах искусственного интеллекта или аналитики, которые направляют компании в будущее: «Вчерашние данные столь же важны для понимания того, откуда вы пришли и, возможно, куда вы идете». А исторические или архивные данные за многие годы очень сложно воссоздать.

Проблема в том, как объясняет Сумит Калия, специалист по управлению данными и хранению данных AWS, традиционные подходы к защите данных не были разработаны с учетом современных угроз: «Акцент был сделан на каком-то стихийном бедствии, таком как наводнение или землетрясение, и сосредоточены на физическом разделении, доставке на магнитную ленту и высокой доступности между площадками».

Действительно ли эти стратегии защищают вас от атаки программ-вымогателей? Например, как компании обеспечивают безопасность своего вторичного центра обработки данных? Какими должны быть рекомендации по RPO и RTO после атаки программы-вымогателя? Как восстановление с ленты квадрата с возвращением бизнеса электронной коммерции в онлайн, чтобы минимизировать потерянный доход?

«Это вопрос, который вам нужно задать бизнесу», - советует Калия. «И ответ «ну, не совсем» - это то, что мы слышим довольно часто».

Итак, как вы должны подойти к защите этих данных? И гарантировать, что вы сможете восстановить его и запустить в случае вымогателя или любого типа кибератаки?

По словам Калии, компании должны начинать с чего-то вроде NIST Cybersecurity Framework, которая предоставляет пятиступенчатую инструкцию по выявлению рисков, защите сервисов, обнаружению угроз и реагированию на атаки. Пятый шаг - выздоровление. И именно этим часто пренебрегают.

«Это становится одной из наиболее важных областей для клиентов с точки зрения обеспечения того, чтобы у них был страховой полис, который позволяет им восстанавливаться в любой момент», - говорит Калиа. «Это то, что помогает нашим клиентам быстро восстанавливаться, сводя к минимуму любые сбои, а также соблюдая любые бизнес-требования и нормативные требования».

«Фреймворк NIST служит основой всего рабочего процесса Veeam по защите данных, - отмечает Вуд. Первый шаг - помочь клиентам определить, что нужно защитить, и обеспечить это в неизменяемом хранилище. Платформу Veeam также можно использовать для мониторинга и сканирования данных на предмет потенциальных уязвимостей или компрометаций, например, путем обнаружения значительных изменений в наборах данных.

Но «другая половина любой защиты данных - это возможность восстановления в случае возникновения события, будь то использование технологий мгновенного восстановления или технологий безопасного восстановления».

Veeam Instant Recovery обеспечивает немедленное восстановление рабочих нагрузок в виде виртуальных машин, запуская их непосредственно из сжатых и удаленных файлов резервных копий, без необходимости извлекать виртуальные машины и копировать их в производственное хранилище.

Но вы действительно поправились?

Secure Restore предоставляет возможность сканировать данные на наличие вредоносных программ перед их восстановлением в производственной среде, позволяя администраторам либо остановить процесс, либо позволить ему продолжить с ограничениями.

И хотя иметь план восстановления - это здорово, еще лучше знать, что он действительно работает, поэтому Veeam также подчеркивает возможность тестирования возможности восстановления данных в случае, например, атаки программы-вымогателя.

Наконец, по словам Вуда, Veeam обязана обеспечить максимальную безопасность своих процессов, особенно с учетом растущей угрозы распространения программ-вымогателей, например, через скомпрометированные цепочки поставок.

«Нам нужно практиковать то, что мы проповедуем… убедиться, что наша цепочка поставок безопасна, чтобы гарантировать, что то, что мы доставляем нашим клиентам, имеет встроенную безопасность, чтобы они могли быть уверены, что мы относимся к безопасности как к нулевому приоритету дня.»

Но если разработка правильного процесса - это одна задача, то другая - решить, где на самом деле ее осуществить.

Как отмечает Калиа, даже если у компаний есть традиционные резервные центры обработки данных, им, возможно, придется столкнуться с возможностью того, что компрометация одного почти наверняка будет означать, что вторичный центр обработки данных также будет скомпрометирован.

Он объясняет, что AWS «в значительной степени использует проактивный подход к безопасности инфраструктуры, который не полагается на типичные защитные или реактивные подходы, а вместо этого обеспечивает безопасность инфраструктуры с нуля. Это также включает культуру».

Как может предприятие или другая крупная организация надеяться имитировать это? «Используя те же инструменты, что и AWS это те же инструменты, которые доступны вам сегодня, поэтому вы можете создавать эти решения для обеспечения безопасности на основе событий с помощью различных сервисов AWS»

Например, AWS предлагает объектное хранилище с возможностями объектной блокировки через AWS S3, эффективно предлагая модель WORM, что означает, что клиенты могут быть уверены, что данные не были изменены. «Всякий раз, когда у бизнеса возникает потребность в соблюдении нормативных требований, особенно в финансовом и медицинском секторах, вы можете просто сделать золотую копию этой деловой документации».

Но если AWS может предоставить основную платформу и инструменты для безопасного хранения данных, говорит Вуд, «вам нужны партнеры, такие как Veeam, чтобы в полной мере воспользоваться этой возможностью».

Это включает в себя обеспечение того, чтобы «данные были там правильным образом, в правильной форме, но также не ограничиваясь данными. Как мне вернуть его вовремя? Я храню его наиболее эффективным способом? Это все, на что на самом деле смотрит Veeam. Это не просто «брось туда мои данные, и все будет хорошо».

И это принципиальный вопрос. Компании часто рассматривают резервное копирование и аварийное восстановление как последнюю линию защиты, когда с их критически важной инфраструктурой случается немыслимое. Это нужно перевернуть с ног на голову.

Компании должны смириться с тем, что они будут подвергаться атакам, и будут делать это неоднократно. Это означает, что процессы восстановления больше не являются крайней мерой, а станут, если не рутинными, то, несомненно, регулярным явлением.

И как только вы совершите этот скачок, проблема защиты данных перестанет быть дополнением к вашей критически важной инфраструктуре. Вместо этого резервное копирование и восстановление сами по себе становятся критически важной инфраструктурой». ***(Joseph Martins. Protecting your critical infrastructure is one thing…protecting your backups is the same thing // The Register (https://www.theregister.com/2021/12/03/protecting_backups_ransomware/). 03.12.2021).***

***

Програми-трояни

«Qakbot, ведущий троян для кражи банковских учетных данных, в прошлом году начал предоставлять программы-вымогатели, и эта новая бизнес-модель усложняет сетевым защитникам обнаружение того, что является атакой Qakbot, а что нет.

Qakbot - это особенно универсальная вредоносная программа, которая существует уже более десяти лет и выжила, несмотря на многолетние усилия Microsoft и других фирм, занимающихся безопасностью, по ее искоренению. Qakbot в 2017 году применил методы бокового перемещения WannaCry, такие как заражение всех сетевых ресурсов и дисков, брутфорс учетных записей Active Directory и использование протокола обмена файлами SMB для создания собственных копий.

Недавний анализ Qakbot, проведенный «Лабораторией Касперского», показал, что он не исчезнет в ближайшее время. Статистика обнаружения Qakbot показала, что в период с января по июль 2021 года он заразил на 65% больше компьютеров по сравнению с тем же периодом прошлого года. Итак, это растущая угроза.

Microsoft подчеркивает, что Qakbot является модульным, что позволяет ему проявлять себя как отдельные атаки на каждое устройство в сети, что затрудняет обнаружение, предотвращение и удаление средств защиты и средств безопасности. Защитникам также сложно обнаружить это, потому что Qakbot используется для распространения нескольких вариантов вымогателей.

«Из-за высокой вероятности перехода Qakbot к атакам, управляемым человеком, включая кражу данных, боковое перемещение и вымогательство несколькими участниками, обнаружение, наблюдаемое после заражения, может сильно различаться», - говорится в отчете группы аналитики угроз Microsoft 365 Defender.

Учитывая эти трудности при выявлении общей кампании Qakbot, команда Microsoft проанализировала методы и поведение вредоносного ПО, чтобы помочь

аналитикам в области безопасности искоренить это универсальное вредоносное ПО.

Основной механизм доставки - это вложения, ссылки или встроенные изображения по электронной почте. Однако также известно использование макросов Visual Basic для приложений (VBA), а также устаревших макросов Excel 4.0 для заражения компьютеров. В июле компания TrendMicro проанализировала крупную кампанию Qakbot, в которой использовался этот метод.

Другие группы, такие как Trickbot, недавно начали использовать макросы Excel 4.0 для вызова Win32 API и выполнения команд оболочки. В результате Microsoft отключила эти типы макросов по умолчанию, но Qakbot использует текст в документе Excel, чтобы обманом заставить цели вручную включить макрос.

Qakbot использует внедрение процессов, чтобы скрыть вредоносные процессы, создавая запланированные задачи для сохранения на компьютере и манипулируя реестром Windows.

После запуска на зараженном устройстве он использует несколько методов бокового перемещения, использует среду тестирования на проникновение Cobalt Strike или развертывает программы-вымогатели.

В прошлом году ФБР предупредило, что трояны Qakbot поставляют ProLock, вариант программы-вымогателя, управляемой человеком. Это было тревожным событием, потому что компьютеры, зараженные Qakbot в сети, должны быть изолированы, поскольку они служат мостом для атаки программ-вымогателей.

Microsoft отмечает, что MSRA.exe и Mobsync.exe использовались Qakbot для внедрения этого процесса, чтобы запустить несколько команд сетевого «обнаружения» и затем украсть учетные данные Windows и данные браузера.

Модуль Cobalt Strike Qakbot поддается другим преступным группировкам, которые могут сбрасывать свои собственные полезные нагрузки, такие как программы-вымогатели. Согласно Trend Micro, Qakbot предоставил MegaCortex и PwndLocker (2019 г.), Egregor и ProLock (2020 г.) и Sodinokibi / REvil (2021 г.).

«У Qakbot есть модуль Cobalt Strike, и участники, которые покупают доступ к машинам с предыдущими заражениями Qakbot, могут также использовать свои собственные маяки Cobalt Strike и дополнительные полезные нагрузки», - отмечает Microsoft.

«Использование Cobalt Strike позволяет злоумышленникам получить полный доступ с клавиатуры к затронутым устройствам, что позволяет им выполнять дополнительное обнаружение, находить важные цели в сети, перемещаться в боковом направлении и сбрасывать дополнительные полезные нагрузки, особенно варианты программ-вымогателей, управляемых человеком, такие как как Конти и Эгрегор ".

Рекомендуемые Microsoft меры по минимизации воздействия Qakbot включают включение защиты от фишинга Office 365, включение SmartScreen и сети в браузере Edge и обеспечение сканирования макросов во время выполнения путем включения интерфейса сканирования на вредоносное ПО Windows (AMSI).

AMSI поддерживается антивирусом Microsoft Defender и несколькими сторонними поставщиками антивирусов. Поддержка AMSI для макросов Excel 4.0 появилась в марте, так что это все еще относительно новая функция». ***(Liam Tung.***

This old malware has just picked up some nasty new tricks // ZDNet (https://www.zdnet.com/article/this-decade-old-malware-has-picked-up-some-nasty-new-tricks/). 10.12.2021).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«У понеділок в рамках спільної операції між Румунською національною поліцією, ФБР та Європолом заарештували румуна, якого звинувачують у використанні програм-вимагачів для націлювання на «високі» організації та компанії.

Чоловіка, ідентифікованого лише як 41-річного мешканця в Крайові, Румунія, звинувачують у скомпрометації неназваної румунської компанії з ІТ-послуги з клієнтами у роздрібній торгівлі, енергетиці та комунальних послугах, йдеться в заяві Європолу, опублікованій на веб-сайті агентства.

Потім він використав цей доступ для розгортання програм-вимагачів і викрадення конфіденційних даних у клієнтів ІТ-компанії в Румунії та за кордоном, перш ніж зашифрувати файли. Викрадені дані включали фінансову інформацію, особисту інформацію про співробітників і клієнтів та інші важливі документи.

Потім чоловік попросив «значний викуп у криптовалюті», йдеться у заяві Європолу, із загрозою опублікувати викрадені дані на форумах про кіберзлочинність.

Аллан Ліска, директор із розвідки загроз у фірмі з кібербезпеки Recorded Future, сказав у понеділок, що, виходячи з наявної інформації, це «видається, що це була одноразова, а не традиційна партнерська модель програмного забезпечення-вимагача». Незрозуміло, чи був цей чоловік інсайдерською загрозою, чи він придумав, як проникнути в мережу ІТ-компанії, сказала Ліска.

«Мене заінтригує використання вимагання без традиційного сайту вимагання», – додала Ліска, посилаючись на поширену практику зловмисників-вимагачів, які розміщують зразки вкрадених даних на веб-сайтах, щоб примусити жертв платити. «Як часто це трапляється? Чи є набагато більше атак програм-вимагачів, які ми ніколи не бачимо, тому що вони налаштовані таким чином, разова атака з боку когось поза партнерською системою, хто не має доступу до сайту з вимаганням?»

ФБР не відразу відповіло на запит про коментарі щодо його ролі в операції.

Арешт в понеділок приходить приблизно через місяць після того, як влада Румунії, Європол та інші правоохоронні органи по всьому світу оголосили про арешт двох кіберзлочинності не підозрює обвинувачений в запуску 5000 вимагачів атак з використанням Revil / Sodinokibi шкідливих програм, до недавнього часу один з найбільш часто використовуваних штамів вимагачів. Ця операція збіглася з вилученням Міністерством юстиції США 6 мільйонів доларів у вигляді платежів із програмним забезпеченням-вимагачем і звинувачень проти росіянина Євгена

Поляніна та громадянина України Ярослава Васінського за операції, пов’язані з програмним забезпеченням-вимагачем REvil». ***(AJ Vicens. Romanian ransomware suspect arrested in joint Europol, FBI operation // CyberScoop (https://www.cyberscoop.com/ransomware-suspect-romanian-revil-europol-fbi/). 13.12.2021).***

***

«За даними міністерства юстиції США, громадянина Росії засудили до 48 місяців ув'язнення за сприяння схемі бот-мережі, яка заражала пристрої жертв зловмисним програмним забезпеченням Kelihos і програмним забезпеченням-вимагачем.

