Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 4 (квітень)

Київ – 2020

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2020 – №4 (квітень) . 113с.

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

«В Україні хочуть продовжити санкції проти російських сайтів і програмних продуктів. Зокрема, Вконтакте, Одноклассники, Яндекс, Mail.ru, Доктор Веб, Касперський, 1С і Парус.

Про це заявив глава СБУ Іван Баканов.

– Сьогодні ми не просто захищаємо українських громадян від фейків та інформаційних вкидань з російських соцмереж, а й дбаємо про кібербезпеку для представників бізнесу, державних та освітніх установ. Адже будь-який російський поштовий сервіс або антивірус можуть використовувати на шкоду Україні. Тому треба мінімізувати ризики. Блокуючи такі ресурси і програми, ми дбаємо про безпеку країни в цілому, – сказав він.

Також він запропонував створити і забезпечити функціонування в Україні Єдиного реєстру програмного забезпечення, дозволеного для використання в державних інформаційно-телекомунікаційних системах.

На думку кіберспеціалістів СБУ, це обмежить закупівлю і використання забороненого програмного забезпечення і створить сприятливі умови для розвитку вітчизняної ІТ-сфери…» ***(СБУ пропонує продовжити заборону на сайти і програми РФ // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20200423-sbu-proponuye-prodovzhyty-zaboronu-na-sajty-i-programy-rf/). 23.04.2020).***

***

«Количество кибератак, как и их масштабы в мире, увеличиваются от года к году. В 2019 году, по данным из открытых источников, они выросли на 20%, а общее количество зараженных вредоносным ПО устройств — почти на 40%. Чаще всего хакеры выбирают своими жертвами государственные учреждения, промышленные компании, медицину, образование и финансовые организации. Главной целью является похищение персональных, учетных и финансовых данных. На втором месте — шифрование данных с последующим вымогательством.

От тактики «сломать все, что ломается» злоумышленники переходят к целенаправленным атакам на конкретные бизнесы. Таких случаев в прошлом году было 60% от всех зафиксированных атак. Целевые атаки (targeted attacks) могут осуществляться скоординировано несколькими группами хакеров, после чего они делят выручку.

Растет популярность APT-атак (англ. Advanced Persistent Threat, то есть «сложная постоянная угроза» когда злоумышленники внедряются в системы компании, долго не дают о себе знать, наращивают свои возможности, а когда их деятельность становится заметна, защищаться уже поздно.

По опыту компании «Софтлист», взлом компьютеров, серверов и сетевого оборудования с помощью вредоносного программного обеспечения, которое все время усложняется, все еще занимает первое место по популярности методов. На втором, с небольшим отрывом, идет социальная инженерия. Хакеры получают данные учетных записей пользователей и стремятся открыть как можно большее количество «замков» в защите компании, оставаясь незамеченными. Эти два

метода находятся в топе во всех сферах деятельности, но особенно с большим отрывом лидируют в госсекторе и промышленности. Наименее подвержены IT-компании.

Украина: также под прицелом хакеров

За последние пять лет Украина пережила волну громких хакерских атак. Вирус Petya нанес урон стране в размере 0,5% ВВП. Еще до «пети» атакам подвергались региональные облэнерго: Черновицкой, Закарпатской и т.д. «Северная» в Киевской области даже стала героем масштабного расследования Wired.

Причина такой популярности Украины у хакеров легко объяснима. Большинство бизнесов разного размера и в разных секторах экономики не осознавали важность лицензионного ПО, установки обновлений, покупке комплексных защит. В кризисные и пост-кризисные 2015-2016 государству и бизнесу сложно было выделить бюджет на инвестиции в безопасность.

В последние годы ситуация начала меняться, хотя коренной сдвиг еще не произошел. Кроме того, сейчас на компании указывает давление еще один фактор — это массовый переход на удаленную работу в связи с пандемией COVID-19. «Организации вынуждены делать доступными корпоративные ресурсы удаленно в разных точках мира, где им сложно что бы то ни было контролировать. Эти запросы выходят за рамки прогнозируемых потребностей в увеличении емкости корпоративных ресурсов и требуют от компаний быстрых реакций: изменений в политиках удаленной работы и средствах обеспечения безопасности. По данным McAfee, во время пандемии 6% таргетированных атак приходится именно на украинские компании.

Как отмечают в компании «Софтлист», в госсекторе все еще не очень радужно. Но те компании, которые выделяют бюджеты на киберзащиту, чаще подходят к вопросу комплексно, осознавая серьезность угрозы. Например, энергетический сектор, который успел пострадать в былые годы, строит комплексную защиту против кибератак. Серьезные финансовые организации, в частности, крупные банки, также развивают это направление. Есть интерес со стороны промышленности, хотя пока еще не массовый. В других секторах ситуация меняется от предприятия к предприятию, разброс большой. Есть те, кто все еще считает, что они маленькие и незаметные (хотя в современном мире таких просто нет) и вообще не тратит денег на безопасность. Есть те, кто готов выделять бюджеты, но считает, что может справиться своими силами, есть компании, для которых кибербезопасность на первом месте и они внедряют лучшие практики.

Типичные ошибки в сфере кибербезопасности

Компания «Софтлист» работает 15 лет на IT-рынке. Как отмечает один из ее основателей Дмитрий Прокопенко, главное — это экспертиза команды.

«Мы постоянно работаем над собой, проходим обучение, трансформируем личный опыт каждого в командный, развитие внутренней экспертизы – наш приоритет», — говорит он.

По опыту Дмитрия, сегодня у предприятий бывает пять типичных ошибок в подходе к безопасности. Во-первых, когда бизнес вообще не инвестирует в это направление и считает, что его не коснется. Но 2015-2017-е годы показали, что те,

кто не защищен, страдают от всех известных печальных последствий. Компании, которые не задумывались не то что о серьезной киберзащите, а даже о бэкапах, остались без бизнеса.

Во-вторых, экономия на кибербезопасности. Украинские компании в основном живут сегодняшним днем, а IT — это всегда про инвестиции в будущее. Собственник не хочет тратить деньги здесь и сейчас, поэтому IT-департамент выкручивается условными или условно-бесплатными решениями, «взломанными» антивирусами, игнорирует установку обновлений и в целом экономит как может.

В-третьих, бизнес, который уже готов тратиться на киберзащиту, тоже не обязательно делает это правильно. Зачастую тут есть два ключевых заблуждения. Первое — что можно поставить какое-то известное решение по защите от одного вектора атак, не обязательно подходящее и направленное именно на то, что надо, перекреститься и забыть. Еще хуже — если админ сам сделал какое-то самописное решение, и если он ушел, никто не знает как с этим жить дальше.

Сегодня опасности подвержены не только компьютеры, сетевое оборудование и корпоративные ресурсы. Преступники атакуют мобильные устройства, устройства IoT, банкоматы, POS-терминалы и т.д. Если не выстроен периметр, если работа ведется не системно, дыры в безопасности будут, даже если компания обучила сотрудников менять пароли и не хранит чувствительную информацию в открытом доступе.

В-четвертых, — и это самая обидная ситуация — это тратить большие деньги на защиту, но делая все in house, без привлечения партнеров-экспертов.

«Недостаточно купить коробку. Не факт, что получится все внедрить самостоятельно. А если возникнут проблемы, кто будет их решать? На рынке просто нет специалистов такого уровня за пределами компаний-интеграторов. Чтобы их обучить, нужно иметь в запасе минимум несколько лет. За это время технологии опять поменяются и нужно заново учить людей», — говорит Дмитрий.

Будучи платиновым партнером McAfee компания «Софтлист» регулярно проводит обучение своих сотрудников и имеет доступ к лучшим мировым практикам.

Наконец, в-пятых, — это сделать все правильно, инвестировать в покупку лучших решений на рынке и остановиться на этом.

«Безопасность — это процесс. Нельзя купить самую дорогую и великолепную «коробку» и успокоиться. Сопровождение и поддержка каждого решения по защите данных и контроля доступа требует постоянных немаленьких трудовых, временных и финансовых затрат. Для этого мы создали профессиональный сервис для наших клиентов и предлагаем им уже готовые решения», — объясняет Дмитрий Прокопенко.

Как защищаться от угрозы?

Для противодействия серьезным атакам эксперты компании «Софтлист» рекомендуют применять комплексные меры. В частности, это установка систем централизованного управления обновлениями и патчами, глубокого анализа сетевого трафика, антивирусов со встроенной изолированной средой («песочницей») для динамической проверки файлов, межсетевых экранов уровня приложений, сервисов анти-DDoS, автоматизированных средств анализа

защищенности и выявления уязвимостей, а также SIEM-решений (Security Information и Event Management).

В «Софтлист» приводят в пример типичный кейс по кибербезопасности для энергоотрасли. Своим клиентам компания внедряет средства обнаружения и реагирования, позволяющие защитить конечные точки от сложных угроз, шлюз для всесторонней защиты входящего и исходящего трафика, а также контроля доступа пользователей к интернету, решение для защиты баз данных критически важных систем, защита конечных точек и т.д. Данные из всех этих систем стекаются в McAfee SIEM, это позволяет своевременно выявлять инциденты информационной безопасности и эффективно на них реагировать.

SIEM-система предназначена для анализа информации, которая поступает от других систем — антивирусов, оборудования, DLP, IDS и т.д. Она обнаруживает отклонения от нормы по разным критериям и генерирует инцидент. Например, аномалии в трафике, поведении пользователей, неопознанных устройствах и т.д. Допустим, сотрудник компании отправил письмо с чувствительной информацией не тому адресату или случайно перешел по ссылке из письма, которое на самом деле было фишинговым и т.д., в SIEM это видно.

По сути, сегодня SIEM — это самый важный инструмент защиты, так как именно он обеспечивает комплексность подхода. Каждый по отдельности инструмент важен и закрывает свою область. Но в случае сложных комбинированных атак важно видеть картину целиком, происходит ли что-то аномальное в системе.