41-річний Олег Кошкін був засуджений федеральним журі США 15 червня за одним звинуваченням у змові з метою скоєння комп'ютерного шахрайства та зловживання, а також за одним звинуваченням у комп'ютерному шахрайстві та зловживанні. Він був заарештований у Берклі, штат Каліфорнія, у вересні 2019 року і з тих пір перебуває під вартою.

Кошкін керував веб-сайтами Crypt4U.com, fud.bz та іншими, які всі пропоновані послуги використовували для приховування шкідливого програмного забезпечення Kelihos від антивірусного програмного забезпечення. Веб-сайти обіцяли зробити шкідливе програмне забезпечення повністю невиявленим майже всіма основними постачальниками антивірусного програмного забезпечення.

За словами прокурора, його визнали винним у пособництві Петру Левашову, оператору ботнету Kelihos, у нанесенні шкоди 10 або більше захищених комп’ютерів.

Схема ботнету

Кошкін і його співпідсудний Павло Цуркан заявили, що зловмисне програмне забезпечення може використовуватися для шифрування бот-мереж, троянських програм віддаленого доступу, кейлоггерів, крадіжок облікових даних і майнерів криптовалюти, повідомляє Міністерство юстиції.

«Обвинувачений надав важливу послугу, яку використовували кіберзлочинці, щоб уникнути однієї з перших ліній захисту кібербезпеки — антивірусного програмного забезпечення», — каже Кеннет А. Полит-молодший, помічник генерального прокурора кримінального відділу Міністерства юстиції. «Кіберзлочинці залежать від подібних служб для зараження комп’ютерів у всьому світі зловмисним програмним забезпеченням, зокрема програмним забезпеченням-вимагачем».

Співпідсудного Цуркана, заарештованого 6 вересня 2019 року в Естонії та екстрадованого до США 4 березня 2021 року, звинувачують у змові з метою заподіяння шкоди 10 або більше захищених комп’ютерів, а також у пособництві Левашову у нанесенні шкоди захищеним комп’ютерам., злочин, який передбачає покарання у вигляді позбавлення волі на строк до 10 років.

Цуркан, який був звільнений під заставу в 200 тисяч доларів, очікує вироку.

Кошкін і Левашов разом розробили систему, яка дозволила б Левашову шифрувати шкідливе програмне забезпечення Kelihos кілька разів на день.

«Кошкін надав Левашову спеціальну послугу шифрування великого обсягу, яка дозволила Левашову розповсюджувати Kelihos через декілька кримінальних філій», - заявили прокурори.

За словами суду, ботнет використовувався для розсилки спам-листів, збору облікових даних банківського рахунку та проведення поширених атак відмови в обслуговуванні, а також розповсюдження програм-вимагачів та іншого шкідливого програмного забезпечення.

«Келіхос покладався на послуги шифрування, які надавалися Crypt4U з 2014 року до арешту Левашова в квітні 2017 року; і лише за останні чотири місяці цієї змови Келіхос заразив приблизно 200 000 комп'ютерів по всьому світу», – кажуть прокурори.

Левашов був заарештований Національною поліцією Іспанії в квітні 2017 року і екстрадований до США. У вересні 2018 року він визнав себе винним у навмисному пошкодженні захищеного комп'ютера, змові, шахрайстві та крадіжці особистих даних при обтяжуючих обставинах.

У обвинувальному акті проти Левашова 2017 року прокуратура заявила, що ботнет Kelihos щороку розповсюджував сотні мільйонів шахрайських електронних листів, перехоплював облікові дані в Інтернеті та фінансові рахунки тисяч американців, а також поширював програми-вимагачі в їхніх мережах.

У обвинуваченні Левашова стверджується, що він брав участь і модерував кримінальні онлайн-форуми, на яких торгували та продавалися викрадені особи, кредитні картки, шкідливі програми та інші засоби кіберзлочинності.

У обвинуваченні також стверджується, що Левашов платив Кошкіну 3000 доларів на місяць за його послуги, і що на момент арешту Левашова Келіхос заразив щонайменше 50 000 комп'ютерів, включаючи комп'ютери в Коннектикуті.

Алан Колдер, генеральний директор GRC International Group, глобального постачальника рішень з управління IT, управління ризиками та відповідності, розповідає ISMG: «Це класичний приклад сучасного середовища кіберзагроз – надзвичайно складні кіберзлочинці, які працюють у великих масштабах та розгортають програмне забезпечення для атаки через філії та ботнети. Це хороша новина, що двох злочинців вилучили з обігу, хоча це лише тимчасовий вирок. Цілком ймовірно, що вони не будуть останніми, хто скористається вразливими місцями в Інтернеті, тому ми повинні залишатися пильними». ***(Prajeet Nair. Russian Who Aided Kelihos Botnet Receives 4-Year Sentence // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russian-who-aided-kelihos-botnet-receives-4-year-sentence-a-18111). 13.12.2021).***

***

«Федеральний обвинувальний акт, опублікований сьогодні на Алясці, звинувачує громадянина Канади у скоєнні кібератак.

Згідно з судовими документами, 31-річний Метью Філберт з Оттави, Онтаріо, Канада, у квітні 2018 року вчинив змову та пошкодив комп'ютер, що належить штату Аляска.

Під час окремого паралельного розслідування канадська влада сьогодні також оголосила проти Філберта кіберзвинувачення. Він був заарештований 30 листопада поліцією провінції Онтаріо, де він залишається під вартою.

Філберта звинувачують за одним звинуваченням у змові з метою шахрайства та пов'язаної з ним діяльності, пов'язаної з комп'ютерами, та одного звинувачення в шахрайстві та пов'язаній діяльності з комп'ютерами. Це звинувачення в окрузі Аляски є частиною поточних національних зусиль Міністерства юстиції щодо боротьби з кіберзлочинами, спрямованими на громадян США з-за кордону.

Про це повідомили помічник генерального прокурора Кеннет А. Полит-молодший із кримінального відділу міністерства юстиції, виконувач обов'язків прокурора США Браян Вілсон з округу Аляска та відповідальний спеціальний агент Ентоні Юнг з польового офісу ФБР в Анкоріджі.

Польовий офіс ФБР в Анкоріджі розслідує справу. Помічник генерального прокурора Ввічливий, виконувач обов'язків прокурора США Вілсон і відповідальний спеціальний агент ФБР Юнг подякували владі Канади та Нідерландів за допомогу.

Помічник прокурора США Адам Александер і прокурор Олден Пелкер із відділу комп'ютерних злочинів та інтелектуальної власності Відділу кримінальних проваджень переслідують справу». ***(Canadian Man Charged with Scheme to Commit Cyberattacks // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/canadian-man-charged-with-scheme-to-commit-cyberattacks/). 07.12.2021).***

***

«Европейский центр киберпреступности Европола работал с национальной полицией Румынии и ФБР над арестом подозреваемого филиала вымогателя, который якобы преследовал важные организации и компании за их конфиденциальные данные.

Европол сообщил, что 41-летний румын был арестован в Крайове, Румыния. В нем говорится, что этот человек подозревается в компрометации сети крупной румынской ИТ-компании, которая предоставляет услуги клиентам в розничной торговле, энергетике и коммунальном хозяйстве.

Подозреваемый обвиняется в атаках программ-вымогателей, шифровании файлов и краже конфиденциальных данных. Его подозревают в требовании «значительного» выкупа в криптовалюте и угрозе утечки украденных данных, если жертва не поддастся попытке вымогательства.

Злоумышленник украл финансовую информацию о компании, личную информацию о сотрудниках, сведения о клиентах и другие конфиденциальные данные, а также попытался шантажировать жертву с целью выплаты выкупа с угрозой публикации данных. Была ли попытка вымогательства успешной или нет, не сообщается.

Европол поддержал расследование, отслеживая платежи в криптовалюте, предоставляя анализ вредоносных программ и криминалистическую поддержку, а также направляя экспертов в Румынию.

Этот арест является последним в череде арестов румынскими властями, которые в прошлом месяце арестовали двух человек, подозреваемых в причастности к атакам с использованием программ-вымогателей Sodinokibi / REvil.

В недавнем отчете Европола говорится, что атаки программ-вымогателей становятся все более изощренными, поскольку киберпреступники обращаются к новым тактикам и методам, чтобы максимизировать шансы на успешное получение выкупа, что регулярно обходится жертвам в миллионы долларов.

«Преступники продолжают действовать все более безжалостно и методично», - говорится в сообщении». ***(Danny Palmer. Ransomware suspect arrested over attacks on 'high-profile' organisations // ZDNet (https://www.zdnet.com/article/ransomware-suspect-arrested-over-attacks-on-high-profile-organisations/). 13.12.2021).***

***

«Британская полиция произвела серию арестов за последние несколько месяцев после того, как люди, имеющие очевидный доступ к базам данных NHS, якобы продавали поддельные записи о вакцинации в приложении для паспорта вакцины NHS.

На этой неделе отдел киберпреступности столичной полиции объявил об аресте трех человек после того, как неопознанный фонд NHS «заметил подозрительную картину в некоторых записях о вакцинации в Интернете», как сообщает эссексская газета Yellow Advertiser.

Двое мужчин в возрасте 23 и 27 лет, предположительно из Илфорда на востоке Лондона, были арестованы по подозрению в совершении преступлений, связанных с нарушением Закона о неправомерном использовании компьютеров. Третий мужчина, также из Илфорда, был арестован аналогичным образом в рамках отдельного, не связанного с этим расследования. Полиция провела обыск в домах и изъяла различные электронные устройства, говорится в заявлении полиции, направленном в The Reg.

Детектив-суперинтендант Хелен Рэнс сказала: «Персонал обоих трастов поступил правильно и сообщил о своих опасениях, что позволило нам полностью расследовать обстоятельства. Я хочу заверить общественность, что никакие системы не были взломаны извне сети NHS и целостность систем NHS остается надежной».

Джейк Мур, глобальный советник по кибербезопасности антивирусной компании ESET и бывший руководитель отдела цифровой криминалистики в полиции Дорсета, сказал нам: «Это важный момент для местных групп по борьбе с киберпреступностью, которые часто получают много критики из-за того, что едва могут справиться с ситуацией. даже небольшой процент цифровых преступлений при ограниченных ресурсах и отсутствии централизованно хранимых денег».

Он продолжил: «Хотя это и не было удаленным нападением, эти конкретные аресты подчеркивают важность инсайдера для того, чтобы такая операция могла происходить незаметно. от небрежности в их процессе. Следующим шагом, конечно, будет, если полиция сможет найти достаточно цифровых доказательств для судебного преследования».

Закон о неправомерном использовании компьютеров квалифицирует как уголовное преступление доступ к компьютерной системе без разрешения. Последние аресты последовали за октябрьским расследованием Mail on Sunday, в котором утверждалось, что он разоблачил британца, который использовал учетную запись Telegram для продажи поддельных записей в паспорте с вакцинами. Ранее в этом году Guardian опубликовала статью, в которой освещается растущая мировая торговля поддельными паспортами вакцинации и приложениями.

Спрос на поддельные документы может возрасти после того, как на этой неделе депутаты проголосовали за обязательность паспортов на вакцины, а последние юридические нормы были разъяснены BBC.

Приложение NHS для паспорта вакцины получило зеленый свет в мае, несмотря на то, что борцы за гражданские свободы предупреждали, что оно рискует создать социальные разногласия между теоретиками заговора против вакцины, людьми, выступающими против паспортов вакцины, и сторонниками схемы.

Противники паспортов вакцины подчеркнули предыдущие обещания правительства о том, что паспорта вакцины не будут использоваться в качестве обязательного условия входа в общественные места, и вскоре отказались от них, когда они увидели, что паспорта будут полезны для замедления распространения вредоносных вариантов COVID-19.

Обработка личных данных пациентов в NHS England во время пандемии была туманной. Компания Palantir, занимающаяся технологиями наблюдения в США, оказалась в центре потоков данных NHS - государственная организация здравоохранения, как ни странно, не желала сообщать, сколько данных было передано Palantir и почему. В то время как это происходило, NHS также готовилась к запуску «самого большого сбора данных» в своей истории, перемещая данные пациентов терапевта из их местных кабинетов в центральное хранилище. Это было временно отложено из-за общественного протеста.

Тем временем бывшее техническое подразделение NHS England, NHSX, заявила, что данные, собранные с телефонов людей с помощью приложения для отслеживания контактов, будут храниться для неопределенного «исследования». Став синонимом полусогласованного сбора и перепродажи данных пациентов, NHSX позже был переименован в Управление трансформации NHS England в ноябре 2021 года». ***(Gareth Corfield. East Londoners nicked under Computer Misuse Act after NHS vaccine passport app sprouted clump of fake entries // The Register (https://www.theregister.com/2021/12/16/fake_nhs_vaccine_passport_arrests_met_police/). 16.12.2021).***

***

Технічні аспекти кібербезпеки

«Дослідники кібербезпеки з Університету Рутгерса в Нью-Брансвіку та Технологічного інституту Джорджії запропонували нові способи захисту 3D-

друкованих об'єктів, таких як дрони, протези та медичні пристрої, від прихованих «логічних бомб».

Дослідники презентують свою роботу під назвою «Фізичні логічні бомби в 3D-принтерах за допомогою нових 4D-технологій» на щорічній конференції з комп'ютерної безпеки в грудні 2021 року.

Швидке створення прототипів – це швидке виготовлення деталі, моделі або збірки за допомогою 3D-комп'ютерного проектування, зазвичай з використанням 3D-друку або «адитивного виробництва». Адитивне виробництво все частіше використовується в ряді галузей для виробництва продукції, що має критичне значення для безпеки, але в даний час не існує надійних методів для перевірки їх цілісності проти суперечливих модифікацій перед друком.

«Кібер-фізичне адитивне виробництво наступного покоління забезпечує передові конструкції та можливості продуктів, але воно все більше покладається на високо мережеві промислові системи управління, які створюють можливості для кібератак», – сказав головний дослідник Саман Зонуз, доцент електротехніки та комп'ютерної техніки в інженерна школа Рутгерс-Нью-Брансвік. «Переважний підхід до захисту від цих загроз покладається на детектори вторгнень на базі хоста, які знаходяться в межах одних і тих самих цільових контролерів, а отже, часто є першою метою атак на контролер».

Дослідники розглянули Mystique, новий клас атак на друковані об'єкти, які використовують новітню технологію 4D-друку для впровадження вбудованого комп'ютерного коду – або логічних бомб – шляхом маніпулювання виробничим процесом.

Mystique дозволяє візуально нешкідливим об'єктам поводитися зловмисно, коли логічна бомба спрацьовує подразником, таким як зміна температури, вологості, pH або модифікації матеріалів, які були використані спочатку, що потенційно може викликати катастрофічні збої в роботі під час їх використання.

Дослідники успішно оцінили Mystique на кількох прикладах 3D-друку і показали, що він може уникнути попередніх контрзаходів. Для вирішення цієї проблеми вони запропонували дві стратегії.

Перше рішення зосереджено на розробці датчика, який може вимірювати склад і діаметр сировини, що проходить через екструдер принтера, щоб забезпечити відповідність очікуванням до того, як об'єкт буде надрукований. Діелектричний датчик може виявити зміну діаметра нитки на 0,1 мм і зміну концентраційного складу на 10%.

Друге рішення використовує зображення комп'ютерної томографії з високою роздільною здатністю для виявлення залишкових напружень у друкованих об'єктах, які контрастують між доброякісними та шкідливими дизайнами перед активацією атаки. Це виявлення КТ має точність 94,6% при ідентифікації 4D-атак в одному шарі друку.

Дослідницька група планує надати рекомендації щодо об'єднання рішень щодо стійкості в безпеці програмного забезпечення, розробці систем управління та обробці сигналів, а також для включення надійного та практичного виявлення кібер-фізичних атак у виробництво в реальному світі.

«Наша пропозиція – це новий потенційний вектор атаки, який необхідно враховувати та ефективно пом’якшувати на платформах адитивного виробництва. Ідея полягає в тому, щоб використовувати нові фізичні логічні бомби в 3D-друкованих об’єктах, таких як промислове обладнання та засоби індивідуального захисту, такі як маски від COVID-19», – сказав Зонуз. «Ці логічні бомби пізніше можуть бути активовані супротивниками, використовуючи такі фізичні подразники, як волога або тепло, коли це підходить для них, щоб вивести друковані об’єкти з ладу, наприклад, щоб маска COVID втратила захист від вірусної інфекції». ***(Researchers Unveil New Cyber Protections against «Logic Bombs» // Newswise, Inc (https://www.newswise.com/articles/researchers-unveil-new-cyber-protections-against-logic-bombs). 13 12 2021).***

***

«Новое исследование, проведенное компанией Ermetic, занимающейся облачной безопасностью, показывает, что почти у всех предприятий есть идентификационные данные, которые в случае взлома могут поставить под угрозу не менее 90 процентов корзин S3 в их учетной записи AWS.

Ermetic провела исследование, чтобы определить обстоятельства, при которых программы-вымогатели могут проникнуть в корзины Amazon S3. Исследование выявило очень высокий потенциал программ-вымогателей в среде организаций.

Amazon Simple Storage Service (Amazon S3) - это сервис объектного хранилища, который предлагает масштабируемость, доступность данных, безопасность и производительность. По словам Amazon, клиенты любого размера и отрасли могут использовать его для хранения и защиты любого объема данных в различных сценариях использования. Эти варианты использования включают озера данных, веб-сайты, мобильные приложения, резервное копирование и восстановление, архивирование, корпоративные приложения, устройства Интернета вещей и аналитику больших данных.

Amazon S3 предоставляет простые в использовании функции управления, позволяющие подписчикам систематизировать данные и настраивать точно настроенные средства управления доступом в соответствии с конкретными бизнес-требованиями и требованиями организации и нормативными требованиями. Amazon S3 рассчитан на надежность 99,9% (11 9) и хранит данные для миллионов приложений для компаний по всему миру, утверждает Amazon.

Ковши AWS S3 считаются очень надежными и используются с большой уверенностью. Но заинтересованные стороны в облачной безопасности не осознают, что корзины S3 подвергаются серьезному риску безопасности из-за неожиданного источника: идентификационных данных, - написал Лиор Затлави, старший облачный архитектор в Ermetic, при обсуждении официального отчета компании «Новое исследование: угроза программ-вымогателей для корзин S3». в своем октябрьском отчете.

«Скомпрометированная личность с опасной комбинацией прав может легко запустить программу-вымогатель для данных организации», - написал он.

Основные результаты

Исследователи искали личности с разрешениями, которые имели возможность и не имели эффективного смягчения и воздействия фактора риска. Эти условия позволили злоумышленникам запустить программу-вымогатель как минимум на 90% корзин S3 в учетной записи AWS.

Результаты выявили высокий потенциал проникновения программ-вымогателей, если AWS не использует средства защиты от угроз. Результаты включают:

В каждой из выбранных сред имелась по крайней мере одна учетная запись AWS, удостоверение которой - а часто и несколько - соответствовало указанным выше критериям.

Более чем в 70% сред экземпляры EC2 соответствовали указанным выше критериям, при этом фактором риска было общедоступность в Интернете.

Более того, разрешения, которые давали доступ к корзинам, были чрезмерными. Их можно было значительно уменьшить без ущерба для бизнес-операций, просто удалив ненужные разрешения.

Более чем в 45% сред роли IAM (управление идентификацией и доступом) были доступны для стороннего использования, которым было разрешено повысить свои привилегии до уровня администратора.

Это открытие невероятно и ужасно с точки зрения безопасности облака, помимо программ-вымогателей. Это означает, что корзины S3 в среде были подвержены вымогательству.

Более чем в 95% сред пользователи IAM соответствовали указанным выше критериям, при этом фактором риска были ключи доступа, которые были включены, но не менялись в течение 90 дней.

Почти в 80% сред пользователи IAM соответствовали указанным выше критериям, при этом фактором риска были ключи доступа, которые были включены, но неактивны в течение более 180 дней.

Почти в 60% сред пользователи IAM соответствовали указанным выше критериям, при этом фактором риска был доступ к консоли, который был включен, но без требования использовать MFA при входе в систему.

Более 96 процентов сред имели неактивные роли IAM, и почти 80 процентов сред имели неактивных пользователей IAM, которые соответствовали вышеуказанным критериям.

Тревожные результаты

Эти результаты сосредоточены на операциях «разбей и захвати» с участием одной скомпрометированной личности. По словам Затлави, они раскрывают серьезную ситуацию.

«В целевых кампаниях злоумышленники могут двигаться горизонтально, чтобы скомпрометировать несколько идентификаторов и использовать свои комбинированные разрешения, что значительно улучшит их способность запускать программы-вымогатели», - пояснил он.

Короче говоря, согласно исследованным образцам, миллионы предприятий, которые в настоящее время используют S3 в качестве надежного хранилища данных, подвергаются опасности атак программ-вымогателей. Он предупредил, что высокая вероятность заражения даже простыми операциями с программами-

вымогателями является четким призывом к действиям для заинтересованных сторон, занимающихся безопасностью облачных вычислений.

AWS S3 давно стал стандартом для хранения данных файловых объектов. Несмотря на многочисленные усилия по обеспечению безопасности S3, мониторинг безопасности продолжает обнаруживать данные в частных корзинах, раскрываемых или используемых новыми способами, - сказал Эрканг Чжэн, основатель и генеральный директор JupiterOne.

«Сколькими способами я могу споткнуться о собственные ведра и выплеснуть данные? Короткий ответ - слишком много», - сказал он TechNewsWorld.

Облачные сервисы сегодня почти полностью построены на сторонних инструментах. Подумайте о ролях CI / CD, инструментах мониторинга, сервисах платформы для хранилищ данных, лямбдах и машинном обучении. «У всех есть тонкая прокладка, отражающая особенности бизнеса», - добавил Мохит Тивари, соучредитель и генеральный директор Symmetry Systems.

«Эти идентификаторы могут записывать данные и, следовательно, также могут использовать эти данные с помощью программ-вымогателей. Один этот факт, вероятно, объясняет количество рискованно звучащих личностей в отчете», - сказал он TechNewsWorld.

Смешанный мешок с опасностями для ведра

Эксперты по безопасности в последнее время заметили значительный рост числа случаев взлома открытых корзин S3 просто из-за неправильной конфигурации. «Если пользователи не могут даже настроить базовое безопасное облачное хранилище с надлежащим шифрованием, авторизацией и аутентификацией, мы будем еще хуже защищать реальные уязвимости в самих системах хранения данных», - заметил Чжэн.

«Несмотря на то, что AWS обеспечивает скрытую защиту инфраструктуры, они также позволяют гибко настраивать ресурсы и доступ к ним. Вы несете ответственность за понимание этой гибкости и правильное применение средств управления. Однако такая гибкость иногда может мешать и усложнять ситуацию. Вот почему я долгое время был сторонником использования графической модели данных и автоматизированного анализа данных в помощь», - сказал он.

Он добавил, что узнать, какие киберактивы существуют в данный момент времени, сложно из-за эфемерности облачной инфраструктуры. Организациям необходим постоянный мониторинг своих киберактивов, чтобы обеспечить бдительность, необходимую для предотвращения случайного раскрытия информации в будущем.

По словам Затлави из Ermetic, сегменты S3, к которым имели доступ идентификаторы, не были защищены эффективными готовыми функциями AWS для смягчения воздействия.

Сами по себе третьи стороны не опасны. Собственные удостоверения могут быть подвергнуты фишингу или эксплуатации, что сопряжено с риском. По словам Тивари, числа, вероятно, покажут, что атаки OWASP (Open Web Application Security Project) и фишинговые идентификационные данные являются чрезвычайно надежными угрозами.

«Наконец, отчеты, которые вызывают опасения, неуверенность и сомнения в отношении облачной IAM, опровергают тот факт, что, предоставляя открытый программируемый интерфейс для разрешений, облако позволяет использовать лучшие инструменты безопасности для масштабирования в масштабах всей организации. «Организации, которые внедряют автоматизацию безопасности - и начинают с того, что важно, своих данных - обнаружат, что облако намного безопаснее, чем надежные локальные среды», - предположил он». ***(Jack M. Germain. Threat of Ransomware Lurks in Amazon S3 Buckets // ECT News Network, Inc. (https://www.technewsworld.com/story/threat-of-ransomware-lurks-in-amazon-s3-buckets-87359.html). 07.12.2021).***

***

«Эксперты по ИТ-безопасности из Рурского университета Бохума (RUB) и Университета прикладных наук Нидерландов выявили 14 новых разновидностей атак на веб-браузеры, известных как межсайтовые утечки или XS-Leaks. Используя XS-Leaks, вредоносный веб-сайт может получать личные данные посетителей, взаимодействуя с другими веб-сайтами в фоновом режиме.

Исследователи проверили, насколько хорошо 56 комбинаций браузеров и операционных систем защищены от 34 различных XS-Leaks. Для этого они разработали веб-сайт XSinator.com, который позволяет автоматически тестировать браузеры на наличие таких проблем. Их эксперимент, в частности, продемонстрировал уязвимость к значительному количеству XS-утечек популярных браузеров, таких как Chrome и Firefox.

«XS-Leaks – это часто недоработки браузера, которые должны исправляться его производителем», – говорит Лукас Книттель (Lukas Knittel) из RUB, один из авторов статьи по итогам этого исследования. Статья была опубликована онлайн и представлена на виртуальной конференции ACM по безопасности компьютеров и коммуникаций в середине ноября.

XS-утечки применяются для обхода так называемой политики одинакового происхождения (same-origin), одной из основных линий защиты браузеров от различных типов атак. Задача политики одинакового происхождения – предотвратить кражу информации с надёжного веб-сайта. В случае XS-Leaks злоумышленники, тем не менее, могут распознать отдельные детали веб-сайта и организовать кражу связанных с этими деталями персональных данных. Например, с вредоносного сайта можно будет прочесть электронные письма в почтовом ящике потому что функция поиска будет реагировать по-разному в зависимости от того, были ли результаты для поискового запроса или нет.

Для того, чтобы систематизировать анализ XS-Leaks, группа сначала выделила три отличительные характеристики таких атак. На их основе была разработана формальная модель, которая помогает понять XS-утечки и обнаруживать новые атаки. В результате применения этой модели исследователи смогли обнаружить 14 новых категорий таких атак». ***(Обнаружены 14 новых способов обхода защиты популярных веб-браузеров // Компьютерное Обозрение (https://ko.com.ua/obnaruzheny_14_novyh_sposobom_obhoda_zashhity_populyarnyh_veb-brauzerov_139605). 03.12.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Остерегайтесь уязвимости Log4j! Эта неприятная программная ошибка вызывает панику в ИТ-мире, преследуя нас в преддверии Нового года.

Несомненно, многие организации и малые и средние предприятия, у которых нет ИТ-персонала, не знают о его существовании. Но незнание Log4j только делает их более уязвимыми для атак. Они остаются беззащитными.

Log4j - это очень распространенный раздел кода, который помогает программным приложениям отслеживать свои прошлые действия. Авторы кода полагаются на этот повторяющийся код, а не изобретают колесо программного обеспечения, создавая больше программ регистрации или ведения записей для дублирования одних и тех же функций.

Ранее в этом месяце эксперты по кибербезопасности обнаружили, что, прося Log4j регистрировать строку вредоносного кода, Log4j выполняет этот код в процессе. Это дает злоумышленникам доступ к управляющим серверам, на которых работает Log4j.

Это открытие поставило почти каждую крупную софтверную компанию в режим кризиса. Они искали свои продукты, чтобы узнать, затронула ли их уязвимость Log4j, и если да, то как они могут залатать дыру.

Эта уязвимость имеет огромное значение. Log4j существует уже почти десять лет, отметила Тереза Пэйтон, бывший директор по информационным технологиям Белого дома и генеральный директор консалтинговой фирмы Fortalice Solutions по кибербезопасности.

«Думайте об этом как о своей библиотеке всего, что можно регистрировать. Мы говорим организациям [] регистрировать все, [поскольку] вам это может понадобиться позже для криминалистической экспертизы. Таким образом, Log4J часто используется разработчиками Java, когда они хотят регистрировать, что человек вошел в систему, и может даже использовать его для отслеживания доступа к приложениям», - сказала Пэйтон TechNewsWorld.

Многие компании могут даже не знать, использовали ли они Log4j, что еще больше затрудняет понимание масштабов проблемы. Она добавила, что для того, чтобы это выяснить, им понадобится инженер-программист, который изучит различные системы, чтобы найти способы использования, а затем просмотреть версии.