Независимо от размера, организации в Украине испытывают сложности с самостоятельным внедрением продуктов по информационной безопасности. Построение комплексной архитектуры защиты информации — долгий процесс, который состоит из установки, настройки, написания дополнительных правил реагирования, тестовой эксплуатации, внесения корректировок и т.д. На обучение специалистов уходят годы, для компании — это слишком большие затраты. Следовательно, инвестиции при полностью самостоятельной работе не всегда оправдывают себя, и максимальной эффективности достигают те компании, которые добавляют в проект услуги интеграторов, как «Софтлист». Более того, статус платинового партнера McAfee позволяет «Софтлист» перенимать опыт и новые практики внедрения от производителя напрямую, что способствует оперативному решению любых вопросов клиента…». ***(Кибератаки становятся комплексными и целенаправленными. Роль SIEM системы в комплексной защите компании // AIN.UA (https://ain.ua/2020/04/24/kiberataki-stanovyatsya-kompleksnymi-i-celenapravlennymi-rol-siem-sistemy-v-kompleksnoj-zashhite-kompanii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ainua+%28AIN.UA%29). 24.05.2020).***

***

«Команда CERT-UA Госспецсвязи с 18 по 24 апреля зарегистрировала 2882 киберинцидента. Это в три раза больше, чем было зарегистрировано неделю тому назад и в 2-2,5 раза больше, чем в среднем еженедельно регистрировалось в марте-апреле.

Об этом сообщается на сайте Госспецсвязи.

"В рамках взаимодействия с центрами реагирования на компьютерные инциденты, участия в международном сотрудничестве в сфере реагирования на компьютерные угрозы команда CERT-UA Госспецсвязи в период с 18 по 24 апреля зарегистрировала 2882 киберинцидента. Обработаны 2878 инцидентов (в доменных зонах uagov – 5, uacom – 2873, fgov – 0, fcom – 0, из них запросов иностранных CERT – 2867)", – говорится в сообщении.

Так, было зафиксировано 17 фактов DDoS-атак (в том числе на сайты Офиса Президента Украины, ГБР, Госспецсвязи).

В течение указанного периода были усилены меры безопасности и даны рекомендации по работе 22 сайтов органов государственной власти (сайт Луганской ОГА, Госспецсвязи, МВД, НАБУ, КМУ, Мининфраструктуры, ГФС).» ***(В Украине за неделю зафиксировали почти три тысячи кибератак // «Новости онлайн 24» (https://newsonline24.com.ua/v-ukraine-za-nedelyu-zafiksirovali-pochti-tri-tysyachi-kiberatak/). 28.04.2020).***

***

Національна система кібербезпеки

«Государственная служба специальной связи и защиты информации Украины завершила аудит кибербезопасности ГК «Укроборонпром», инициированный концерном в марте 2020 г. Об этом сообщает пресс-служба госконцерна.

В процессе оценки специалисты рассмотрели политику информационной безопасности «Укроборонпрома», организацию системы информационной безопасности, управления информационными активами концерна, управление доступом и другие аспекты физической и сетевой безопасности.

«На этой неделе мы получили финальный отчет о проведенном аудите кибербезопасности концерна.

Инициируя эту оценку, мы ставили четкую цель - определить существующий уровень киберзащиты концерна, а также направления и подходы к ее улучшению в соответствии с новыми нормативными. Аудит показал, что в целом IT-система и система информационной безопасности концерна довольно надежно защищены существующими организационными и техническими средствами. в то же время, есть ряд элементов, которые нуждаются в совершенствовании. Проработав рекомендации аудита, мы решили создать в концерне Операционный центр безопасности и единый Центр компетенций по кибербезопасности, который будет оказывать помощь предприятиям-участникам «Укроборонпрома». Также запускаем онлайн-программу по «кибергигиене» для сотрудников всех предприятий, чтобы научить их основам поведения в современном киберпространстве», - прокомментировала результаты аудита заместитель генерального директора «Укроборонпрома» по инновациям Надежда Васильева.

Она рассказала, что в процессе цифровой трансформации «Укроборонпрома» была проведена оценка всех предприятий концерна, которая показала очень разный

уровень организации процессов и защиты информации и IT-систем. «Мы хотим ускорить цифровую трансформацию оборонного сектора Украины, в т.ч., за счет внедрения современных надежно защищенных IT-систем и постоянного обучения наших сотрудников. Благодаря программе по кибергигиене, осведомленность и бдительность наших сотрудников по правильному обращению с киберугрозами существенно выросла, это в том числе помогает нам противостоять многочисленным атакам», - добавляет Н.Васильева.

В течение 2020 г. «Укроборонпром» постоянно атакуется киберпреступниками. Атаки осуществляются не только с целью блокирования работы предприятий и искажения информации, но и кибершпионажа - с целью получения коммерческой информации государственного характера.

«На днях специалисты Концерна блокировали одну из таких массированных кибератак типа brute-force: мы зафиксировали более миллиона попыток доступов к электронным почтовым ящикам сотрудников концерна, которые поступают из 18 стран Европы. Впрочем, система информационной безопасности концерна позволяет заблаговременно выявлять и отражать такие атаки», - сообщил заместитель генерального директора по безопасности концерна Константин Бушуев». ***(«Укроборонпром» прошел аудит кибербезопасности // Транспортный бизнес (http://tbu.com.ua/news/ukroboronprom_proshel_audit_kiberbezopasnosti_.html). 27.04.2020).***

***

Кібервійна проти України

«Українські хакери у полум'ї кібервійни стали міжнародним брендом

Україна і раніше була заповідником дрібної злочинності в Інтернеті. Потім почалася війна з Росією. І вже сьогодні тут випробуються засоби цифрової війни. Колишні хакери стали самостійною силою…

«П'ять-десять років тому Україна була чимось на зразок хакерського раю. Але ера приватних хакерів завершується. Кардери майже пропали. Хакінг став організованим. Якщо спіймають молодика за хакерством – до нього прийде поліція. А наступного дня до нього завітає компанія, яка йому запропонує $5 тис. на місяць, якщо він на неї працюватиме» - розповідає адвокат Артем Афіян.

США надсилають «кібербійців» до України

Така еволюція має й політичні передумови: в 2014 році Україна революцією на Майдані відірвалася від Росії; столиця з тієї пори не бажає називатися «Кієвом», а називається «Київ», це українська транскрипція. Але цей відрив також перетворив країну на тестовий полігон для кіберзброї.

Якщо в 2000-ні та на початку 2010-х Україна була ще «ігровим майданчиком» для хакерів, то зараз тут точиться справжня цифрова війна. Наразі вже й США надсилають кібербійців до України, аби вони тут навчалися, як робляться кібератаки, та самі готувалися до них. Після того, як на сервери Демократичної партії США було здійснено хакерський напад, і це допомогло

Дональду Трампу перемогти на президентських виборах, американцям достеменно стало зрозуміло, до яких наслідків може призвести дія кіберзброї.

Хоча майже неможливо точно визначити, яка держава та яка командна структура провела ту чи іншу кібератаку, але можливість її відбити, зрештою, з самого початку закладена в саму атаку. У великих атаках, які спрямовані на Україну, експерти та співробітники спецслужб чітко впізнають російський «почерк».

Кібер-«хробак», який обійшовся в мільярди

Наразі наймасштабнішим нападом на тестовому полігоні «Україна» вважається Notpetya. Це комп'ютерний вірус, який влітку 2017 року, стартував зі зламаного серверу маленької київської компанії з розробки програмного забезпечення, паралізував усю країну. «Хробак» знищив інформацію на 10% усіх українських комп'ютерів та тимчасово паралізував в Україні два аеропорти, 22 банки та купу різноманітних державних закладів.

З українських комп'ютерів Notpetya перестрибнув на сервери таких концернів, як Merck (фармацевтичний гігант) або перевізників Fedex та Maersk. Американському концерну Merck, за оцінкою експерта Енді Грінберга, Notpetya обійшовся в $870 млн. Найбільшій в світі контейнерній компанії Maersk він коштував $300 млн.

Експерти Білого Дому з питань безпеки вважають, що загалом вірус завдав шкоди приблизно на $10 млрд. Вони звинувачують у всьому російську ГРУ.

Постійна загроза для української IT-інфраструктури перетворила комп'ютерну безпеку на центральну тему: з класичної аутсорсингової індустрії ця діяльність виросла у стрімко зростаючий сектор кібербезпеки. Хакери та фахівці з IT-безпеки працюють зараз для уряду та отримують все більше зарубіжних контрактів.

Віктор Жора сидить в центрі Києва в кафе та їсть пиріг. Йому під сорок, одягнений в чорний светр. Біля нашого столика стоїть двохметрова малинова пластикова скульптура собаки, яка нагадує роботи американського скульптора Джефа Коонса й надає розмові якоїсь сюрреалістичності.

З початку 2000-х Жора працює у секторі IT-безпеки. «15 років тому щось, подібне кібервійні, й уявити собі не можна було», - розповідає він та бере виделкою шматок пирога. З того часу, як Україна політично відокремилася від Росії, все змінилося. Він та його фірма Infosafe з 2009 року допомагали убезпечити вісім парламентських та президентських виборів.

«Вебсайт ЦВК постійно атакували»

Взагалі-то, в Україні все ще використовують паперові бюлетені для голосування, тож результати виборів дуже важко «хакнути» цифровими методами. Але в країні, яка з 2004 року пережила дві революції, якісь невідповідності на виборах можуть призвести до вибуху.

«У ніч виборів та наступного дня на сайті виборчої комісії був просто шалений трафік» - згадує Жора. – На сайт ЦВК постійно нападали. Ми намагалися втримати його всіма силами – від створення «дзеркальних» сторінок до захисту від DDoS-атак».

Найінтенсивніші атаки Жора датує 25 травня 2014 року. «Наш великий сусід вирішив тоді довести всьому світові, що ми в Києві обрали собі хунту», - розповідає він. Хунта – це визначення, яке в 2014 році використовували, перш за все, російські ЗМІ, аби дискредитувати тодішню українську владу.

«Напад виконувався у три фази» - розповідає Жора. Ще перед виборами хакери за допомогою цілеспрямованих фішінг-атак непомітно проникли до комп'ютерної системи Центральної виборчої комісії. За пару годин до того, як на сайті ЦВК були оприлюднені перші попередні результати, він та його колеги отримали повідомлення про злам системи.

Хтось помітив, що вже перед першими попередніми результатами на сайт було завантажено світлину нібито переможця, щоб її можна було будь-якої миті оприлюднити. На світлині був Дмитро Ярош, лідер праворадикальних бойовиків «Правого Сектора» (прим. «Главкома» - саме так автор матеріалу у німецькому виданні визначив цю організацію, переклад дослівний).

Політичні кібератаки на Україну

Світлина Яроша, як переможця виборів, на офіційній сторінці Центральної виборчої комісії мала б катастрофічні наслідки для України: російські ЗМІ, які мають багато читачів і в Україні, роздмухали б до небес свою тезу про хунту. Повідомлення про перемогу Яроша миттєво вивела б на вулицю як прихильників Правого Сектору, так і людей, які підтримують інші партії, які б впали у розпач. Цей хаос би постав під сумнів всі вибори.