«Это может занять много времени, - отмечает Пэйтон, - а времени - это то, чего у вас нет, когда вы мчитесь на время против злоумышленников, стремящихся воспользоваться этими уязвимостями».

Черный ход для хакеров

Подумайте о дверном замке, который используется в различных установках оборудования безопасности в миллионах мест по всему миру. Некоторые дверные

замки имеют такую же неисправность детали, как крошечная звездочка, которая позволяет открыть замок практически любым ключом.

Заменить собственный замок - это простое решение, если вы знаете о потенциальной неисправности и имеете инструменты для выполнения работы по замене. Сделать это во всем мире - непреодолимая задача. Эта концепция делает фиаско Log4j таким угрожающим.

Log4j является частью языка программирования Java, используемого при написании программного обеспечения с середины 1990-х годов. Программное обеспечение, использующее код Log4j, повсюду управляет корпоративными и потребительскими приложениями.

Компании облачных хранилищ, которые обеспечивают цифровую основу для миллионов других приложений, также затронуты. Участвуют также крупные продавцы программного обеспечения, используемого в миллионах устройств.

Как объяснила Пэйтон, обычно при обнаружении уязвимости в системе безопасности главный специалист по информационной безопасности (CISO) берет на себя ответственность за обновление и исправление систем или вводит ручные меры по их устранению. Log4j более коварен и скрыт и не полностью контролируется CISO.

«Для поиска и обнаружения этой уязвимости требуется каждый программист. Где сейчас происходит развитие - везде! «Разработчики могут быть внутренними сотрудниками, сторонними разработчиками, сторонними разработчиками или сторонними поставщиками», - отметила она.

Все это дает хакерам неиссякаемую возможность атаковать. Конечно, не всех взломают, по крайней мере, сразу. Ключевой большой вопрос - выяснить, не обременено ли ваше оборудование проблемным кодом. Простое обнаружение приводит к перегрузке ИТ-отделов и инженеров-программистов.

«Последствия эксплуатации этой уязвимости - это мои кошмары. «Неэтичный хакер, обладающий знаниями и доступом, может использовать эту уязвимость и нацелить серверы, используя эту возможность ведения журнала с удаленным выполнением кода на серверах», - предупредила Пэйтон.

Расширение векторов атаки

Теперь хакеры полностью осведомлены об уязвимости Log4j. Охотники за кибербезопасностью сталкиваются с многочисленными случаями, когда злоумышленники расширяют возможности своих атак.

Исследовательская группа Blumira недавно обнаружила альтернативный вектор атаки в уязвимости Log4j, которая полагается на базовое соединение Javascript WebSocket для локального запуска уязвимости удаленного выполнения кода (RCE) посредством взлома. Это открытие ухудшает ситуацию с уязвимостью.

Одно из первых предположений экспертов по кибербезопасности заключалось в том, что влияние Log4j ограничивалось открытыми уязвимыми серверами. Этот недавно обнаруженный вектор атаки означает, что любой человек с уязвимой версией Log4j может быть использован через прослушивающий сервер на своем компьютере или в локальной сети, перейдя на веб-сайт и запуская уязвимость.

WebSockets ранее использовались для сканирования портов внутренних систем, но это один из первых эксплойтов удаленного выполнения кода, передаваемых WebSockets, - предложил Джейк Уильямс, соучредитель и технический директор компании BreachQuest, занимающейся реагированием на инциденты.

«Однако это не должно изменить чью-либо позицию в отношении управления уязвимостями. Организации должны стремиться к быстрому внесению исправлений и смягчению последствий, предотвращая исходящие соединения от потенциально уязвимых служб, для которых установка исправлений невозможна», - сказал он TechNewsWorld.

Хотя это и значимо, злоумышленники, скорее всего, предпочтут удаленный эксплойт, а не локальный, добавил Джон Бамбенек, главный охотник за угрозами в компании Netenrich, занимающейся цифровыми ИТ и безопасностью. При этом эта новость означает, что использование WAF или других средств защиты сети больше не является эффективным средством защиты.

«Установка исправлений остается самым важным шагом, который может предпринять организация, - сказал он TechNewsWorld.

Уязвимость Log4Shell

В отчете Блюмиры отмечается, что уязвимость Log4j, получившая название Log4Shell, уже обеспечивает относительно простой путь использования для злоумышленников. Для получения полного контроля над веб-серверами не требуется аутентификация.

Используя эту уязвимость, злоумышленники могут вызывать внешние библиотеки Java через $ {jdni: ldap: // и $ {jndi: ldaps: // и отбрасывать оболочки для развертывания атаки RCE без дополнительных усилий. По словам Блумиры, этот новый вектор атаки расширяет поверхность атаки для Log4j еще больше и может повлиять на службы, даже работающие как localhost, которые не были открыты для какой-либо сети.

«Когда была обнаружена уязвимость Log4j, быстро стало очевидно, что она может стать более серьезной проблемой. Этот вектор атаки открывает множество потенциальных случаев злонамеренного использования, от распространения вредоносных программ до создания дыр для скрытых атак , - сказал Мэтью Уорнер, технический директор и соучредитель Blumira.

«Обнародование этой информации гарантирует, что организации имеют возможность действовать быстро и защищаться от злонамеренных злоумышленников», - добавил он.

Log4j связан с Dridex, Meterpreter

Ответвление уязвимости Log4j Log4Shell - это еще один путь заражения, который недавно обнаружили исследователи при установке печально известного банковского трояна Dridex или Meterpreter на уязвимые устройства, согласно отчету Bleeping Computer.

Вредоносное ПО Dridex - это банковский троян, впервые разработанный для кражи учетных данных онлайн-банкинга. Он превратился в загрузчик, который загружает различные модули для выполнения таких задач, как установка

дополнительных полезных нагрузок, распространение на другие устройства и создание снимков экрана.

В основном используется для выполнения команд Windows, если Dridex попадает на машину, отличную от Windows, вместо этого он загружает и выполняет сценарий Python для Linux / Unix для установки Meterpreter.

Meterpreter, полезная нагрузка для атаки Metasploit, развертывается с помощью внедрения DLL в память, которая находится в памяти и ничего не записывает на диск. Он предоставляет интерактивную оболочку, которую злоумышленник использует для исследования целевой машины и выполнения кода.

Джен Истерли, директор Агентства по кибербезопасности и безопасности инфраструктуры США, заявила в недавних презентациях для СМИ, что уязвимость Log4j является самой серьезной уязвимостью, которую она видела за свою многолетнюю карьеру. Эксперты по кибербезопасности предупреждают, что уязвимость Log4j - самая большая программная дыра за всю историю с точки зрения количества открытых сервисов, сайтов и устройств». ***(Jack M. Germain. Deadly Log4j Hole Expands Victim Vulnerability // ECT News Network, Inc. (https://www.technewsworld.com/story/deadly-log4j-hole-expands-victim-vulnerability-87373.html). 28.12.2021).***

***

«Згідно з заявою, Агентство кібербезпеки та безпеки інфраструктури Міністерства внутрішньої безпеки в понеділок вдень проведе телефонну розмову із зацікавленими сторонами критичної інфраструктури щодо критичної вразливості, яка впливає на продукти з бібліотекою програмного забезпечення Log4j.

У п’ятницю CISA розіслав попередження про те, що агентство додало недолік до свого списку використаних уразливостей, і закликало федеральні та цивільні організації негайно виправити та вжити заходів для пом’якшення шкоди. Log4j — це широко використовувана утиліта ведення журналу з відкритим кодом, яка використовується в багатьох хмарних і корпоративних програмах, включаючи Minecraft, Apple iCloud, Cloudflare і Twitter, для відстеження активності програмного забезпечення. Повсюдність інструменту робить потенційну шкоду від нульового дня, ймовірно, широкомасштабною.

«CISA тісно співпрацює з нашими партнерами у державному та приватному секторах, щоб активно усунути критичну вразливість, яка впливає на продукти, що містять бібліотеку програмного забезпечення log4j», – сказала директор CISA Джен Істерлі. «Ця вразливість, якою широко користується зростаюча група загроз, становить невідкладну проблему для захисників мережі, враховуючи її широке використання».

На вихідних дослідники кібербезпеки відзначили, що кіберзлочинці намагаються скористатися перевагами нещодавно оголошеної вразливості.

«Ми активно звертаємося до організацій, чиї мережі можуть бути вразливими, і використовуємо наші інструменти сканування та виявлення вторгнень, щоб допомогти державним і галузевим партнерам виявити вплив або використання вразливості», – сказав Істерлі.

Ботнети, які запускають зловмисні операції генерації криптовалюти, почали використовувати цю вразливість, написав у неділю дослідник Sophos Шон Галлахер. З 9 грудня Sophos помітив тисячі спроб використати недолік Log4j, включаючи спроби вилучення інформації з ключів Amazon Web Services та інших приватних даних.

Дослідники порівняли серйозність уразливості до EternalBlue, який був використаний в глобальній WannaCry вимагачів атаки і 2014 ShellShock експлуатує.

У той час як більшість діяльності, які дослідники помітили досі, є злочинами з можливістю, коли злочинці сканують будь-які вразливі системи, дослідницька фірма GreyNoise помітила потенціал для більш цілеспрямованих атак. Дослідники Microsoft також помітили атаки за допомогою CobaltStrike, який можна використовувати для подальшої скомпрометації вразливих систем». ***(Tonya Riley. CISA to brief critical infrastructure companies about urgent new Log4j vulnerability // CyberScoop (https://www.cyberscoop.com/log4j-cisa-vulnerability/). 13.12.2021).***

***

«Федеральний орган охорони кібербезпеки Німеччини, BSI, у суботу оприлюднив найвище червоне попередження щодо дефектного програмного забезпечення, яке широко використовується, заявивши, що воно становить «надзвичайно критичну загрозу» для веб-серверів.

Уразливість у бібліотеці на основі Java, відомій як Log4j, може бути використана для повного захоплення ураженої системи, йдеться в заяві BSI на своєму веб-сайті.

«Причиною для цієї оцінки є дуже широке поширення продукту, на який уражений вплив, і пов'язаний з цим вплив на незліченну кількість інших продуктів. Уразливість також легко використовується, а підтвердження концепції є загальнодоступним», – повідомили в BSI.

«BSI знає про масове сканування в усьому світі та Німеччині, а також про спроби компромісу. Про початкові успішні компроміси також публічно повідомляється», – додали в ньому.

BSI сказав, що хоча було оновлення безпеки для Log4j, усі продукти, які використовують його, також необхідно адаптувати, рекомендуючи компаніям та організаціям вжити заходів, зазначених у попередженні про кібербезпеку». ***(Syndicated Content. German cybersecurity watchdog issues red alert warning on software // Midwest Communications, Inc. (https://jack1065.com/2021/12/12/german-cybersecurity-watchdog-issues-red-alert-warning-on-software/). 12.12.2021).***

***

«Log4Shell, интернет-уязвимость, поражающая миллионы компьютеров, включает малоизвестное, но почти повсеместное программное обеспечение Log4j. Программное обеспечение используется для записи всех видов деятельности, происходящей под капотом в широком диапазоне компьютерных систем.

Джен Истерли, директор Агентства по кибербезопасности и безопасности инфраструктуры США, назвала Log4Shell самой серьезной уязвимостью, которую

она видела в своей карьере. Уже были сотни тысяч, возможно, миллионы попыток использовать уязвимость.

Так что же это за скромный кусок интернет-инфраструктуры, как хакеры могут его использовать и какой хаос может последовать?

Что делает Log4j?

Log4j записывает события - ошибки и рутинные операции системы - и передает диагностические сообщения о них системным администраторам и пользователям. Это программное обеспечение с открытым исходным кодом, предоставленное Apache Software Foundation.

Типичный пример работы Log4j - это когда вы вводите или нажимаете плохую веб-ссылку и получаете сообщение об ошибке 404. Веб-сервер, на котором запущен домен веб-ссылки, на которую вы пытались перейти, сообщает вам, что такой веб-страницы нет. Он также записывает это событие в журнал для системных администраторов сервера, использующих Log4j.

Подобные диагностические сообщения используются во всех программных приложениях. Например, в онлайн-игре Minecraft Log4j используется сервером для регистрации таких действий, как общий объем используемой памяти и пользовательские команды, введенные в консоль.

Как работает Log4Shell?

Log4Shell работает, злоупотребляя функцией Log4j, которая позволяет пользователям указывать собственный код для форматирования сообщения журнала. Эта функция позволяет Log4j, например, регистрировать не только имя пользователя, связанное с каждой попыткой входа на сервер, но и настоящее имя человека, если отдельный сервер содержит каталог, связывающий имена пользователей и настоящие имена. Для этого сервер Log4j должен связаться с сервером, на котором хранятся настоящие имена.

К сожалению, такой код можно использовать не только для форматирования сообщений журнала. Log4j позволяет сторонним серверам отправлять программный код, который может выполнять все виды действий на целевом компьютере. Это открывает дверь для гнусных действий, таких как кража конфиденциальной информации, получение контроля над целевой системой и передача вредоносного контента другим пользователям, которые общаются с затронутым сервером.

Использовать Log4Shell относительно просто. Мне удалось воспроизвести проблему в моей копии Ghidra, фреймворка обратного проектирования для исследователей безопасности, всего за пару минут. Уровень использования этого эксплойта очень низкий, что означает, что его может использовать более широкий круг людей со злым умыслом.

Log4j везде

Одна из основных проблем Log4Shell - это положение Log4j в экосистеме программного обеспечения. Ведение журнала - это фундаментальная функция большинства программ, которая делает Log4j очень широко распространенным. Помимо популярных игр, таких как Minecraft, он используется в облачных сервисах, таких как Apple iCloud и Amazon Web Services, а также в широком

спектре программ, от инструментов разработки программного обеспечения до инструментов безопасности.

Это означает, что у хакеров есть большое меню целей на выбор: домашние пользователи, поставщики услуг, разработчики исходного кода и даже исследователи безопасности. Таким образом, в то время как крупные компании, такие как Amazon, могут быстро исправлять свои веб-сервисы, чтобы предотвратить их использование хакерами, существует гораздо больше организаций, которым требуется больше времени для исправления своих систем, а некоторые могут даже не знать, что им это нужно.