«Щойно ми побачили цю світлину, нам стало зрозуміло, що систему зламано» - розповідає Жора. Повністю перевірити всю систему та гарантовано викинути нападника – це б забрало дуже багато часу. «Тому ми почали повністю міняти всі точки доступу та саму сторінку», - пояснює він. Нова сторінка вийшла в онлайн невдовзі перед отриманням попередніх результатів.

«Єдиний захід на стару адресу, де висіла світлина Яроша, було здійснено з IP-адреси одного з російських телеканалів», - каже Жора з багатозначним виразом на обличчі. Злам сторінки української виборчої комісії став чимось на кшталт стартового пострілу для великих політичних кібератак на Україну.

Хакери планували захопити електромережі

23 грудня 2015 року в 230 тисяч жителів Івано-Франківської області раннім вечором раптом вимкнулося світло. Вперше в світі, за допомогою спецоперації, хакери захопили контроль над електромережею.

Вони добре підготувалися. За допомогою надісланого через емейл вордівського файлу з назвою BlackEnergy ще навесні 2015 року вони почали інфікувати комп'ютери співробітників енергопостачальних компаній на Заході України.

Хакери витратили місяці на те, щоб обійти захист електропостачальників та розібратися, як функціонують їх виробничі комп'ютери. Момент, коли вони були повністю готові, наступив 23 грудня 2015 року. Тоді зловмисники «перемкнули важелі» в трьох розподільчих центрах та на 30 підстанціях. Електроенергія зникла. «Вишенька на торті» - хакери під час нападу вимкнули ще й запасні агрегати трьох атакованих розподільчих центрів, так, що навіть і без того збиті з пантелику співробітники сиділи в темряві.

Приблизно рік потому, в грудні 2016 року, було здійснено напад на «Київенерго». «При цьому на пів ночі вирубилося світло у Києві. Хакерський софт, який було використано, був написаний окремо для промислової контрольної системи цієї компанії, - розповідає Жора. – Вони відпрацювали свої хакерські програми на комп'ютерній системі «Київенерго» й тепер можуть використати їх будь-де в світі».

Американські кіберспецпідрозділи в Україні

Але в Україні тренуються не лише нападники. З моменту кібернападу на систему виборів та енергетичні системи США надсилають сюди не лише обладнання та допомогу для захисту, а й спецпідрозділи, які вивчають ці атаки на місці, аби підготувати до них Америку.

«Наша протидія нападу BlackEnergy полягала в тому, що ми відновили струм в розподільчих центрах вручну. В США це б просто не вийшло, тому що там електромережі керуються повністю комп'ютерами», - пояснює Жора.

«Ймовірно, хакери хотіли побачити, чи працюють їхні віруси належним чином. А також як на це відреагує міжнародна спільнота», - пояснює Марія Безнер у розмові по скайпу. Безнер в Центрі безпекових досліджень технічного університету ETH в Цюриху досліджує питання, яку роль кібератаки грають в конфліктах, подібних війнам в Сирії чи Україні.

В одній із своїх наукових статей вона перераховує 64 атаки та контратаки в українському конфлікті за період між листопадом 2013-го та груднем 2016-го. «Україна, без сумніву, має для США стратегічне значення. Америка може спостерігати в Україні, яким чином здійснюються напади на комп'ютерні системи, які віруси використовуються, та вивчати тактику нападників. Це було дуже корисно перед довиборами в Конгрес США в 2018 році. Перед виборами 2020 року вони чинитимуть так само й надішлють кібербійців до України, Македонії та Чорногорії».

Платформа Hacken Proof

В об'єднаному інтернетом світовому просторі кібератаки, почавшись в якійсь окремій державі, не залишаються в її межах, а розповсюджуються по всьому світі.

Лише в парі кілометрів від кафе, в якому відбулася зустріч з Віктором Жорою, працює маленька українська фірма-розробник програмного забезпечення з назвою Linkos Group.

Linkos продає звичайнісіньку бухгалтерську програму з назвою M.E.Doc, перш за все, українським клієнтам. В червні 2017 року хакери використали один із серверів цієї фірми, аби випустити в світ вірус, який став пізніше відомим з ім'ям Notpetya.

Хакерські атаки проти України, які експерт з кібербезпеки Жора називає «холодним душем», вдихнули нове життя в українську хакерську громаду. В західній частині Києва, в кафе офісної будівлі з назвою Unit City, ми зустрілися з Єгором Аушевим та його бізнес-партнеркою Євгенією Брошеван.

Обидва вдягнені в толстовки: Аушев – у чорну, Брошеван – в червону. За допомогою грошей, отриманих від операцій з криптовалютами, обидва збудували платформу з назвою Hacken Proof. На цій платформі підприємства можуть записатися на тест із вторгнення: свого роду перевірку на міцність свого захисту

від хакерів. Один із трьох тисяч зареєстрованих на сайті легальних хакерів шукає в цьому випадку на слабкі місця в захисті тієї чи іншої фірми – і записує те, що знайде.

Мінлива історія України – від колишнього «садочка» для кіберзлочинців до «дитини кібервійни» – підштовхнула цей бізнес до розвитку. «Знадобилося багато часу, аби переконати клієнтів винайняти для свого кіберзахисту саме українську фірму. З іншого боку, Україна вже стала відомою своїми хакерами та кібератаками», - пояснює Аушев. Одним із клієнтів, якими він особливо пишається, є одна з азіатських авіакомпаній.

Засновник Hacken Proof Аушев вважає, що в Україні наразі існують близько 30 компаній з кібербезпеки. При цьому він підтверджує зростання попиту на фахівців з кібербезпеки. Він скористався цим для власного бізнесу, викладаючи безпекові курси.

Не востаннє через атаки, подібні BlackEnergy та Notpetya індустрія кібербезпеки переживає бум, подібного якому ще не було. Й українські хакери в вогні кібервійни стали міжнародним брендом». ***(Ян Фолльмер. Кібервійна: Україна – тестовий полігон для усього світу // "Українські медійні системи (https://glavcom.ua/publications/kiberviyna-ukrajina-testoviy-poligon-dlya-usogo-svitu-671608.html). 07.04.2020).***

***

«З 28 березня по 2 квітня було зафіксовано та усунуто дві кібератаки на сайт Служби безпеки України та 17 на сайт Офісу Президента України…

"З 28 березня по 2 квітня було зафіксовано та усунуто наступні порушення: в роботі сайтів органів державної влади 18 (сайт Луганської ОДА — 9, Держспецзв'язку — 6, МВС — 2, Мінінфраструктури — 2); 26 фактів DDoS-атак (серед них сайти СБУ — 2, Офіса Президента України — 17, Держспецзв'язку — 6, Міненерго — 1)", — йдеться в повідомленні.

Загалом в рамках взаємодії з центрами реагування на комп'ютерні інциденти, участі у міжнародному співробітництві у сфері реагування на комп'ютерні загрози команда CERT-UA Держспецзв'язку в період з 28 березня по 2 квітня зареєструвала 1375 кіберінцидентів.

Зазначається, що система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури зафіксувала 9253 підозрілих події: серед них — спроби викрадення інформації — 156, мережеве сканування — 2962, виявлення мережевого трояна — 781, Web-атаки — 484, виявлення нестандартних протоколів або подій — 3946, спроби отримання прав адміністратора — 880.» ***(Ілля Нежигай. Зареєстровано 17 кібератак на сайт Офісу Президента України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1862264-zareyestrovano-17-kiberatak-na-sayt-ofisu-prezidenta-ukrayini). 07.04.2020).***

***

«На сервіси КМДА здійснюється масована DDoS-атака. Близько 90% спроб атакувати мережу успішно відбиваються внутрішньою системою кіберзахисту. Про це повідомляє прес-служба КМДА.

Система кіберзахисту забезпечила працездатність усіх міських сервісів. Однак система та зовнішні канали зв'язку працюють із значним навантаженням, через що можливі тимчасові обмеження доступу до е-сервісів або міських сайтів. За першу годину атаки зафіксовано близько 1,5 мільйона оригінальних IP-адрес, із яких здійснювались спроби дестабілізувати роботу е-сервісів. За 20 хвилин система кіберзахисту змогла відхилити близько 4 мільярдів атакуючих запитів.

«Завдяки правильним налаштуванням та гнучкому багаторівневому захисту спеціалісти мінімізували втрати від кібератаки та змогли розблокувати трафік для міських е-сервісів. Ми вже передали інформацію про інцидент до правоохоронних органів та робимо все можливе для якнайшвидшої стабілізації ситуації. Можу сказати точно, що за тривалістю та кількістю атакуючих ботів подібних викликів в Україні ще не було», – повідомив директор Департаменту інформаційно-комунікаційних технологій КМДА Юрій Назаров.

Незважаючи на те, що спеціалісти з кібербезпеки продовжують нейтралізувати DDoS-атаки та роблять все від них залежне для якісної роботи е-сервісів, можливі тимчасові обмеження в доступі до міських сайтів. Міська влада просить з розумінням поставитись до ситуації, що виникла.

«Сервери КМДА продовжують відбивати кібератаки. Кілька днів поспіль», — заявив Віталій Кличко на своєму Telegram-каналі». ***(На сайт мера Кличка здійснюється кібератака: що відомо // Судово-юридична газета (https://sud.ua/ru/news/ukraine/166235-na-sayt-mera-klichka-zdiysnyuyetsya-kiberataka-scho-vidomo). 14.04.2020).***

***

«Команда CERT-UA Державної служби спеціального зв'язку та захисту інформації України у період з 3 по 10 квітня зареєструвала 1174 кіберінциденти. Про це повідомляє пресслужба Держспецзв'язку…

"В рамках взаємодії з центрами реагування на комп'ютерні інциденти, участі у міжнародному співробітництві у сфері реагування на комп'ютерні загрози, команда CERT-UA Держспецзв'язку у період з 3 по 10 квітня зареєструвала 1174 кіберінциденти. Опрацьовано 1168 інцидентів (у доменних зонах uagov – 1, uacom – 1162, fgov – 0, fcom – 5; з них запитів іноземних CERT - 1158)", - повідомили у службі.

Зазначається, що протягом зазначеного періоду було посилено заходи безпеки у роботі 13 сайтів органів державної влади, зокрема сайту Луганської ОДА, Держспецзв'язку, МВС, ДБР, Мінекономрозвитку, МЗС, Мінрегіону, МОН, МОЗ, НАБУ, РНБО, СБУ.