Ущерб, который можно нанести

Хакеры сканируют Интернет в поисках уязвимых серверов и настраивают машины, которые могут доставлять вредоносные данные. Для проведения атаки они запрашивают службы (например, веб-серверы) и пытаются вызвать сообщение журнала (например, ошибку 404). Запрос включает вредоносный текст, который Log4j обрабатывает как инструкции.

Эти инструкции могут создать обратную оболочку, которая позволяет атакующему серверу удаленно управлять целевым сервером, или они могут сделать целевой сервер частью ботнета. Ботнеты используют несколько захваченных компьютеров для выполнения скоординированных действий от имени хакеров.

Большое количество хакеров уже пытаются злоупотребить Log4Shell. Они варьируются от банд вымогателей, блокирующих серверы Minecraft, до хакерских групп, пытающихся добыть биткойны, и хакеров, связанных с Китаем и Северной Кореей, пытающихся получить доступ к конфиденциальной информации от своих геополитических соперников. Министерство обороны Бельгии сообщило, что его компьютеры подвергались атаке с использованием Log4Shell.

Хотя уязвимость впервые привлекла всеобщее внимание 10 декабря 2021 года, люди все еще находят новые способы причинения вреда с помощью этого механизма.

Остановка кровотечения

Трудно узнать, используется ли Log4j в какой-либо конкретной программной системе, потому что он часто входит в состав другого программного обеспечения. Для этого системные администраторы должны провести инвентаризацию своего программного обеспечения, чтобы определить его присутствие. Если некоторые люди даже не знают, что у них есть проблема, гораздо труднее искоренить уязвимость.

Еще одним следствием разнообразного использования Log4j является отсутствие универсального решения для его исправления. В зависимости от того, как Log4j был включен в данную систему, исправление потребует разных подходов. Для этого может потребоваться полное обновление системы, как это делается для некоторых маршрутизаторов Cisco, или обновление до новой версии программного обеспечения, как это делается в Minecraft, или удаление уязвимого кода вручную для тех, кто не может обновить программное обеспечение.

Log4Shell является частью цепочки поставок программного обеспечения. Подобно физическим объектам, которые люди покупают, программное обеспечение проходит через различные организации и программные пакеты,

прежде чем превратиться в конечный продукт. Когда что-то идет не так, вместо того, чтобы проходить процесс отзыва, программное обеспечение обычно «исправляется», то есть фиксируется на месте.

Однако, учитывая, что Log4j по-разному присутствует в программных продуктах, распространение исправления требует координации со стороны разработчиков Log4j, разработчиков программного обеспечения, использующего Log4j, дистрибьюторов программного обеспечения, системных операторов и пользователей. Обычно это приводит к задержке между тем, как исправление становится доступным в коде Log4j, и тем, что компьютеры людей фактически закрывают дверь для уязвимости.

По некоторым оценкам, время ремонта программного обеспечения обычно составляет от недель до месяцев. Однако, если поведение в прошлом указывает на производительность в будущем, вполне вероятно, что уязвимость Log4j возникнет еще долгие годы.

Как пользователь, вы, вероятно, задаетесь вопросом, что вы можете со всем этим поделать. К сожалению, трудно узнать, включает ли используемый вами программный продукт Log4j и используются ли в нем уязвимые версии программного обеспечения. Однако вы можете помочь, прислушиваясь к общему правилу экспертов по компьютерной безопасности: убедитесь, что все ваше программное обеспечение обновлено». ***(Santiago Torres-Arias. What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake // Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/404171). 22.12.2021).***

***

«Оскільки вразливість Log4j продовжує привертати увагу, нова вразливість нульового дня, знайдена в широко використовуваному уніфікованому інструменті керування кінцевими точками Zoho Corp., ManageEngine Desktop Central, яка тепер відстежується як CVE-2021-44515, активно використовується національними державами. актори в дикій природі, за даними ФБР.

Уразливість обходу аутентифікації, яка має критичну оцінку 9,8 з 10, дає розширеним постійним загрозам можливість скомпрометувати сервери, скинути веб-оболонку, яка перевизначає законні функції програмного забезпечення, і скидати облікові дані, повідомляє ФБР.

Агентство каже, що атаки через цю вразливість відбуваються щонайменше з жовтня.

За даними ФБР, зловмисники використовували URL-адресу API «/fos/statuscheck» для надсилання запитів із зовнішніх IP-адрес, законної, але рідко використовуваної функції Desktop Central. Зазвичай зв’язок здійснюється лише з інших серверів Desktop Central. ФБР радить розслідувати будь-які запити, надіслані від зовнішніх користувачів у період з жовтня по грудень 2021 року, оскільки вони є ознакою компромісу.

Інші тактики, прийоми та процедури, викладені ФБР і використовувані національними державами для використання цієї вразливості, включають:

Бібліотека динамічних посилань, або DLL, бічне завантаження;

Сканування мережі;

Вставлення команд за допомогою Microsoft PowerShell;

Завантаження інструментів після експлуатації;

Створення збереження бекдору через Windows;

Демпінг акредитації.

«Організації, які виявляють будь-яку діяльність, пов'язану з цими МОК у своїх мережах, повинні негайно вжити заходів», – стверджує ФБР. Він також заохочує організації повідомляти про випадки, пов'язані з уразливістю, до правоохоронних органів.

Агентство кібербезпеки та безпеки інфраструктури США додало цю вразливість до свого Каталогу відомих використаних уразливостей на початку грудня та призначило дату усунення на п'ятницю.

«Звичайна мішень»

Zoho Corp. - індійська компанія, яка розробляє веб-інструменти для бізнесу - має історію стати жертвою зловмисників, а звіти починаються з 2020 року. Методи, використані в CVE-2021-44515, подібні до тих, які застосовувала китайська хакерська група. APT27, повідомляє Bleeping Computer.

У вересні ФБР, CISA і берегова охорона США опублікували спільну заяву, в якій повідомляли про ще одну критичну вразливість у продуктах Zoho. У цьому випадку національні держави використовували вразливість автентифікації обходу, яка відстежується як CVE-2021-40539, щоб успішно запускати кампанії атак.

Австралійський центр кібербезпеки повідомив про подібні висновки щодо програмного недоліку Zoho.

Zoho Corp. уповноважує близько 180 000 IT-команд по всьому світу, включаючи оборонних підрядників для федерального уряду, таких як Raytheon, Boeing і Northrup Grumman. Компанія також надає спеціальні збірки програмного забезпечення для ВМС США і Корпусу морської піхоти, згідно з її офіційним веб-сайтом.

Карім Хіджазі, генеральний директор компанії Prevailion, яка займається розвідкою кіберзагроз, каже ISMG: «Zoho ManageEngine був звичайною мішенню для APT». Він каже, що ManageEngine Desktop Central дозволяє керувати та контролювати комп'ютерні мережі, а також віддалений доступ до комп'ютерних мереж, і саме тому він особливо вразливий до APT.

Еволюція Zoho Flaw

Деякі експерти прогнозують, що ця вада, якщо її не усунути, може стати шлюзом до іншої атаки ланцюга поставок із потенціалом SolarWinds або Kaseya. Обидва американські розробники програмного забезпечення стали жертвами сумнозвісних пов'язаних з Росією груп програм-вимагачів - Nobelium і REvil відповідно.

SolarWinds і Kaseya відрізняються кількістю жертв, включаючи п'ять урядових установ США, великі технологічні організації та критичну інфраструктуру. Зокрема, багато хто вважає SolarWinds найгіршою кібератакою на сьогоднішній день (див.: Звернення до ланцюга постачання SolarWinds: жертви включають Cisco, Intel).

Недолік Zoho міг навіть рухатися за траєкторією, подібною до Log4j.

«У руках суб'єкта загрози це являє собою ідеальну можливість бічного переміщення «один до багатьох», — каже Хіджазі. Він прогнозує, що можливість розгортання веб-оболонок після початкової експлуатації може стати «грандіозною проблемою, подібною до вектора, який спостерігається у Log4j2».

Інші експерти погоджуються, що ця вразливість може завдати шкоди.

Кріс Пірсон, колишній член Комітету з кібербезпеки Міністерства внутрішньої безпеки США, каже, що як тільки противник закріпиться в навколишньому середовищі, він може відмовитися від інструментів, які дозволяють більш експлуатувати, орієнтуватися в бік по системах компанії, знайти спосіб досягти успіху. постійна наполегливість і в кінцевому підсумку вилучення інформації та даних.

А Ренді Паргман, який раніше працював у кібер-оперативній групі ФБР у Сіетлі, каже, що учасники, які використовують цю вразливість, будуть використовувати її «для крадіжки конфіденційних документів або запуску програм-вимагачів, або того й іншого», доки організації не виправлять уражене програмне забезпечення.

«Управління великим парком настільних і мобільних пристроїв є звичайною потребою бізнесу, тому це, ймовірно, торкнеться багатьох секторів», — каже Паргман, віце-президент із пошуку загроз і контррозвідки в фірмі Binary Defense.

Ефективне пом'якшення

ФБР опублікувало стратегії виявлення та рекомендації щодо зменшення ризиків уразливості Desktop Central із покроковими інструкціями щодо виконання плану реагування на інциденти Zoho.

Zoho викладає план реагування на інцидент у п'ять кроків:

Відключіть заражену систему від мережі.

Створіть резервну копію бази даних Desktop Central.

Відформатуйте зламану машину після створення резервної копії критичних даних.

Відновіть Desktop Central за допомогою версії збірки з резервної бази даних на кроці 2.

Повне оновлення програмного забезпечення для відповідної версії

Zoho також рекомендує завершити скидання пароля для всіх користувачів, які мали доступ до інфікованого пристрою, включаючи паролі адміністратора.

Пірсон, який наразі є генеральним директором фірми з кібербезпеки BlackCloak, каже, що під час оновлення до останньої версії ManageEngine організації повинні обмежити внутрішній доступ до систем, які повинні спілкуватися зі зламаними пристроями, перш ніж почати практику пошуку внутрішніх загроз.

Фахівці з питань безпеки можуть почати з перевірки останньої версії Desktop Central, переконатися, що останні виправлення встановлені, а потім уважно подивитися на виправлені сервери, щоб визначити, чи були вони атаковані, каже Паргман.

Окрім виконання вказівок ФБР, він також рекомендує рекомендувати групам безпеки використовувати журнали подій та інструмент виявлення кінцевої точки та

відповіді, або EDR, інструмент, підключений до центрального сервера, де зловмисник не може видалити журнали.

Hijazi рекомендує завантажити інструмент виявлення експлойтів ManageEngine». ***(Devon Warren-Kachelein. Nation-States Exploiting Critical Flaw in Zoho UEM // Information Security Media Group, Corp. (https://www.govinfosecurity.com/nation-states-exploiting-critical-flaw-in-zoho-uem-a-18178). 22.12.2021).***

***

«Необхідність пошуку та виправлення всіх випадків уразливості в широко використовуваному програмному забезпеченні Apache продовжує зростати.

Експерти з кібербезпеки попереджають, що низка зловмисників, пов'язаних із національними державами, здається, активно зловживають або тестують уразливість Apache Log4j. Деякі експерти попереджають, що злочинні угруповання також почали націлюватися на помилку, щоб скинути шкідливий код, включаючи зловмисне програмне забезпечення, що блокує криптовалюту, а відомі брокери доступу використовують цей недолік для збору облікових даних корпоративного доступу для продажу іншим зловмисникам, у тому числі групам програм-вимагачів.

Підтримується некомерційною організацією Apache Software Foundation, Log4j надає можливості ведення журналів для програм Java і широко використовується, в тому числі для програмного забезпечення веб-сервера Apache. Багаторічна помилка присутня в бібліотеці Apache Log4j, версії 2.0-beta9 до 2.14.1, і Агентство з кібербезпеки та безпеки інфраструктури США заявило, що організації повинні ставитися до її виправлення найвищим пріоритетом.

У четвер Джон Грем-Каммінг, технічний директор постачальника веб-інфраструктури Cloudflare, заявив, що компанія відстежує понад 100 000 спроб сканування або використання Log4j за хвилину.

Уразливість, позначена як CVE-2021-44228, «існує у дії, яку виконує інтерфейс імен і каталогів Java - JNDI, щоб розв'язати змінні», - говорить CISA. «Уражені версії Log4j містять функції JNDI, такі як підстановка пошуку повідомлень, які «не захищають від контрольованого зловмисником легкого протоколу доступу до каталогів – LDAP – та інших кінцевих точок, пов'язаних з JNDI»,», – йдеться в відомостях про вразливості уряду США.

Агентство ЄС з кібербезпеки, ENISA, каже, що «через характер уразливості, її повсюдність і складність виправлення в деяких середовищах, які постраждали», всім організаціям важливо «оцінити їх потенційний ризик якомога швидше».

Але неясно, коли це стане можливим, каже технічний директор Mandiant Чарльз Кармакал. «Організаціям дається проблема з визначенням усіх уразливих екземплярів Log4j на своєму підприємстві. Виправлення не є тривіальним. Багато постачальників все ще визначають, чи використовує їхнє програмне забезпечення Log4j, оскільки організації з нетерпінням чекають, чи варто застосовувати екстрені виправлення», - каже він. «Закриті системи, системи, керовані постачальниками, і

програмне забезпечення, яке більше не обслуговується, але все ще працює в тестовому або навіть виробничому середовищі, додає складності та болю».

Напади на національні держави

Спонукання пом’якшити недолік і якнайшвидше застосувати виправлення зростало після того, як на цьому тижні фірми з кібербезпеки CrowdStrike і Mandiant попередили, що китайські та іранські групи APT націлені на вразливість CVE-2021-44228.

У середу Microsoft повідомила, що бачила активну активність APT, відстежуючи не лише Китай та Іран, а й зловмисників, пов’язаних із Північною Кореєю та Туреччиною.

«Ця діяльність варіюється від експериментів під час розробки, інтеграції вразливості до розгортання корисного навантаження в умовах дикої природи та використання проти цілей для досягнення цілей актора», — говорить Microsoft.

Наприклад, Microsoft каже, що бачила іранську групу APT, відому як Charming Kitten, Phosphorus і TA453, яка «придбала та вносила модифікації експлойту Log4j», і вона вважає, що група тепер може використовувати код атаки для атак у дикій природі.