Крім того, командою було зафіксовано 34 фактів DDoS-атак. Серед них на сайти СБУ, Офіс Президента України, ДБР, Держспецзв'язку, НАБУ, Міненерго.

Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури зафіксувала 12645 підозрілих подій.

Серед них - спроби викрадення інформації – 469, мережеве сканування - 2960, виявлення мережевого трояна – 1454, Web-атаки – 418, виявлення нестандартних протоколів або подій – 4517, спроби отримання прав адміністратора – 2760, спроби отримання прав користувача - 67…». ***(Саша Картер. У Держспецзв'язку зафіксували на початку квітня понад 1 тис. DDoS-атак та кіберінцидентів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1863743-u-derzhspetszvyazku-zafiksuvali-ponad-1-tis-ddos-atak-ta-kiberintsidentiv). 14.04.2020).***

***

Боротьба з кіберзлочинністю в Україні

«СБУ локализовала в Луганской области заражение вирусом компьютерной сети одного из городских советов.

На Луганщине киберспециалисты Службы безопасности Украины установили, что на официальном сайте одного из городских советов размещены файлы, пораженные вредоносным программным обеспечением, сообщает ВВ по информации пресс-службы регионального ведомства.

В ходе проверки сотрудники СБУ установили, что 24 рабочих компьютеры органа местного самоуправления пораженные вирусом. Через все документы публичной информации, которые загружались на сайт горсовета, происходило поражения компьютеров пользователей портала.

Специалисты по кибербезопасности прекратили распространение вредоносной программы, минимизировали негативные последствия поражения и дали рекомендации по устранению недостатков в системе технического компьютерного обеспечения горсовета.

Сейчас проверяется информация о сознательном инфицировании локальной компьютерной системы госучреждения и определения лиц причастных к киберинциденту. По результатам проверки будет принято решение о направлении материалов документирования противоправной деятельности по подследственности для открытия уголовного производства. Выявление киберугрозы проводилось сотрудниками Департамента контрразведывательной защиты интересов государства в сфере информационной безопасности и Главного управления СБ Украины в Донецкой и Луганской областях». ***(Вирусом заразили компьютерную сеть одного городского совета Луганской области // ООО «Схід Медіа Холдинг» (https://cxid.info/150235_virusom-zarazili-kompyuternuyu-set-odnogo-gorodskogo-soveta-luganskoi-oblasti.html). 05.04.2020).***

***

«…Працівниками кіберполіції в Рівненській області спільно із слідчими поліції Рівненщини, під процесуальним керівництвом Рівненської місцевої прокуратури та за сприянням співробітників банківської установи, викрили 21-річну жінку, яка продавала інформацію з обмеженим доступом, що обробляється в автоматизованій банківській системі.

Кіберполіція встановила, що фігурантка була спеціалістом із обслуговування клієнтів у відділені одного з банків у Києві та мала доступ до автоматизованої банківської системи. Користуючись своїми повноваженнями, працівниця банку за допомогою особистого логіну і паролю, здобувала інформацію, що становить банківську таємницю, а саме: паспортні дані, ідентифікаційний код, інформацію про наявність банківських рахунків та рух коштів по них. В подальшому за допомогою закритих груп у месенджері збувала третім особам.

Крім цього, встановлено причетність до скоєння цього кримінального правопорушення співмешканця фігурантки. Останній допомагав продавати інформацію та відповідав за обготівкування коштів отриманих внаслідок злочинної діяльності…

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Незаконне втручання в роботу комп'ютерів, систем та комп'ютерних мереж) Кримінального кодексу України. Наразі вирішується питання щодо оголошення особам про підозру. Їм загрожує до 6 років ув'язнення». ***(Кіберполіція викрила співробітницю банку у продажі конфіденційної інформації // Кібероліція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-spivrobitnyczyu-banku-u-prodazhi-konfidenczijnoyi-informacziyi-4165/). 08.04.2020).***

***

«З початку карантину виявлено 267 фактів розповсюдження фейків. Перевірено 483 повідомлення щодо можливих шахрайств, у тому числі при онлайн купівлі засобів індивідуального захисту.

Під час моніторингу глобальної мережі кіберполіція виявила 267 фактів щодо розміщення на інформаційних ресурсах неправдивої чи провокаційної інформації щодо пандемії коронавірусу. Наразі вже ідентифіковано 152 особи, які цю інформацію розповсюджували.

Також кіберполіцією перевірено 483 повідомлення щодо вчинення можливих протиправних дій, у тому числі онлайн шахрайств, пов'язаних з коронавірусом. За результатами – відкрито 41 кримінальне провадження.

Крім цього, заблоковано 157 Інтернет-посилань, що використовувались шахраями з метою «наживи» під час пандемії.

Так, співробітниками кіберполіції у Харківській області спільно зі слідчими поліції під процесуальним керівництвом прокуратури Харківської області викрито раніше судимого 28-річного чоловіка, який заволодів грошима громадян під приводом продажу засобів індивідуального захисту. Чоловік розмістив оголошення щодо продажу медичних масок та дезінфікуючих засобів на сайтах оголошень. Доставку товару обіцяв тільки на умовах передоплати. Після отримання коштів від потерпілих, не відповідав на телефонні дзвінки та змінював номер телефону в оголошенні. За місцем мешкання фігуранта правоохоронці провели обшук. Наразі чоловіку повідомлено про підозру за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Вирішується питання щодо обрання фігуранту запобіжного заходу.

На Закарпатті працівниками кіберполіції встановлено громадянку, яка за допомогою сайту оголошень здійснювала продаж іноземних пігулок за ціною 250

гривень за упаковку. Згідно інформації МОЗ України ліки, які реалізовувала 48-річна громадянка не отримали декларацію про відповідність на території України. Наразі відносно фігурантки складено адміністративний протокол за ч. 1 ст. 164 (Порушення порядку провадження господарської діяльності) КУпАП. Весь товар вилучено…» ***(Кіберполіція заблокувала 157 шахрайських інтернет-посилань пов'язаних з короновірусом // Кібероліція України (https://cyberpolice.gov.ua/news/z-pochatku-karantynu-vyyavleno--faktiv-rozpovsyudzhennya-fejkiv-perevireno--povidomlennya-shhodo-mozhlyvyx-shaxrajstv-u-tomu-chysli-pry-onlajn-kupivli-zasobiv-indyvidualnogo-zaxystu-5687/). 08.04.2020).***

***

«…Співробітниками кіберполіції в Хмельницькій області спільно з працівниками слідчого управління та роти поліції особливого призначення ГУНП в Хмельницькій області, під процесуальним керівництвом обласної прокуратури, викрито 30-річного місцевого мешканця у збуті та розповсюдженні інформації з обмеженим доступом, яка зберігається в комп'ютерах.

Кіберполіція встановила, що чоловік збував конфіденційну інформацію користувачів мережі Інтернет. А саме логінів та паролів доступу до різних інтернет-ресурсів: електронних поштових скриньок, облікових записів соціальних мереж та електронних гаманців.

Бази даних фігурант купував на тематичних хакерських форумах. Далі правопорушник перевіряв логіни та паролі на наявність позитивного фінансового балансу та в подальшому продавав на закритих форумах та за допомогою месенджерів.

Правоохоронці провели обшук за місцем мешкання фігуранта. За результатом вилучено комп'ютерну техніку, накопичувачі інформації та особисті засоби зв'язку.

За даним фактом відкрито кримінальне провадження за ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Наразі справу скеровано до суду. Чоловіку загрожує до 5 років ув'язнення». ***(Кіберполіція викрила жителя Хмельницького у продажі конфіденційної інформації користувачів мережі Інтернет // Кібероліція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zhytelya-xmelnyczkogo-u-prodazhi-konfidenczijnoyi-informacziyi-korystuvachiv-merezhi-internet-7321/). 02.04.2020).***

***

«Служба безпеки викрила мешканця Івано-Франківська, який продавав інформацію з обмеженим доступом із державних баз даних Державної митної та прикордонної служб.

Як повідомляє СБУ, фахівці з кібербезпеки зафіксували, що на спеціалізованих інтернет-сервісах з'явилися оголошення з пропозиціями придбати інформацію з цих баз даних, передає СТИК.

Під час перевірки з'ясувалося, що «продавець» під фейковими обліковими записами обіцяє клієнтам дані, зокрема, про перетин кордону українськими громадянами та іноземцями, транспортними засобами, терміни їх перебування за кордоном.

Такі відомості належать до інформації з обмеженим доступом, несанкціоноване розповсюдження якої заборонено законом, інформують в СБУ. Оплату від замовників зловмисник приймав на банківські картки.

Оперативники спецслужби задокументували декілька епізодів продажу іванофранківцем інформації з обмеженим доступом. Його клієнтами були мешканці різних регіонів України.

Під час обшуку в нього вилучили мобільні телефони, сімкарти, ноутбук і планшет, за допомогою яких він розміщував незаконні оголошення, та банківські картки, на які приймав оплату «послуг».

Справу відкрили за ч. 2 ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом) Кримінального кодексу. Йому загрожує позбавлення волі від 2 до 5 років». ***(Франківець продавав інформацію з баз даних митниці та прикордонної служби — СБУ // StykNews (http://styknews.info/novyny/kryminal/2020/04/13/frankivets-prodavav-informatsiiu-z-baz-danykh-mytnytsi-ta-prykordonnoi-sluzhby-sbu). 13.04.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«В условиях карантина, связанного с пандемией коронавирусной инфекции (COVID-19), существенно возросла популярность сервисов для общения и конференцсвязи, таких, как Zoom. В связи с этим программное обеспечение попало в поле зрения специалистов в области кибербезопасности, выявивших в нем ряд уязвимостей и проблем .

Разработчики Zoom решили исправить данную ситуацию и представили новые функции, направленные на повышение уровня безопасности во время проведения видеоконференций. Теперь для всех пользователей сервиса с бесплатной лицензией, включая учетные записи образовательных учреждений, по умолчанию будет включена функция «комнаты ожидания». Туда будут попадать все участники, прежде чем владелец сеанса предоставит им доступ к видеоконференции.

Все видеоконференции и вебинары в Zoom будут теперь требовать от пользователей ввести пароль для входа. Новые функции будут реализованы по умолчанию, но пользователи смогут по желанию изменить их в web-версии приложения или при планировании нового события». ***(Zoom представила новые***

настройки безопасности // SecurityLab.ru (https://www.securitylab.ru/news/506465.php). 07.04.2020).

***

«Эксперты компании Check Point подсчитали, что количество кибератак, связанных с коронавирусом, продолжает расти, а также в два раза участились атаки сайтов, выдающих себя за сервисы Netflix.

Исследователи рассказывают, что общее количество кибератак снизилось после начала пандемии коронавируса и последующего экономического спада. Однако число атак, связанных с COIVD-19, на этом фоне сильно возросло.

В период с января по март 2020 года исследователи зафиксировала ежемесячное снижение хакерских атак на организации на 17% по всему миру. Однако с середины февраля наблюдается значительный рост числа атак, связанных с коронавирусом. Так, только за последние две недели их число резко возросло с нескольких сотен до более чем 5 000 в день. В среднем ежедневно совершается более 2 600 атак.

Потенциально вредоносными являются следующие ресурсы:

- сайты с упоминанием в домене слов «corona» или «covid»;
- файлы, названия которых включают слово «corona» или смежные с ним слова;
- файлы, распространённые по электронной почте с упоминанием коронавируса в теме письма.
- 84% всех атак были спровоцированы фишинговыми сайтами. Примерно в 2% случаев переход на вредоносный сайт осуществлялся с мобильного устройства.

За последние две недели было зарегистрировано более 30 103 новых доменов, связанных с темой коронавируса, из них 0,4% (131) были признаны вредоносными, 9% (2 777) — подозрительными. Таким образом, с января 2020 года в общей сложности зарегистрировано более 51 000 доменов, связанных с коронавирусом.

Также пандемия и всеобщий переход на удаленку привели к росту числа подписчиков Netflix, что, в свою очередь, вызвало интерес к стриминговой платформе со стороны мошенников. За последние две недели наблюдается двукратное увеличение фишинговых атак со стороны сайтов, выдающих себя за оригинальные ресурсы Netflix. На некоторых из этих сайтов мошенники устанавливают платежные системы, чтобы обманным путем получить деньги и личные данные пользователей.

«Очевидно, что значительный рост числа кибератак связан с активным распространением новостей о коронавирусе во всем мире. В связи с тем, что сейчас большое количество людей вынуждено работать из дома, мошенники сместили свой фокус внимания с крупного бизнеса на частных пользователей. В результате мы наблюдаем учащение вредоносных атак на таких ресурсах, как Zoom или Netflix, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Чтобы не стать очередной жертвой кибермошенников, крайне важно проявлять повышенную осторожность и

внимательность. Особенно это касается подозрительных сайтов, ссылок или же файлов, полученных по почтовой рассылке».

Специалисты Check Point советуют придерживаться следующих рекомендаций по безопасному поведению в интернете, чтобы не стать жертвой онлайн-мошенничества:

- Обращайте внимание на орфографические ошибки в названиях сайтов и в почтовых рассылках.
- Будьте осторожны с файлами, полученными по электронной почте от неизвестных отправителей, особенно если при их открытии вас просят осуществить нетипичное действие.
- Убедитесь, что вы заказываете товары из официального магазина. Один из способов это сделать — не переходить по ссылкам с рекламой из электронных писем, а найти нужную компанию в Google или Яндекс и перейти по ссылке на странице с результатами поиска.
- Остерегайтесь «специальных предложений». К примеру, предложение «эксклюзивного лекарства от коронавируса за 12 000 рублей» должно вызывать сомнение.
- Убедитесь, что вы используете разные пароли для каждого приложения и каждой учетной записи.» ***(Мария Нефёдова. Check Point: число «коронавирусных» кибератак выросло до 5 000 в день // Xakep (https://xakep.ru/2020/04/03/coivd-19-cyberattacks/). 03.04.2020).***

***

«Бен Булпет, директор EMEA, SailPoint, рассказывает о том, как Coronavirus усиливает проблему кибербезопасности во время «гибкой рабочей революции»

В настоящее время большинство из нас должны следовать советам правительства по работе на дому и придерживаться «стратегии социального дистанцирования». Эту политику должны проводить большинство правительственных ведомств в эти беспрецедентные времена.

Но даже когда все возвращается на круги своя, мы должны найти государственный сектор в качестве «гибкого» дружественного рабочего места для своих сотрудников. Одним из преимуществ карьеры местного и центрального правительства является готовность предоставить сотрудникам разнообразные потребности и требования, что обязательно приводит к гибкой рабочей практике…

Более 1,54 миллиона человек, как правило, уже работают дома из Великобритании - это в два раза больше, чем десять лет назад. Би-би-си обнаружила, что количество людей, работающих в разных местах, увеличилось, но их домом стала база. Это число увеличилось примерно на 200 000 за 10 лет с 2008 по 2018 год до 2,66 миллиона…

Во многих отношениях практика домашнего труда более укоренилась в частном секторе. Apple, Google и Amazon - последние технологические гиганты, которые попросили своих сотрудников держаться подальше от офиса и работать дома…

Персонал также может работать с растущим числом общественных мест, в том числе кафе, библиотек или рабочих мест совместного размещения. Но работать удаленно или из дома далеко не так безопасно, как в офисе. Требуется гораздо больше подготовки для координации действий сотрудников и обеспечения того, чтобы системы могли поддерживать критическую массу сотрудников, работающих удаленно, в любой момент.

Весь этот дополнительный спрос на удаленные рабочие места напрягает существующую офисную и телекоммуникационную инфраструктуру. В офисной среде наличие сотен, если не тысяч дополнительных домашних работников будет проверять возможности сервера организации и ее пропускную способность VPN. Это также отвлечет время и внимание ИТ-специалистов от потенциальных угроз кибербезопасности…

В более общем плане, для тех работников, которые находятся дома, в кафе и в рабочих местах, вопрос, который им нужно задать, это: «Насколько безопасна Wi-Fi-связь, с которой я работаю?». Теперь они зависят от сторонней службы, и кто знает, кто сидит за соседним столом или напротив киоска, чтобы отследить их электронную почту. Это дает злоумышленникам и хакерам возможность доступа к критически важным данным государственного сектора…

Самой легкой точкой входа в любую организацию являются их пользователи, в том числе сотрудники, подрядчики, виртуальные рабочие, фрилансеры, боты и контингент сотрудников. Закаленный периметр безопасности больше не существует. Сейчас мы находимся в мире без периметра, где каждый может получить доступ к чему угодно из любого места.

Это заставляет компании придерживаться подхода «нулевого доверия» к постоянно расширяющейся поверхности кибератак. Это идеальное время, чтобы обратиться к «идентичности» как к решению, особенно в сочетании с мощными инструментами искусственного интеллекта (AI) и машинного обучения (ML).

Теперь доступ должен основываться на защите корпоративных систем в ядре и предоставлении привилегированных прав доступа только наиболее защищенному персоналу. Инструменты AI и ML могут определять шаблоны, основанные на предыдущей истории использования, для предупреждения о подозрительном поведении. Новейшие решения для идентификации могут предоставлять оповещения о геолокации, если пользователь отправляет электронное письмо из Бразилии, но, как предполагается, находится в Бейзингстоке, например. Или распознать ненормальный доступ или действия загрузки, которые не являются типичными для данной роли или отдельного человека.

Но для того, чтобы государственный сектор прошел успешную цифровую революцию, он должен начинаться с безопасности и управления идентификацией. Как только этот фонд будет создан, и они смогут все видеть, управлять всем и расширять возможности каждого в своей организации, они смогут сосредоточиться на более фундаментальных изменениях в бизнесе, которые должны произойти.

Пора государственным организациям начать использовать правильные инструменты для работы. Основная задача любого ИТ-специалиста - защитить свою организацию и ее персонал от нарушений кибербезопасности. Это круглосуточная операция, так как хакеры никогда не спят. Задачей ИТ-менеджера

является обеспечение того, чтобы их сотрудники, их организация, и особенно исполнительный директор, могли легко отдыхать, не беспокоясь о том, что их ИТ-система будет работать ночью…» ***(The issue of cybersecurity when taking work to the home // Open Access Government (https://www.openaccessgovernment.org/issue-of-cybersecurity-work-home/85023/). 07.04.2020).***

***

«За последний месяц количество вредоносных кампаний, которые каким-либо образом эксплуатируют тему COVID-19, увеличивается со скоростью лесного пожара. Так, вредоносные домены, посвященные коронавирусу уже исчисляются десятками тысяч, и даже взломанные роутеры пугают своих владельцев именно срочной информацией о пандемии.

Теперь эксперты заметили малварь, целенаправленно уничтожающую данные пострадавших пользователей и перезаписывающую MBR (Master Boot Record), что препятствует нормальному запуску системы.

…в общей сложности им удалось выявить четыре штамма подобных вайперов (wiper, от английского to wipe — «стирать»), которые объединяет эксплуатация темы коронавируса, а также ориентированность на уничтожение информации, а не на финансовую выгоду. Из четырех образцов малвари, обнаруженных ИБ-исследователями в прошлом месяце, наиболее продвинутыми оказались два, переписывающие MBR.

Так, первый вайпер был обнаружен MalwareHunterTeam и подробно описан в отчете компании SonicWall на этой неделе. Эта малварь распространяется как файл COVID-19.exe и имеет два этапа заражения.

На первом этапе вредонос просто демонстрирует раздражающее окно, которое пользователи не могут закрыть, так как малварь уже отключила диспетчер задач Windows. Но пока пользователи пытаются разобраться с окном, малварь повреждает MBR, а затем перезагружает ПК. В итоге пользователь оказывается блокирован, а система не загружается дальше экрана предварительной загрузки.

К счастью, в данном случае восстановить доступ к машине и данным возможно, хотя для этого понадобится специальный софт для восстановления MBR.

Второй штамм «коронавирусной» малвари тоже перезаписывает MBR, но выглядит уже более сложным. На первый взгляд, это лишь очередной вымогатель с названием CoronaVirus, однако это лишь прикрытие. Основная функция этой малвари — хищение паролей с зараженного хоста, а затем имитация вымогательской деятельности, призванная скрыть от жертвы реальное положение дел.

Дело в том, что как только CoronaVirus похитил данные жертвы, он перезаписывает MBR и тем самым блокирует систему пользователя, фактически лишая жертву доступа к ПК. Так как на этом этапе пользователь видит сообщение с требованием выкупа и информацию о том, что его данные зашифрованы, вряд ли ему сразу придет в голову, что нужно проверить, не похитил ли кто-нибудь пароли от приложений.