Microsoft також стверджує, що бачив іранську APT групу, відому як гафній, інакше APT31 і APT40, використовуючи експлойт для визначення нових цілей. Група була пов’язана з серією атак нульового дня на сервери Exchange на початку цього року, запущених через орендовані віртуальні приватні сервери переважно в США.

Під час останніх атак «системи, пов'язані з гафнієм, спостерігалися за допомогою служби DNS» - або пошуку доменних імен – «служби, зазвичай пов'язаної з тестуванням систем відбитків пальців», - каже Microsoft.

Кримінальна діяльність

Злочинці також намагалися розгорнути зловмисне програмне забезпечення в системах Linux, а також програмне забезпечення.NET під назвою Khonsari на кінцевих точках Windows, як детально розповіла фірма безпеки Bitdefender.

Зловмисники також атакували сервери Minecraft, які не керуються Microsoft, попереджають дослідники безпеки компанії, кажучи, що метою атак є не просто розгортання програм-вимагачів Khonsari на серверах, а й збір облікових даних для подальшого використання.

«Хоча Minecraft нерідко встановлюють у корпоративних мережах, ми також спостерігали, як зворотні оболонки на основі PowerShell передаються клієнтським системам Minecraft за допомогою тієї ж методики шкідливих повідомлень, надаючи акторові повний доступ до скомпрометованої системи, яку вони потім використовують для запустіть Mimikatz, щоб вкрасти облікові дані», - йдеться в ньому. «Ці методи зазвичай пов'язані з компромісами підприємства з метою бічного переміщення. На даний момент Microsoft не спостерігала жодної подальшої діяльності цієї кампанії, що вказує на те, що зловмисник може отримати доступ для подальшого використання».

Відомі брокери початкового доступу також намагалися отримати доступ до корпоративних мереж. «Ці брокери доступу потім продають доступ до цих мереж філіям-вимагальникам як послуга» та іншим, каже Microsoft.

Інструкція: оновлення до 2.16

Щоб виправити недолік, Apache у п'ятницю випустив Log4j версії 2.15.0. Але в понеділок Apache випустив Log4j версії 2.16, яка включає виправлення нещодавно знайденого недоліку, CVE-2021-45046, який можна використовувати для створення атаки відмови в обслуговуванні.

Експерти рекомендують організаціям спочатку застосувати виправлення версії 2.16.0 до всього, що ще не було оновлено до 2.15.0, а потім оновити всі системи версії 2.15 до 2.16.

«Ми вживаємо невідкладних заходів для пом'якшення цієї вразливості та виявлення будь-якої пов'язаної загрози», – сказала директор CISA Джен Істерлі.

CISA додала CVE-2021-44228 до свого списку відомих уразливостей. Це «примушує федеральні цивільні агенції - і сигналізує нефедеральним партнерам - терміново виправити або усунути цю вразливість», - сказав Істерлі.

«Ми активно звертаємося до організацій, чиї мережі можуть бути вразливими, і використовуємо наші інструменти сканування та виявлення вторгнень, щоб допомогти державним і галузевим партнерам виявити вплив або використання вразливості», – сказала вона.

CISA закликала будь-яку американську організацію, яка зазнала атаки Log4j, негайно повідомити про інцидент CISA або ФБР.

Крім того, CISA продовжує пропонувати оновлені вказівки щодо вразливості Apache Log4j і веде список програмного забезпечення, яке, як відомо, постраждало, а також програмного забезпечення, яке наразі не зачепило, який наразі містить понад 750 записів.

Обов'язкове значення: швидке пом'якшення та виправлення

CISA надала федеральним цивільним органам виконавчої влади жорсткий термін для виправлення вразливості CVE-2021-44228: 24 грудня. Він також закликав їх негайно розгорнути брандмауери веб-додатків, щоб блокувати спроби атаки та подавати сигнали тривоги центру безпеки у разі таких атак. потрапити в мережу.

Численні постачальники та проекти з розробки програмного забезпечення, які використовують це програмне забезпечення, ще не визначили, чи є їхні інструменти вразливими, і підготували виправлення. Перш ніж застосовувати будь-які виправлення, експерти кажуть, що організації повинні вважати, що зловмисники вже використали недолік проти них, поки не буде доведено протилежне. «Виправлення не усуває існуючий компроміс», — каже Джейк Вільямс, технічний директор компанії BreachQuest з кібербезпеки.

У зв'язку з повсюдним поширенням вади та потребою в оновленні великої кількості різних програм, Джон Халтквіст, віце-президент Mandiant з аналізу розвідувальних даних, очікує, що вплив цього недоліку буде відчуватися деякий час. Він каже: «Наслідки цієї вразливості будуть відображатися протягом наступних місяців — можливо, навіть років, — коли ми намагатимемося закрити ці двері та намагатися вистежити всіх акторів, які проникли всередину». ***(Mathew J. Schwartz. Nation-State Attackers Wielding Log4j Against Targets // Information Security Media Group, Corp. (https://www.govinfosecurity.com/nation-state-attackers-wielding-log4j-against-targets-a-18138). 16.12.2021).***

***

«Через тиждень після оголошення нової програми винагороди за помилки під назвою «Hack DHS», призначеної для захисту систем федерального агентства, міністр внутрішньої безпеки США Алехандро Майоркас оголосив, що DHS розширює сферу дії програми, щоб включати пошук і виправлення вразливостей, пов'язаних з Log4j. в системах.

Планується, що програма винагороди за помилки Hack DHS матиме поетапне впровадження, яке розтягнеться на весь 2022 фінансовий рік і незабаром буде прийнято на різних рівнях уряду…

У твіті директор CISA Джен Істерлі привітала цей крок і подякувала світовій дослідницькій спільноті за участь у програмі, тим більше, що вразливість Apache Log4j тепер є загрозою глобального рівня.

Під час прес-брифінгу 14 грудня помічник виконавчого директора CISA з кібербезпеки Ерік Голдштейн заявив, що на сьогоднішній день не було підтверджено компромісів з боку будь-яких федеральних агенцій через Log4j, але він назвав ситуацію «надзвичайно тривожною», як повідомляє Federal. Мережа новин.

Навіщо включати Log4j?

Повідомлення про те, що Log4j буде включено в програму винагороди за помилки, з'явилося після повідомлення про те, що Міністерство оборони Бельгії стало жертвою кібератаки, яка була пов'язана з використанням широко поширеної вразливості Apache Log4j. У міністерстві підтвердили, що уражені системи були ізольовані, але не розкрили жодної інформації про зловмисника чи тип кібератаки.

У звітах стверджується, що учасники національних держав із потенційно ворожих країн, таких як Китай, Іран, Північна Корея та Туреччина, також намагаються отримати максимальну вигоду від уразливості Apache Log4j, і, схоже, вони активно намагалися зловживати нею, за словами експертів з кібербезпеки.

Відповідний підхід

Деякі експерти бачать використання винагород за помилки для виявлення недоліків Log4j як відповідний підхід. Кріс Клементс, віце-президент з архітектури рішень фірми безпеки Cerberus Sentinel, каже Information Security Media Group, що вразливості Log4j є шкідливими, оскільки «їх важко виявити за допомогою традиційних сканерів уразливостей, вони вбудовані в численні програми, яких ви могли б не очікувати, і впливають на системи. і неочевидні програми після первинних операційних потоків».

Він каже, що найефективніша форма виявлення вимагає сканування всіх файлів у системах для пошуку вразливих версій бібліотеки Log4j. Хоча існує багато інструментів з відкритим кодом для цього, каже він, багатьом організаціям може бути важко зробити це в масштабі.

«Усі ці фактори роблять ці вразливості тими, що мають величезну вигоду від наявності більшої кількості очей для пошуку потенційних уразливих систем. Програми винагороди за помилки можуть бути особливо ефективними для привернення саме такого обсягу перевірки, створюючи ефективний цикл, узгоджуючи стимули між організаціями та зовнішніми дослідниками безпеки. », -

каже Клементс. Але він попереджає, що виявлення – це лише перший крок, і каже, що організації повинні створити плани пом'якшення та відновлення, щоб гарантувати, що вони захищені від атак через ці вектори.

За словами Джеймса МакКвіґгана, захисника поінформованості про безпеку в KnowBe4 і директора з освіти Флоридського кібер-альянсу, особливою перевагою цього підходу є усунення потреби в ресурсах. «Використання експертів у суспільстві полегшує необхідність наймати, включати і просто використовувати [співробітників] як «витягнутих» підрядників з одноразовою оплатою», — каже він.

Сканер Log4j, рекомендований CISA

Згідно з твітом CISA, CISA опублікувала на GitHub сканер Log4j з відкритим кодом, який був побудований на основі кількох сканерів, створених членами спільноти з відкритим кодом.

«Цей репозиторій надає рішення для сканування вразливостей віддаленого виконання коду Log4j (CVE-2021-44228 і CVE-2021-45046)», — йдеться у дописі GitHub. Там сказано, що інформація та код у сховищі надаються «як є» і були зібрані за допомогою спільноти з відкритим кодом та оновлені CISA у співпраці з більш широким співтовариством кібербезпеки.

CISA приписує рішення для сканування кільком дослідникам. Мазін Ахмед — одне з імен, яке з'являється в розділі кредитів публікації GitHub. Ахмед є засновником стартапу з кібербезпеки FullHunt.

13 грудня FullHunt випустив сканер виявлення єдиної відомої на той час уразливості Apache Log4j RCE, яка відстежується як CVE-2021-4428.

CISA у своїй публікації на GitHub говорить, що вона «трохи змінила» цей сканер з відкритим кодом і використала «два додаткові проекти, щоб уникнути використання сторонніх розробників».

FullHunt ще не відповів на запит ISMG щодо інформації про ці модифікації». ***(Mihir Bagwe. 'Hack DHS' Program Expanded to Include Log4j Bug Hunters // Information Security Media Group, Corp. (https://www.govinfosecurity.com/hack-dhs-program-expanded-to-include-log4j-bug-hunters-a-18175). 22.12.2021).***

***

«Агентство кібербезпеки та безпеки інфраструктури (CISA), а також Федеральне бюро розслідувань (ФБР), Агентство національної безпеки (NSA), Австралійський центр кібербезпеки (ACSC), Канадський центр кібербезпеки (CCCS), команда реагування на надзвичайні комп'ютерні Зеландія (CERT NZ), Національний центр кібербезпеки Нової Зеландії (NZ NCSC) і Національний центр кібербезпеки Сполученого Королівства (NCSC-UK) опублікували спільні рекомендації щодо кібербезпеки з технічними деталями, пом'якшеннями наслідків та ресурсами для усунення відомих уразливостей у Apache. Бібліотека програмного забезпечення Log4j. Ця рекомендація містить важливі рекомендації, які будь-яка організація, яка використовує продукти з Log4j, повинна негайно запровадити.

Спільна рекомендація є відповіддю на активну всесвітню експлуатацію численними загрозами, включаючи зловмисних кіберзагроз, уразливостей,

виявлених у широко використовуваному пакеті журналів Log4j на базі Java. CISA, ФБР, АНБ та наші міжнародні агенції-партнери працювали з організаціями в державному та приватному секторах з моменту виявлення першої вразливості, щоб виявити вразливі продукти, підвищити обізнаність та заохотити всі потенційно постраждалі організації вжити негайних заходів.

«Уразливі місця Log4j представляють серйозну і постійну загрозу організаціям та урядам у всьому світі; ми закликаємо всі організації вжити негайних заходів для впровадження останніх рекомендацій щодо пом'якшення наслідків для захисту своїх мереж», – сказала директор CISA Джен Істерлі. «CISA співпрацює пліч-о-пліч з нашими міжвідомчими, приватним сектором та міжнародними партнерами, щоб зрозуміти серйозні ризики, пов'язані з вразливими місцями Log4j, і надати необхідну інформацію для всіх організацій, щоб якнайшвидше вжити відповідних заходів. Ці вразливості є найсерйознішими, які я бачив у своїй кар'єрі, і дуже важливо, щоб ми працювали разом, щоб захистити наші мережі».

«ФБР продовжує працювати разом із нашими федеральними та міжнародними партнерами, щоб пом'якшити шкідливу кіберактивність та озброїти державний та приватний сектори інформацією, щоб краще захистити їхні системи», – сказав помічник директора кібервідділу ФБР Браян Ворндран. «Ми продовжуємо закликати всіх, хто постраждав від уразливості Log4j, застосувати всі рекомендовані від CISA заходи пом'якшення та відвідати fbi.gov/log4j, щоб повідомити деталі вашого підозрюваного компромісу».

«Партнерство з метою чіткого визначення проблеми та способів її пом'якшення має вирішальне значення для того, щоб уникнути шуму та надати відповідну інформацію для дій», – сказав директор з кібербезпеки АНБ Роб Джойс. «Враховуючи серйозність уразливостей Log4j та ймовірність посилення експлуатації, ми наполегливо закликаємо організації застосовувати заходи пом'якшення, рекомендовані в наших спільних рекомендаціях щодо кібербезпеки».

«Зловмисники в кіберпрограмі вже сканують та експлуатують деякі з багатьох тисяч уразливих систем у всьому світі. Щоб подолати цю загрозу, ми всі повинні бути активними в наших зусиллях щодо виправлення, партнерства та моніторингу», — сказала виконуюча обов'язки керівника Австралійського центру кібербезпеки пані Джессіка Хантер. «Ця спільна консультація підкреслює цінність такого підходу. ACSC разом з нашими партнерами з CISA, ФБР, АНБ, CCCS, CERT-NZ, NZ NCSC і NCSC-UK залишаються відданими розвитку кібербезпеки».

«Вразливості, пов'язані з Log4, становлять серйозний ризик для організацій у всьому світі», – сказав Самі Хурі, керівник Канадського центру кібербезпеки. «Приєднавшись разом із нашими партнерами до випуску сьогоднішньої спільної консультації, Управління безпеки зв'язку та його Канадський центр кібербезпеки раді продовжувати робити інформацію про загрози більш загальнодоступною, надаючи конкретні поради та рекомендації щодо захисту від таких видів ризиків».

«Вкрай важливо, щоб організації в терміновому порядку виправляли програмне забезпечення та продовжували слідувати опублікованим порадам», – сказав директор з операцій NCSC Пол Чічестер. «Це значна вразливість, і ми

будемо тісно співпрацювати з нашими міжнародними партнерами, щоб мінімізувати ризики та пом'якшити будь-який вплив».