Согласно анализу компании SentinelOne, ИБ-эксперта Виталия Кремеза и издания Bleeping Computer, данная малварь также содержит код для стирания файлов с машины жертвы, однако на момент изучения вредоноса этот код не был активен.

Вторая версия этой же угрозы была замечена экспертом компании G DATA Карстеном Ханом две недели спустя. Малварь сохранила возможность перезаписи MBR, однако заменила неактивную функцию стирания данных на работающий блокировщик экрана.

Но если вышеописанные угрозы лишь повреждали MBR и не уничтожали данные на зараженной машине, то два другие вредоноса, найденные MalwareHunterTeam, занимаются именно этим.

Первый вайпер был замечен еще в феврале текущего года. Судя по имени файла на китайском языке, он предназначался для китайских пользователей, хотя у исследователей и ZDNet нет точных данных о том, распространялась ли эта малварь в реальности или была лишь тестовой версией. Второй вайпер был обнаружен на этой неделе: кто-то из Италии загрузил образец вредоноса на VirusTotal.

MalwareHunterTeam описывает обе угрозы как весьма слабые вайперы, имея в виду используемые ими методы удаления файлов — неэффективные, подверженные ошибкам и трудоемкие. Впрочем, оба вредоноса работают и действительно уничтожают данные своих жертв, хотя эксперт не уверен, являются они чьей-то шуткой или же создавались как вполне серьезная малварь». ***(Мария Нефёдова. Обнаружены вайперы, эксплуатирующие тему COVID-19 и перезаписывающие MBR // Xakep (https://xakep.ru/2020/04/03/covid-wipers/). 03.04.2020).***

***

«Вымогатели из киберпреступной группировки REvil атаковали калифорнийскую биотехнологическую компанию, занимающуюся исследованием лекарств от коронавирусной инфекции (COVID-19).

Как сообщается в документе Комиссии по ценным бумагам и биржам США, компания 10x Genomics стала жертвой атаки с использованием вымогательского ПО, в ходе которой были похищены конфиденциальные данные.

После атаки вымогатели опубликовали в Сети документы компании с информацией о более чем 1200 сотрудниках и ее внутренних компьютерных системах. По заявлению преступников, они похитили терабайт информации у компании 10x Genomics. Фирма восстановила нормальную работу «без существенных последствий» и заявила, что работает с правоохранительными органами для расследования инцидента.

В настоящее время компания является частью международного альянса, занимающегося секвенированием клеток выздоровевших от COVID-19 пациентов в рамках попытки изучить возможные способы лечения данной болезни». ***(Группировка REvil похитила терабайт данных у биотехнологической компании // SecurityLab.ru (https://www.securitylab.ru/news/506381.php). 03.04.2020).***

***

«Группа европейских ученых и специалистов в области цифровых технологий под руководством экспертов Института Фраунгофера по телекоммуникациям (Fraunhofer Heinrich Hertz Institute for telecoms, HHI) в Германии работают над технологией отслеживания близких контактов с инфицированными COVID-19, не нарушающей законы Евросоюза о защите данных.

Проект Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) является ответом специалистов на растущий спрос со стороны властей на данные местоположения пользователей. Однако, в отличие от других приложений для отслеживания возможных контактов с инфицированными людьми, PEPP-PT использует подход, «полностью сохраняющий конфиденциальность», уверяют специалисты.

Идея заключается в использовании смартфонов для предотвращения следующей волны заражений коронавирусом. Пользователи, тесно контактировавшие с инфицированным человеком, будут получать предупреждения через прокси смартфонов, находящихся достаточно близко друг к другу для сопряжения по Bluetooth. Однако авторы проекта намерены приложить все усилия для того, чтобы не допустить использования в ЕС китайского сценария, когда власти следят за местоположением каждого гражданина через его смартфон.

В Европе не будет какого-то единого приложения для отслеживания распространения коронавируса. Уже сейчас таких приложений есть несколько. Авторы PEPP-PT предлагают правительствам стран и разработчикам набор «стандартов, технологий и услуг», а также стандартизированный подход к отслеживанию контактов с зараженными COVID-19 по всему ЕС.

«PEPP-PR полностью соответствует строгим европейским законам и принципам защиты конфиденциальности данных. Идея состоит в том, чтобы сделать технологию доступной как можно большему количеству стран, руководителям служб реагирования на инфекционные заболевания и разработчикам. Предоставляемые PEPP-PT технические механизмы и стандарты полностью защищают конфиденциальность пользователей и при этом используют возможности цифровых технологий для максимизации скорости и возможностей реагирования властей на пандемию», - пояснили авторы проекта». ***(В ЕС работают над стандартом для отслеживания контактов с больными COVID-19 // SecurityLab.ru (https://www.securitylab.ru/news/506370.php). 02.04.2020).***

***

«Компания Eset обнаружила новые виды кибермошенничества, появившиеся на фоне пандемии коронавируса и перехода большинства предприятий на режим удаленного офиса. Злоумышленники становятся все более изобретательными, и распознать их действия не всегда под силу даже продвинутому пользователю.

Киберпреступники продолжают распространять фейковые сообщения «с актуальной и достоверной информацией о COVID-19». Эксперты Eset выяснили,

что одна из таких рассылок нацелена на распространение трояна, похищающего данные. Вредоносный файл находился в приложении к письму под видом документа, в котором якобы содержались секретные сведения о том, как избежать заражения.

Цель следующего вида атак – компании, оказавшиеся в сложной финансовой ситуации в результате экономического кризиса на фоне пандемии. Сегодня многие предприятия как никогда нуждаются в новых источниках дохода. Этим пользуются мошенники, которые делают рассылки со срочными заказами и прикладывают к письмам зараженные файлы под видом сопроводительных документов. Таким образом, вредонос может попасть в корпоративную сеть.

Ссылаясь на то, что работа финансовых учреждений замедлена из-за пандемии, мошенники отправляют вредоносный файл под видом гарантии оплаты (например, выписки с банковского счета), вынуждая пользователя открыть его.

Растущий спрос на медицинские маски продолжает становиться причиной фишинговых атак. Обнаружен сайт, выманивающий данные пользователей при помощи объявлений о продаже масок OxyBreath Pro с большой скидкой.

Пользователи сами передают мошенникам платежную информацию, в том числе номер кредитной карты и CVV.

Эксперты Eset полагают, что количество подобных кибератак будет расти, а сами они – становиться еще сложнее и опаснее. Рекомендуется соблюдать фундаментальные правила информационной безопасности: не открывать письма от незнакомых отправителей, искать информацию о пандемии только на официальных ресурсах (ВОЗ и локальных организаций здравоохранения). Снизить киберриски поможет использование комплексных антивирусных решений с дополнительными модулями.» ***(«Антифишинг» и фильтрация e-mail) как в корпоративной сети, так и в домашней. (Новые виды кибермошеничества на фоне пандемии коронавируса // Компьютерное Обозрение (https://ko.com.ua/moshenniki_aktivno_ispolzuyut_temu_koronavirusa_vo_vredonosnyh_kampaniyah_132538). 07.04.2020).***

***

«Кіберзлочинці у більшості країн світу, використовуючи панічні настрої серед громадян у період пандемії, здійснюють фішинг-атаки з використанням шкідливого програмного забезпечення. Їх метою є отримання персональних даних користувачів мережі, а саме логінів та паролів доступу до різних інтернет-ресурсів: електронних поштових скриньок, облікових записів соціальних мереж, електронних гаманців тощо для подальшого привласнення грошей.

Хакери замаскували свої атаки під інформування громадян про розвиток пандемії. Найчастіше, аби ввести в оману, вони використовують у своїх фішинг-розсилках посиланням на слово “Corona”, а також розповсюджують шкідливе програмне забезпечення шляхом копіювання інформаційних панелей організацій, що надають актуальну інформацію про COVID-19.

У зв’язку з цим, кіберполіція радить:

— використовувати виключно ліцензійне програмне забезпечення;

— постійно оновлювати операційну систему;

— використовувати ліцензійні антивірусні програми з актуальними базами та постійно оновлювати їх;

— не завантажувати підозрілі файли із листів електронної пошти, якщо Ви не чекаєте цей лист;

— не переходити за сумнівними посиланнями;

— завантажувати файли лише з перевірених ресурсів.» ***(Кіберполіція попереджає про активізацію хакерів в період карантину // Баба Клава дает добро (https://blin.mk.ua/news/124285). 07.04.2020).***

***

«Киберспециалисты Службы безопасности Украины пресекли деятельность ботофермы, через которую злоумышленники распространяли фейки о COVID-19 и призывали к свержению конституционного строя. Руководили их деятельностью из Российской Федерации, оборудование организаторы развернули в одном из бизнес-центров Днепра. Об этом информирует пресс-центр ведомства.

Сотрудники спецслужбы установили, что ботоферма создавала и управляла учетными записями в соцсетях, которые, якобы, принадлежали гражданам Украины, хотя на самом деле использовали фейковые персональные данные. Мощность «фермы» — более 5000 ботов.

Соответствующее телекоммуникационное оборудование и специализированное программное обеспечение организаторы приобрели через запрещенные в Украине российские небанковские платежные системы. Они использовали также SIM-карты украинских операторов связи и proxy-серверы отечественного сегмента Интернет.

Анализ контента, который распространяла ботоферма, обнаружил публичные призывы к насильственному изменению конституционного строя и захвату государственной власти. Кроме того, боты распространяли ложную информацию о ситуации в Украине, возникшей из-за пандемии COVID-19.

Следователями СБУ начато уголовное производство по ст. 109 Уголовного кодекса Украины. Под процессуальным руководством прокуратуры Днепропетровской области проведены обыски и изъято оборудование, которое использовали злоумышленники. Продолжается следствие.

С начала карантина Служба безопасности Украины разоблачила две управляемые из РФ ботофермы в Киеве и в Днепре. Деятельность 7 интернет-агитаторов, действовавших по заданию российской стороны, расследуется в рамках уголовных производств, начатых следователями СБУ по статьям 109 (действия, направленные на насильственное изменение или свержение конституционного строя или на захват государственной власти) и 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины». ***(СБУ разоблачила ботоферму, через которую распространяли фейки о COVID-19 и призывы к свержению конституционного строя // Волнорез (http://volnorez.com.ua/novosti/sbu-razoblachila-botofermu-cherez-kotoruyu-rasprostranyali-fejki-o-covid-19-i-prizyvy-k-sverzheniyu-konstitucionnogo-stroya.html). 06.04.2020).***

***

«Во время пандемии, когда все сидят по домам в интернете, активизировались злоумышленники. Так, по данным Atlas VPN, в марте мошенники создали более 35,5 тысяч уникальных сайтов, связанных с COVID-19. Здесь они пытались обмануть потребителей, чтобы выручить деньги, продавая маски, дезинфицирующие средства для рук или даже наборы для тестирования на вирусы. Участились случаи вымогательства под шумок и в Украине.

Из-за резкого повышения цен Amazon удалил более 530 тысяч размещенных продуктов, связанных с коронавирусом, а также заблокировал или удалил более 1 миллиона вводящих в заблуждение позиций товаров.

Один из последних примеров киберпреступлений – инсталляция вредоносного программного обеспечения с вирусами на компьютеры пользователей через карты распространения коронавируса. Таким образом считываются пароли и другие данные доступа, которые преступники могут использовать в своих целях.

Как, сидя дома на карантине, нам не стать жертвами киберзлодеев?

“Это такая активность, которая происходит при любых поводах. Злоумышленники используют разные поводы, страхи людей, чего они желают. Это вечная халява получить какие-то деньги. Если раньше это были нигерийские письма, то сейчас коронавирус, - говорит Константин Корсун, директор Berezha Security. - Как с этим бороться или противостоять? Как всегда, изменился лишь повод. Механика мошеннических действий осталась та же самая. Это побуждение пользователя перейти на определенный мошеннический ресурс. Поэтому рекомендации такие же, как и до того, как и будут еще. Необходимо сомневаться и проверять информацию, особенно если предлагается что-либо бесплатно, надо проверять источники, проверять хотя бы информацию из двух, а лучше трех независимых источников”.

“Естественно, мошенники пользуются инфоповодом (всегда так делают), и более того, так как многие люди в связи с карантином начали работать из дому, это создаёт дополнительные риски - дома у вас нет администраторов и службы безопасности, чтобы присматривать за сетью и компьютером, и во многих организациях ослаблены правила безопасности, чтобы сотрудники вообще смогли добраться до необходимых им материалов и сервисов”, - отмечает Шон Таунсенд, пресс-секретарь Украинского кибер-альянса.

Обращайте внимание: если предлагается передать банковскую информацию, то наверняка это мошенники. Необходимо сразу же закрывать данную страницу, а лучше сообщить в киберполицию.

С продолжением карантина снизилась деловая активность, многие бизнес-процессы перешли в интернет. В то же время у людей элементарно заканчиваются деньги, и на этом фоне активизируется и киберпреступность. Поэтому не стоит ожидать снижения мошеннических проектов в будущем, а наоборот волны их нарастания.

“Чем больше людей используют современные технологии для работы и общения, так же пропорционально будет развиваться и киберпреступность. Если многие компании и предприятия перешли на удаленный доступ, преступники этим безусловно пользуются. Далеко не все компании к этому готовы, многие из них используют небезопасные или непроверенные на безопасность сервисы, - рассказывает Константин Корсун. - Мошенникам становится доступным корпоративный трафик, и они могут легче попасть в закрытые сети компаний, получать коммерческую информацию. Это как доступ к дистанционному банковскому обслуживанию с целью ворования средств, так и для распространения фейков, паники, дезинформации. Но подавляющее количество киберпреступников хотят денег, поэтому они будут стараться полученную информацию каким-либо образом монетизировать. Это как доступ к банковским счетам, так и промышленный шпионаж, продажа секретов, шантаж сотрудников, выманивание личных средств и т.д.”.

“Киберугрозы появляются быстрее, чем полноценная защита. Здесь больше стоит думать о комплексных решениях защиты критических ИТ-инфраструктур и данных бизнеса, что требует времени, знаний ИТ-персонала и финансовых ресурсов. Однако необходимо соблюдать минимальные простые, как и мытье рук в реальной жизни, требования по кибергигиене”, - подчеркивает Артур Филатов, эксперт по кибербезопасности компании Tet…». ***(Герман Богапов. Как уберечься от киберп реступников в период карантина // Internetua (https://internetua.com/kak-uberecssya-ot-kiberprestupnikov-v-period-karantina). 03.04.2020).***

***

«Когда хакеры взломали компьютеры в лондонской компании Hammersmith Medicines Reseao rch, которая проводит клинические испытания новых лекарств, для управляющего директора Малкольма Бойса это стало кошмаром.

Кризис коронавируса только начинал распространяться в Великобритании, и компания вела переговоры с другими фирмами о возможном тестировании вакцины. Хакеры использовали шифрование, чтобы заблокировать тысячи записей пациентов, и пообещали опубликовать их в Интернете, если выкуп не будет уплачен.

Вместо этого Бойс вызвал полицию, а ИТ-персонал его компании работал круглосуточно, чтобы попытаться смягчить ущерб.

«Мы усилили нашу защиту с момента атаки на всех видах программного обеспечения», - сказал Бойс, добавив, что его компания теперь работает нормально после временных трудностей. «Я обращаюсь к другим компаниям с призывом сделать все возможное, чтобы обезопасить себя, потому что они вполне способны вывести вас из бизнеса, и совершенно не имеют совести».

В то время, когда медицинские учреждения по всему миру изо всех сил пытаются справиться с наплывом пациентов, страдающих от Covid-19, компании-поставщики медицинских услуг и медицинские учреждения в США и Европе, пережили всплеск атак вирусов-вымогателей. По словам нескольких экспертов по

кибербезопасности, преступники стремятся использовать кризис, чтобы поразить медицинский сектор, когда он находится в самом отчаянном положении.

«В настоящее время мы наблюдали ряд случаев, когда клинические лаборатории, занимающиеся тестированием, или крупные больницы, подвергались атакам вирусов-вымогателей, в реузльтате чего все их ИТ-системы были остановлены», - сказал Андре Пиенаар, основатель венчурной компании C5 Capital. C5 создал альянс компаний по кибербезопасности, который предоставляет бесплатную помощь больницам и клиникам в Великобритании и Европе.

Несколько атак, по словам Пиенаара, имели место в Великобритании и других странах Европы и были связаны с организованным преступным синдикатом, который использует вирус-вымогатель, известный как Maze.

В настоящее время эксперты по кибербезопасности со всего мира объединяются для противодействия хакерским атакам на мед.учреждения в период кризиса COVID-19.

Европол, правоохранительный орган ЕС, получил сообщения об усилении кибератак почти во всех своих 27 странах-членах, по словам пресс-секретаря Яна Оп Ген Уорта.

«Мы видели, как организованная преступность быстро воспользовалась распространением коронавируса», - сказал Оп Ген Уорт. «Увеличивается число атак с использованием вредоносных программ и программ-вымогателей, стремящихся извлечь выгоду из этого глобального кризиса».

В США Билл Сигел, исполнительный директор Coveware, который помогает компаниям, пострадавшим от атак вымогателей, сказал, что он работал с примерно полдюжиной поставщиков медицинских услуг, которые пострадали от вымогателей во время кризиса Covid-19.

По его словам, организации, которые были взломаны самые разные, включая больницы, медицинские лаборатории, небольшой педиатрический кабинет и городской центр помощи. Он отказался назвать их, сославшись на соглашения о конфиденциальности.

По словам Сигеля, атака на поставщика медицинских услуг блокирует компьютеры, которые обычно содержат электронные медицинские карты, а это означает, что врачи и медсестры не могут получить доступ к информации об истории болезни своих пациентов, дозировкам лекарств, которые требуются пациентам, и другой важной информации.

По словам Сигеля, последствия такого нападения, особенно во время вспышки пандемии, могут быть разрушительными. В случае блокировки ИТ-систем больницы, на которую осуществляется атака, «жертвы, которые иначе не произошли бы, являются вероятным результатом из-за атаки киберпреступников», - говорит он.

Ransomware - это тип вредоносного ПО, которое шифрует файлы на компьютерах жертвы, делая содержащиеся в них данные недоступными, пока выкуп за ключ дешифрования не будет выплачен. Суммы выкупа варьируются, хотя Пиенаар сказал, что он видел «огромную инфляцию» в требованиях выкупа за последние два месяца.

Во многих случаях, по его словам, выкупы оплачиваются, потому что организации здравоохранения находятся в условиях ограниченного времени и давления - именно на это и рассчитывают хакеры.

Атаки вирусов-вымогателей происходят на фоне роста других кибератак, связанных с пандемией. Они включают в себя множество «фишинговых» электронных писем, которые пытаются использовать кризис, чтобы убедить людей нажимать на ссылки, загружающие вредоносное или вымогательское ПО на свои компьютеры.

Джон Фитцпатрик, директор HPCsec, лондонской компании по кибербезопасности, создал инструмент для мониторинга создания подозрительных доменов веб-сайтов, связанных с коронавирусом.

По результатам отслеживания за четырехдневный период с 19 по 23 марта, Фитцпатрик выявил более 650 доменных имен, многие из которых, по его словам, «весьма вероятно» были связаны с всплеском фишинговых сообщений.

Больницы и медицинские учреждения были объектами хакеров и вымогателей в течение многих лет, отчасти из-за хранения конфиденциальной информации о пациентах на компьютерах и недостатков в кибербезопасности.

В 2017-м десятки больниц и мед.учреждений пострадали от вымогателей, известных как WannaCry, что привело к тысячам отмененных встреч и закрытию некоторых отделений скорой и неотложной помощи.

В 2019-м нескольким больницам США пришлось отказаться от пациентов после очередной серии атак с использованием вирусов-вымогателей. Эксперты считают, что глобальная пандемия только усилила уязвимость мед. учреждений.

«Злоумышленники знают, что в настоящий момент эти организации так отчаянно пытаются создать аппараты для ИВЛ или не дать людям заболеть, что у них порой нет времени на заботу о кибербезопасности», - сказал Малколм Тейлор, глава отдела кибербезопасности в ITC Secure, одной из компаний, которые является частью альянса C5 Capital по оказанию помощи медицинским учреждениям и исследовательским лабораториям.

Например, в начале месяца в Чехии университетская больница Брно подверглась кибератаке, которая вынудила выключить все компьютеры, отменить операции и переместить пациентов.

Больница, которая является второй по величине в Чехии, проводила тесты на наличие коронавируса. По словам представителя больницы, некоторые результаты теста были отложены из-за инцидента.

Роберт Кахофер, глава кабинета чешского агентства кибербезопасности NUKIB, сказал, что его команда в настоящее время работает над восстановлением работоспособности компьютеров больницы. Он отказался уточнить, сославшись на продолжающееся полицейское расследование.