«Ми не можемо підкреслити, наскільки важливо для всіх якнайшвидше виправити цю вразливість», — сказав директор CERT NZ Роб Поуп. «Ми знаємо, що зловмисники постійно шукають доступ до систем по всьому світу, використовуючи вразливість Log4j. Лише за допомогою колективних дій ми можемо ефективно протистояти цим видам атак, тому ми пишаємося тим, що є частиною міжнародних зусиль, спрямованих на забезпечення безпеки організацій».

CISA створила спеціальну веб-сторінку Log4J, щоб надати авторитетний, сучасний ресурс із рекомендаціями щодо пом'якшення наслідків та ресурсами для мережевих захисників, а також сховище GitHub із джерелами спільноти пристроїв і служб, які постраждали. Керівники організацій повинні також переглянути допис у блозі NCSC «Вразливість Log4j: що повинні запитувати ради?», щоб отримати інформацію про можливий вплив Log4Shell на їхню організацію, а також рекомендації щодо відповіді.

Кожному керівнику та керівнику настійно рекомендується переконатися, що їхній бізнес, організація чи державна установа вживають відповідних заходів для пом'якшення цих уразливостей Log4j. Ця спільна консультація також надає цінні ресурси, щоб допомогти організаціям у подальшому зміцнити свій захист і стійкість до цих вразливостей, а також інших кіберзагроз.» ***(CISA, FBI, NSA, and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-fbi-nsa-and-international-partners-issue-advisory-to-mitigate-apache-log4j-vulnerabilities/). 22.12.2021).***

***

«Взлом просто означает проникновение в чужую систему и кражу их данных без их разрешения. Однако есть и другие виды взлома, которые носят более позитивный характер, и их называют этичным взломом. Этический взлом - это термин, обозначающий процедуру обнаружения лазеек безопасности в инфраструктуре и системе компании.

Организации довольно часто используют этический взлом. Они получают эту легально взломанную систему, когда им нужно предотвратить кибератаки и нарушения безопасности в своей системе на платформе HackerOne.

HackerOne - это платформа, объединяющая компании со специалистами по кибербезопасности и специалистами по поиску ошибок. Каждый год HackerOne делится своим отчетом о безопасности из внутреннего мира этического взлома крупнейшей в мире базы данных уязвимостей, и в этом году в 2021 году этические хакеры обнаружили на 20% больше уязвимостей по сравнению с 2020 годом.

Их последний отчет об этическом взломе также указывает на обнадеживающую тенденцию к повышению осведомленности организаций о кибербезопасности, поскольку все больше компаний, похоже, уделяют особое внимание управлению уязвимостями.

В текущем году этический хакер обнаружил более 66 500 точных уязвимостей в отчете по безопасности HackerOne за 2021 год.

Это на 264% больше ошибок по сравнению с прошлым годом (из года в год) по результатам теста на проникновение. Тест на проникновение - это своего рода тест безопасности, в ходе которого компания нанимает квалифицированных этичных хакеров, чтобы узнать силу ее кибербезопасности.

В то же время программа раскрытия уязвимостей зафиксировала рост уязвимостей на 47%.

Десять основных уязвимостей также входит в отчет HackerOne, обнаруженный на платформе.

Перекрестные сценарии находятся в верхней части списка уязвимостей, за ними следует раскрытие информации, а третье место в списке занимает ненадлежащий контроль доступа.

Когда дело доходит до признания этичных хакеров, многие организации предлагают этим людям отличные предложения от 250 до 3000 долларов или даже 15000 долларов, в зависимости от строгости обнаруженных ошибок, в 2021 году можно увидеть значительное увеличение этих вознаграждений». ***(Arooj Ahmed. HackerOne releases its ethical hacking security report for the year 2021 // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/hackerone-releases-its-ethical-hacking.html). 13.12.2021).***

***

«Кибератаки развиваются день ото дня. Недавно группа исследователей обнаружила новую угрозу, которая может использовать общие данные из Wi-Fi и других частей Bluetooth.

Знаменитая платформа новостей о кибербезопасности Bleeping Computer была первой, кто покрыл эту уязвимость. Выводы, связанные с этими атаками, были распространены в двух университетах, а именно в Университете Брешии и Университете Дармштадта. По словам исследователей, Bluetooth способен отвлекать трафик Wi-Fi при сборе сетевых паролей. Причина этого в том, что и Bluetooth, и Wi-Fi имеют одни и те же вещи, например антенну.

Чтобы узнать больше об этой уязвимости, было установлено 9 общих уязвимостей и уязвимостей, вскоре известных как CVE. Исследовательский комитет уведомил производителей устройств, используемых в качестве мишеней, а также группу особого интереса к Bluetooth.

Единственное, что нужно сделать злоумышленнику, чтобы использовать такие уязвимости против других устройств, - это взломать только одну беспроводную цепь. Этот шаг позволит хакерам получить в свои руки код для WiFi, как только кремниевый чип Bluetooth будет полностью взломан.

Такие атаки невозможно остановить, это связано с тем, что такие микросхемы подключаются через жесткий проводной интерфейс, в результате обработчик операционной системы не может остановить их. Хотя об этой уязвимости сообщили 2 года назад, она все еще остается уязвимой для атак.

Однако эти удары были более эффективны против предыдущих версий iOS 14.7 и Android 11, которые теперь заменены на iOS 15 и Android 12 соответственно. Другие устройства также использовались, чтобы больше узнать об угрозе.

Исследовательская группа также поделилась результатами, полученными с других устройств.

Исследовательская группа добавила, что, несмотря на то, что властям сообщается об угрозе, такие меры не принимаются, чтобы предотвратить ее возникновение, вместо этого они внесли лишь незначительные изменения, потому что для устранения уязвимости эти чипы потребуются для отремонтировать с нуля». ***(Arooj Ahmed. Wi-Fi and Bluetooth chips could be under attack according to researchers // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/wi-fi-and-bluetooth-chips-could-be.html). 15.12.2021).***

***

«Китайські ЗМІ повідомляють, що Alibaba Cloud стикається з реакцією урядових регуляторів після того, як вони повідомили про вразливість Log4J для Apache перед Міністерством промисловості та інформаційних технологій (МІІТ).

21st Century Business Herald повідомила, що в середу місцевих репортерів поінформували про те, що Адміністрація кібербезпеки МІІТ призупиняє своє партнерство з обміном інформацією з Alibaba Cloud на шість місяців, зокрема посилаючись на те, що причиною цього не було повідомлення про Log4J.

Чен Чжаоцзюнь, інженер з безпеки Alibaba Cloud, був визначений Bloomberg News як перша людина, яка виявила вразливість Log4J і повідомила про це Apache. Чжаоцзюнь повідомив Apache 24 листопада, а третя сторона пізніше повідомила МІІТ у звіті 9 грудня, повідомляє Reuters.

«Нещодавно, виявивши серйозні вразливості безпеки в компоненті Apache Log4j2, Alibaba Cloud не змогла своєчасно звітувати до органів телекомунікацій та не надала ефективно підтримку Міністерству промисловості та інформаційних технологій у здійсненні загроз кібербезпеці та управління вразливістю», повідомляють місцеві ЗМІ.

Останніми місяцями уряд Китаю намагався краще впоратися з кібербезпекою та конфіденційністю, прийнявши кілька законів і попередивши великі компанії про необхідність захисту даних, що передаються за межами Китаю.

На Alibaba було накладено рекордний штраф у 18,2 мільярда юанів, а 33 інші мобільні додатки зазнали критики з боку Пекіна за політику збору даних. Діді пройшла серйозну перевірку кібербезпеки, в той час як Alibaba і Tencent також опинилися під пильною увагою уряду в останні місяці.

У листопаді Управління кіберпростору Китаю оприлюднило новий набір законів, які перекласифікують дані та встановлюють численні набори штрафів за порушення політики кібербезпеки». ***(Jonathan Greig. Chinese regulators suspend Alibaba Cloud over failure to report Log4j vulnerability // ZDNet (https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/). 22.12.2021).***

***

«Linux повсюду. Это то, что запускают все облака, даже Microsoft Azure. Это то, что заставляет работать все 500 суперкомпьютеров из 500 лучших. Черт возьми, даже настольный Linux растет, если верить Pornhub, который утверждает, что количество пользователей Linux выросло на 28%, а количество пользователей Windows сократилось на 3%.

Программное обеспечение с открытым исходным кодом также растет не по дням, а по часам. Согласно отчету Gartner о цикле развития программного обеспечения с открытым исходным кодом (OSS) в 2021 году : «К 2025 году более 70% предприятий увеличат свои ИТ-расходы на OSS по сравнению с их текущими расходами на ИТ. Кроме того, к 2025 году программное обеспечение как услуга (SaaS) станет предпочтительной моделью потребления для OSS из-за его способности обеспечивать лучшую операционную простоту, безопасность и масштабируемость».

Думая о базах данных, о сути корпоративного программного обеспечения, Gartner предсказывает, что более 70% новых собственных приложений будут разрабатываться на базе данных с открытым исходным кодом. Одновременно 50% существующих экземпляров проприетарных реляционных баз данных будут преобразованы или конвертируются в СУБД с открытым исходным кодом.

Я куплю эти числа. Я с самого первого дня слежу за Linux и программным обеспечением с открытым исходным кодом. Куда бы я ни пошел, и все, с кем я разговариваю, признают, что эта пара управляет вселенной программного обеспечения.

Но Человек-паук знает, что с большой силой приходит и большая ответственность. И, как недавно выяснили многие разработчики, когда было обнаружено несколько уязвимостей безопасности в библиотеке с открытым исходным кодом для ведения журналов Apache Java log4j2, это тоже приносит большие головные боли.

Проблемы с log4j2 настолько серьезны, насколько это возможно. По шкале Национальной базы данных уязвимостей (NVD) он получил 10,0 CVSSv3, что совершенно ужасно.

Его настоящая проблема не столько в самом открытом исходном коде. Нет ничего волшебного в методологии и безопасности открытого исходного кода. Ошибки безопасности все еще могут ввести код. Закон Линуса гласит, что при достаточном внимании к ним все ошибки будут неглубокими. Но, если разработчиков не будет искать, уязвимости в системе безопасности все равно останутся незамеченными. Поскольку то, что я сейчас называю законом Шнайера, «Безопасность - это процесс, а не продукт», указывает на то, что для защиты всего программного обеспечения требуется постоянная бдительность.

Тем не менее, настоящая головная боль с log4j заключается в том, как Java скрывает, какие библиотеки используются в ее исходном коде и двоичных файлах в многочисленных вариациях Java Archive (JAR). Результат? Возможно, вы используете уязвимую версию log4j и не знаете, пока она не была взломана.

Как недавно объяснил Джош Брессерс, вице-президент Анкора по безопасности: «Одна из проблем, связанных с уязвимостью log4j, - это ее фактическое обнаружение. Java-приложения и зависимости обычно имеют какой-то

формат упаковки, который делает распространение и запуск очень простым, но это может затруднить выяснение того, что находится внутри этих программных пакетов ".

К счастью, существуют сканеры log4j, которые могут помочь вам обнаружить используемые дефектные библиотеки log4j. Но они не идеальны.

За беспорядком log4j стоит еще одна проблема: «Как узнать, какие компоненты с открытым исходным кодом использует ваше программное обеспечение?» Например, log4j2 используется с 2014 года. Вы не можете ожидать, что кто-то вспомнит, использовали ли они эту первую версию в какой-то программе, которую вы все еще используете.

Ответ - тот, к которому сообщество разработчиков ПО с открытым исходным кодом начало серьезно относиться в последние годы: создание ведомостей материалов по программному обеспечению (SBOM). SBOM точно указывает, какие программные библиотеки, процедуры и другой код использовались в любой программе. Вооружившись этим, вы можете проверить, какие версии компонентов используются в вашей программе.

Как объяснил Дэвид А. Уиллер, директор Linux Foundation по безопасности цепочки поставок с открытым исходным кодом, используя SBOM и проверенные воспроизводимые сборки, вы можете быть уверены, что знаете, что к чему в ваших программах. Таким образом, если в компоненте обнаружена дыра в безопасности, вы можете просто исправить ее, а не искать, как маньяк, любой возможный проблемный код, прежде чем иметь возможность ее исправить.

«Воспроизводимая сборка», кстати, объясняет Уиллер, - это «та, которая всегда дает одни и те же выходные данные при одинаковых входных данных, так что результаты сборки могут быть проверены. Проверенная воспроизводимая сборка - это процесс, при котором независимые организации создают сборку из исходного кода. и убедитесь, что полученные результаты получены из заявленного исходного кода».

Для этого вам и вашим разработчикам необходимо отслеживать свои программы в SBOM, используя формат обмена данными пакетов программного обеспечения (SPDX) Linux Foundation. Затем, чтобы еще больше гарантировать, что ваш код действительно является тем, за что он претендует, вам необходимо нотариально заверить и подтвердить свой SBOM с помощью таких сервисов, как Codenotary Community Attestation Service и Tidelift Catalogs.

Все это легко сказать. Делать это тяжело. В 2022 году почти все разработчики с открытым исходным кодом будут тратить много времени на проверку своего кода на наличие проблем, а затем на создание SBOM на основе SPDX. Пользователи, обеспокоенные катастрофами типа Solarwind и проблемами безопасности log4j, будут требовать этого.

В то же время разработчики Linux работают над дальнейшей защитой операционной системы, сделав Rust Linux вторым языком. Почему? Потому что, в отличие от C, основного языка Linux, Rust намного безопаснее. В частности, Rust намного безопаснее C при обработке ошибок памяти.

Как пояснил Райан Левик, главный защитник Microsoft облачных разработчиков, «Rust полностью безопасен для памяти». Это большое дело,

поскольку, как отметили разработчики ядра Linux Алекс Гейнор и Джеффри Томас на саммите по безопасности Linux 2019 года, почти две трети дыр в безопасности ядра Linux связаны с проблемами безопасности памяти. И откуда они берутся? Проблемы, присущие C и C ++.

Теперь Linux переписывают на Rust. По крайней мере, не в этом десятилетии, посоветуйтесь со мной еще раз в 2030-х, но в будущем на Rust будет написано много драйверов для Linux и другой код.

Как сказал мне Линус Торвальдс, хотя он «никоим образом не «настаивает на Rust», он «открыт для этого, учитывая обещанные преимущества и избегая некоторых ловушек безопасности. Тем не менее, он заключил: «Я также знаю, что иногда обещания не сбываются.»

Посмотрим, как это все получится. Независимо от того, как обстоят дела в деталях, одно я знаю наверняка. Мы увидим, что защита кода станет главной проблемой для разработчиков Linux и открытого исходного кода в 2022 году. И то, и другое стало слишком важным, чтобы все могло пойти по-другому». ***(Steven Vaughan-Nichols. In 2022, security will be Linux and open-source developers job number one // ZDNet (https://www.zdnet.com/article/in-2022-security-will-be-linux-and-open-source-developers-job-number-one/). 27.12.2021).***

***

«Apache Software Foundation (ASF) обнаружила третью ошибку в своей основанной на Java библиотеке регистрации Log4j с открытым исходным кодом.

CVE-2021-45105 - это ошибка бесконечной рекурсии с рейтингом 7,5 / 10, которая присутствовала в Log4j2 версий от 2.0-alpha1 до 2.16.0. Исправление - это версия 2.17.0 программы Log4j.

Это третья новая версия инструмента за последние десять дней.

Если вы не обратили внимания, версия 2.15.0 была создана для исправления CVE-2021-44228, критически важной и простой для использования уязвимости удаленного выполнения кода, присутствующей во многих версиях до 2.14.0.

Но в версии 2.15.0 не решена другая проблема - CVE-2021-45046, которая позволяла удаленному злоумышленнику с контролем над Thread Context Map (MDC) подготавливать вредоносный ввод с использованием шаблона поиска JNDI. Результатом может быть удаленное выполнение кода, к счастью, не во всех средах.

В версии 2.16.0 эта проблема устранена.

Но он не исправил CVE-2021-45105, который ASF описывает следующим образом:

Apache Log4j2 версий от 2.0-alpha1 до 2.16.0 не защищал от неконтролируемой рекурсии при поиске по ссылкам. Когда конфигурация ведения журнала использует нестандартный макет шаблона с поиском контекста (for example, $${ctx:loginId}), злоумышленники с контролем над входными данными карты контекста потока могут создавать вредоносные входные данные, содержащие рекурсивный поиск, что приводит к ошибке StackOverflowError, которая завершает процесс.

Программа вознаграждения за ошибки Zero Day Initiative, не зависящая от поставщика, описала недостаток следующим образом.

Когда вложенная переменная заменяется StrSubstitutorклассом, он рекурсивно вызывает substitute()класс. Однако, когда вложенная переменная ссылается на заменяемую переменную, рекурсия вызывается с той же строкой. Это приводит к бесконечной рекурсии и состоянию DoS на сервере.

Что делать?

К настоящему времени вы знаете, что такое упражнение: загрузите последнюю версию 2.17.0 Log4J здесь и установите ее везде, где работает Log4j, что, конечно, оказывается везде (в том числе в некоторых труднодоступных местах).

ASF также обрисовал в общих чертах следующие меры:

В PatternLayout в конфигурации ведения журнала замените Context Lookups, например, шаблонами ${ctx:loginId}or $${ctx:loginId}Thread Context Map (%X, %mdc, or %MDC).

В противном случае в конфигурации удалите ссылки на поисковые запросы контекста, например, ${ctx:loginId}или $${ctx:loginId}где они происходят из источников, внешних по отношению к приложению, таких как заголовки HTTP или вводимые пользователем данные.

Как только вы закончите, скрестите пальцы и надейтесь, что ASF обнаружил все недостатки, которые требуют немедленного исправления, чтобы мы все могли перестать беспокоиться об этом программном обеспечении до Рождества». ***(Simon Sharwood. Bad things come in threes: Apache reveals another Log4J bug // The Register (https://www.theregister.com/2021/12/19/log4j_new_flaw_cve_2021_45105/). 19.12.2021).***

***

«Компания Check Point Software Technologies сообщила о том, что ее специалисты зафиксировали более 1 272 000 кибератак, связанных с уязвимостью Log4j.

С пятницы, 9 декабря, когда впервые было сообщено об уязвимости, атаки с использованием Log4j начали нарастать, как снежный ком. Количество комбинаций того, как можно использовать эту уязвимость, дают злоумышленникам множество альтернатив для обхода недавно введенных средств защиты. Как отмечают эксперты, это означает, что одного уровня защиты недостаточно, и только многоуровневая система безопасности может обеспечить надежную защиту. Ранние сообщения от 10 декабря показывали всего тысячи попыток атак, а в субботу, 11 декабря, их число превысило 40 000. Через 24 часа после первоначальной вспышки сенсоры Check Point зафиксировали почти 200 000 попыток атак по всему миру.

В Check Point Research считают, что Log4j может вызвать настоящую киберпандемию, поэтому даже был создан специальный сайт, посвященный этому зловреду.

Как сообщается, хакеры с помощью ранее незамеченной уязвимости в библиотеке логирования Apache Log4j запускают до 100 атак в минуту.

Уязвимость CVE-2021-44228 или Log4j позволяет преступникам развёртывать вредоносный код с повышенными системными привилегиями. Она тривиально проста в эксплуатации и позволяет обходить защиту большинства традиционных решений безопасности.

Анализ Check Point показывает, что в большинстве случаев хакеры используют Log4j для получения контроля над компьютерами жертвы, используя их для майнинга или же подключения к ботнетам.

Согласно данным Check Point Research, около половины всех атак, связанных с Log4j совершены определенными хакерскими группировками, которые управляют крупными ботнетами Tsunami и Mirai». ***(Check Point зафиксировала 1 272 000 кибератак, связанных с Log4j // Компьютерное Обозрение (https://ko.com.ua/check_point_zafiksirovala_1_272_000_kiberatak_svyazannyh_s_log4shell_139722). 15.12.2021).***

***

«Компанія Eset повідомляє про сотні тисяч спроб використання уразливості в Log4j. Найбільша кількість була зафіксована у США, Великобританії, Туреччині, Німеччині та Нідерландах.

«Кількість спроб підтверджує, що ця масштабна проблема не зникне найближчим часом. Звичайно, зловмисники тестують багато варіантів експлойтів, але не всі спроби обов'язково є зловмисними. Деякі можуть бути безпечними, враховуючи, що дослідники та компанії з інформаційної безпеки також тестують експлойти на практиці в цілях захисту», – розповідає коментує Роман Ковач, директор з досліджень компанії Eset.

Варто зазначити, що Log4j – це бібліотека журналів на основі Java з відкритим вихідним кодом, яка широко використовується у багатьох популярних додатках і сервісах, наприклад, Apple, Twitter, Amazon, Google, LinkedIn.

У кінці листопада в цій бібліотеці було виявлено уразливість Log4Shell, яка дозволяє зловмиснику запускати довільний код на певному сервері. При цьому для запуску коду, що може призвести до повного контролю над системами та крадіжки конфіденційних даних, кіберзлочинцю не потрібен навіть фізичний доступ до них.

Вже 1 грудня було зафіксовано перший відомий експлойт для уразливості Log4Shell. Виправлення для Log4Shell було випущено 10 грудня.

Завдяки доступності в Інтернеті коду експлойту хакери активно сканують та використовують уразливі системи. З іншого боку спеціалісти з інформаційної безпеки оновлюють системи та мінімізують потенційні ризики, а розробники перевіряють програми та бібліотеки коду на наявність уразливих версій Log4j.

Для захисту від експлойтів важливо знайти всі уразливі версії бібліотеки Log4j. Почніть зі створення пріоритетного списку систем для пошуку та оцінюйте їх всі в порядку важливості. Нижче наведено декілька рекомендацій, які допоможуть у цьому процесі.

Виявіть Log4Shell у ваших системах (для Linux і Windows). Цей скрипт, доступний на GitHub, шукає проблемний файл JndiLookup.class у будь-якому архіві.jar;

Виявіть спроби використання уразливості Log4Shell у ваших журналах (для Linux). Скрипт, який також доступний за посиланням GitHub вище, шукає випадки використання Log4Shell в нестиснених файлах у каталозі журналів Linux /var/log та всіх його підкаталогах;

Зафіксуйте результати. Після запуску будь-яких скриптів або інструментів виявлення обов'язково запишіть результати, щоб створити повну документацію аудиту всіх ваших систем. Аудит має вказати, чи було знайдено Log4Shell та виявлено в журналах спроби її використання;

Використовуйте останню версію Log4j. Уразливими є всі версії з ядром log4j від 2.0-beta9 до 2.15.0. Таким чином, варто оновити бібліотеку до версії 2.16.0, яка є наразі актуальною. Зауважте, що цю бібліотеку не слід плутати з log4j-api, на яку Log4Shell не впливає;

Блокуйте підозрілі IP-адреси. І, зрештою, підозрілі IP-адреси можна заблокувати за допомогою брандмауера або системи запобігання вторгненням». ***(Eset виявила сотні тисяч спроб використання уразливості в Log4j, в тому числі в Україні // Компьютерное Обозрение (https://ko.com.ua/eset_viyavila_sotni_tisyach_sprob_vikoristannya_urazlivosti_v_log4j_v_tomu_chisli_v_ukrayini_139737). 16.12.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«AV-TEST недавно опубликовал список лучших антивирусных программ для macOS как для домашних, так и для бизнес-пользователей.

Антивирусы невероятно важны, учитывая безумно большое количество угроз кибербезопасности, с которыми сегодня сталкиваются в сети. В недавнем отчете, опубликованном Akamai, было обнаружено, что всего за последние 30 дней было обнаружено более 720 миллионов отдельных угроз кибербезопасности. Из них 73% были основаны на вредоносном ПО, а это означает, что антивирусное программное обеспечение, которое мы игнорировали всякий раз, когда оно просило нас об обновлении, начинает выглядеть действительно полезным. Во всяком случае, антивирусы не обязательно идут в ногу с настольными компьютерами macOS, и многие пользователи даже считают, что продукты Apple просто не могут быть заражены вирусами. Однако такое мнение немного ошибочно, и вредоносное ПО - это своего рода угроза, которая может не только заразить что-либо, но и причинить серьезный вред в процессе. Что плохого в том, чтобы потратить несколько лишних долларов, чтобы обезопасить себя от любых внешних источников вреда для вашего рабочего стола? невероятно полезный и актуальный механизм в современном мире.

Публикации антивирусного анализа AV-TEST разделены на две отдельные категории: одна для домашних пользователей, а другая для бизнес-пользователей. Это имеет смысл, учитывая, насколько различаются онлайн-взаимодействия и использование настольных компьютеров для обеих групп. Антивирусное

программное обеспечение оценивалось по трем различным критериям: защита, производительность и удобство использования; с каждым из трех присужденных баллов из общего числа 6. Установив параметры нашего исследования, давайте приступим к детализации, какое программное обеспечение лучше всего и для чего.

Для домашних пользователей было оценено в общей сложности восемь отдельных антивирусов, и все, кроме одного, получили максимально достижимую оценку 18 по всем трем критериям. Среди них известные имена включают Avast, F-Secure, AVG, NortonLifeLock и Avira. Единственное программное обеспечение, которому не удалось получить 18, было Protected.com, набрав 17 баллов из-за пяти из шести в категории защиты. В любом случае, занять последнее место, потеряв всего одну оценку в таком впечатляющем соревновании, - это вовсе не тот ущерб, который может показаться на первый взгляд. В целом, у домашних пользователей есть множество вариантов, на которые можно положиться.

Теперь давайте перейдем к бизнес-пользователям, поскольку у нас есть шесть антивирусов на выбор. Как и домашние пользователи, бизнес-пользователи имеют довольно хороший набор программного обеспечения на выбор, причем все антивирусы, кроме одного, имеют отличную оценку 18. Еще более обнадеживает тот факт, что единственное программное обеспечение, которое этого не делает, Acronis, по-прежнему набрал 17,5 балла, проиграв эту неуловимую половину балла результативности. Это оставляет бизнес-пользователям еще более лучший список антивирусов для выбора, даже если этот список короче, чем те, которые нравятся домашним пользователям». ***(Arooj Ahmed. AV-TEST Published Its Findings On The Best macOS Anti-Virus Software, With Separate Lists For Home And Business Users // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/av-test-published-its-findings-on-best.html). 28.12.2021).***

***

«Не так давно многие люди были более или менее не уверены в необходимости таких вещей, как антивирусы и тому подобное. Однако в настоящее время стало яснее, что антивирусы необходимы, потому что это то, что потенциально может в конечном итоге сдерживать вредоносное ПО и хакеров. Однако достаточно сказать, что многие из антивирусов, которые мы привыкли использовать за эти годы, на самом деле не так уж хороши.

В последнее время потребность в стороннем антивирусном программном обеспечении действительно начала снижаться, и основной причиной этого явления является наличие высококачественного встроенного программного обеспечения, такого как Защитник Windows. Многие люди склонны считать, что Защитник Windows не так хорош, как некоторые другие варианты, которые могут быть в вашем распоряжении, но это совсем не так. Фактически, недавние тесты антивируса показали, что он на самом деле один из лучших, со всеми соображениями и учётом.

AV-TEST - это немецкая фирма по кибербезопасности, специализирующаяся на проведении тестов на антивирусы и тому подобное. Их основная область знаний - определение того, насколько хорошо различные антивирусы выполняют свою

работу, и они оценивают каждый тестируемый антивирус по трем параметрам, а именно: защита, производительность и удобство использования. Антивирус может получить максимум шесть баллов в каждой из этих областей, что в основном означает, что программное обеспечение может получить высший балл в восемнадцать баллов в целом.

Учитывая все вышесказанное, важно отметить, что Защитник Windows фактически получил полные шесть баллов в каждой из трех областей, в которых он был протестирован, в результате чего он получил идеальную оценку 18. Это привело к тому, что он получил ярлык AV-TEST Top Product, который зарезервирован только для программного обеспечения, которому удается набрать максимально возможные баллы, поэтому справедливо предположить, что с Защитником Windows вам действительно не нужно какое-либо другое программное обеспечение, особенно когда вы считайте, что он поставляется бесплатно с вашей операционной системой…». ***(Zia Muhammad. Why Windows Defender is the Only Antivirus You Need // DIGITALINFORMATIONWORLD.COM (https://www.digitalinformationworld.com/2021/12/why-windows-defender-is-only-antivirus.html). 01.12.2021).***

***