В Калифорнии биотехнологическая компания 10x Genomics, похоже, недавно также подверглась нападению.

Компания, которая разрабатывает оборудование для секвенирования генов, используемое в научных исследованиях, предоставляет технологию Университетскому медицинскому центру Вандербильта, которая изучает

иммунную систему для использования при разработке потенциальной терапии антителами для Covid-19.

13 марта группа хакеров с использованием вирусов-вымогателей, известная как REvil, опубликовала внутренний документ компании из 10x Genomics онлайн, в где утверждается, что в нем содержится информация о более чем 1200 сотрудников компании и ее внутренних компьютерных системах. Копия документа была замечена Bloomberg News.

Группа заявила, что украла терабайт информации из 10x Genomics. Исследователь по безопасности из израильской компании Under The Breach, занимающейся мониторингом утечки данных, сказал, что 10x Genomics «довольно сильно скомпрометированы». Исследователь заявил об этом анонимно, боясь мести со стороны преступников.

10x Genomics пока не комментирует ситуацию.

Некоторые группы хакеров пообещали не наносить удары по больницам и другим поставщикам медицинских услуг, пока продолжается коронавирус. Но эксперты по безопасности говорят, что хакерам не стоит доверять.

«Это полностью ложно», - сказал Сигел из Coveware. «Мы видели, что почти каждый из них недавно имел целью атаки организацию здравоохранения». ***(Романов Роман. Медицинские учреждения наиболее уязвимы для хакерских атак в период пандемии // Internetua (https://internetua.com/medicinskie-ucsrejdeniya-naibolee-uyazvimy-dlya-hakerskih-atak-v-period-pandemii). 01.04.2020).***

***

«Почти три недели назад миллионы людей по всему миру перешли на работу из дома. В их числе оказались и более 100.000 сотрудников «Сименс». «Сименс» и 16 других международных компаний, присоединившихся к инициативе «Хартия доверия», разработали восемь решений для повышения уровня кибербезопасности, чтобы люди могли продолжать работать из дома с тем же уровнем защиты, что и в офисе.

Их рекомендации призваны помочь компаниям оградить себя от хакерских атак и обеспечить бесперебойную работу. Сюда вошли самые разные решения: от отключения устройств с функцией управления голосом и заклеивания веб-камер до отказа от использования офисных устройств в личных целях.

«В сложившейся кризисной ситуации крупные предприятия должны проявить особую ответственность, – считает Президент и Председатель Правления «Сименс АГ» Джо Кэзер. – Эти обязательства также подразумевают оказание поддержки другим компаниям, совместную разработку решений и обмен знаниями на благо всех нас. Именно эти принципы стали основными для членов инициативы «Хартия доверия» в последние два года».

COVID-19 не только представляет серьезную опасность для здоровья, но и повышает риски в области кибербезопасности для многих компаний. Чтобы сократить вероятность заражения, практически весь персонал переведен на дистанционную работу. Сотрудникам все чаще приходится обмениваться конфиденциальными данными из дома, чтобы не допустить операционных простоев. В одной лишь компании «Сименс» с середины марта к корпоративному

Интранету из дома подключаются около 130.000 сотрудников по всему миру, что в четыре раза превышает норму.

Однако, как правило, ИТ инфраструктура в домашних условиях не гарантирует безопасности на том же уровне, что и в офисе. Хакеры все чаще пользуются этой уязвимостью. В этой ситуации роль сотрудника как ответственного за обеспечение кибербезопасности возрастает. Партнеры «Хартии доверия» предлагают восемь рекомендаций, призванных оградить пользователей от хакерских атак:

• Забирайте домой только те устройства и информацию, которые вам необходимы.

• Не забывайте о защите домашней сети и пользуйтесь только защищенными подключениями.

• Регулярно обновляйте ПО на всех устройствах до актуальной версии.

• Отключите функцию управления голосом на смартфонах и планшетах на домашнем рабочем месте и заклейте камеру, если вы ей не пользуетесь.

• Не используйте офисные устройства в личных целях.

• Заранее проверяйте имена всех участников в онлайн-конференциях.

• Выходите из учетной записи на устройствах, которые вам не нужны, и организуйте их безопасное хранение.

• С особым вниманием относитесь к подозрительным электронным письмам или вложениям, особенно если отправитель вам не знаком.

Чтобы большое количество сотрудников могли подключиться к корпоративной сети «Сименс» из дома максимально безопасно, ИТ-эксперты компании предприняли соответствующие меры еще в середине марта, в самом начале сложившейся кризисной ситуации. За 24 часа они организовали стабильное подключение к Интранету приблизительно для 140.000 сотрудников, тем самым обеспечив уровень кибербезопасности, сопоставимый с офисным». ***(«Сименс» и 16 других международных компаний обеспечили кибербезопасность дистанционной работы // IKSMEDIA.RU (http://www.iksmedia.ru/news/5656409-Simens-i-16-drugix-mezhdunarodnyx.html). 08.04.2020).***

***

«Trend Micro опубликовала свежие данные о киберугрозах, приобретающих наиболее заметное распространение в период пандемии коронавируса COVID-19 и связанного с ней карантина. Как и любой кризис мирового масштаба, текущая ситуация привлекла внимание киберпреступников, которые используют её для распространения своего вредоносного ПО и атак на коммерческие структуры и пользователей.

Trend Micro выделяет три основных типа атак, которые хакеры пытаются проводить, используя в качестве приманки важную информацию и сайты о коронавирусе, сообщения в электронной почте и файлы с данными. Спам в этом списке занимает первое место — на него приходится 65,7% атак, на втором месте находятся атаки с применением вредоносного ПО, включая трояны и программы-вымогатели (с 26,8%); на третьем месте по частоте выявления (7,5%) вредоносные URL и сайты.

Карта киберугроз в условиях пандемии коронавируса, информация взята из исследования Trend Micro

Наибольшее количество спама с упоминанием коронавируса — почти 200 000 писем — за период исследования было выявлено в Великобритании (20,8%), Франции (11,5%) и США (8,2%). Стоит отметить, что из-за перехода на удалённую работу в период карантина также участились случаи компрометации корпоративной переписки (BEC-атаки), в рамках которых злоумышленники направляют сотрудникам письма якобы от руководства и требуют перечислить средства на принадлежащие им счета.

Первыми в списке стран с наибольшим количеством обнаруженных файлов с вредоносным содержимым и названиями, включающими слова «covid» или «covid19», стали США (26,6%), Франция (12,2%) и Канада (11,2%). Всего было обнаружено более 81 000 таких файлов. Особой популярностью начинают пользоваться программы-вымогатели, которые в период пандемии могут нанести гораздо больший ущерб, особенно если заражённой окажется инфраструктура медицинских учреждений или лабораторий, проводящих тестирование на коронавирус.

Вредоносные URL, обнаруженные Trend Micro, в основном относятся к трём категориям. В первую очередь злоумышленники используют их для фишинга — таких ссылок пользователи получают более 56,7%. Ещё 34,3% ведут на скачиваемое вредоносное ПО, а 7,5% — на страницы с мошенническими схемами, например, на поддельные сайты различных благотворительных организаций, собирающих средства на борьбу с коронавирусом. Также подобные ссылки могут вести на сайты с информацией о распространении коронавируса и информационными приложениями, которые заражают систему или мобильные устройства пользователей вредоносным ПО. В этом списке из почти 23 000 выявленных угроз первые места занимают США (26,5%), Германия (13,3%) и Великобритания (10,4%).

Ещё одним распространённым и тревожным трендом становится использование полученной в ходе фишинга информации для шантажа пользователей, которым угрожают уже не публикацией переписки или списка посещённых сайтов, а заражением коронавирусом при личной встрече с ними или их родственниками и друзьями из списка контактов.

В условиях пандемии Trend Micro рекомендует не паниковать и придерживаться стандартных механик защиты сетевой инфраструктуры и использовать многоуровневую защиту, включая системы защиты конечных устройств, электронной почты, файрволы и антивирусные решения.

Trend Micro понимает серьёзность ситуации, поэтому в соответствии с требованиями местных органов власти предоставляет возможность своим сотрудникам работать удалённо, временно приостанавливает все их международные поездки, чтобы свести к минимуму риск заражения, и сохраняет постоянную бдительность. Эти же меры компания рекомендует соблюдать и своим клиентам». ***(Как киберпреступники используют пандемию коронавируса // IKSMEDIA.RU (http://www.iksmedia.ru/news/5656365-Kak-kiberprestupniki-ispolzuyut-pan.html). 08.04.2020).***

***

«Аналитики компании Qrator Labs обнародовали результаты исследования динамики атак и изменений трафика онлайн-ресурсов компаний из различных сфер бизнеса во время в период распространения коронавируса. Отчет был подготовлен на основе статистики, собранной по клиентам Qrator Labs за февраль-март 2020 года.

Распространение COVID-19 по всему миру, а также карантин, в условиях которого оказались многие российские регионы, заметно сказались на характере интернет-трафика: объем трафика многих ресурсов существенно сократился, в то время как интерес аудитории переключился на ряд других сервисов, которые стали испытывать пиковые нагрузки.

По данным экспертов, изменение статистического профиля трафика в рунете носило достаточно плавный характер, обусловленный изменениями в экономике страны и мира.

Основным фактором роста трафика в марте в России стали видеосервисы, включая как известные ресурсы, так и пиратские сайты. Развлекательный контент пользуется сейчас большим спросом у людей, вынужденных постоянно находиться дома: многие смотрят фильмы и сериалы в свободное время, что заметно увеличивает нагрузку на ресурсы компаний, предоставляющих подобные услуги.

Вслед за ростом популярности видеосервисов резко стала расти онлайн-реклама (на 17,92%) – многие смотрят кино на пиратских сайтах, где размещается большое количество рекламных роликов.

Отдельно обращает на себя внимание рост трафика у религиозных сервисов – от 30% до 500%. Возможно, это связано с тем, что многие верующие люди, находящиеся дома, участвуют в службах по видеосвязи, а также активно интересуются взглядом духовенства на происходящее.

Характерно, что трафик туристических компаний, операторов, авиа- и железнодорожных перевозчиков в целом сократился ненамного – на 0,78% – граждане продолжают приобретать и использовать билеты на перелеты и поездки внутри страны, а также, по всей видимости, пытаются вернуть себе деньги на отмененные рейсы и туры, купленные на ближайшее время.

Существенное падение в секторе конкретно туроператоров и туркомпаний в целом компенсируется более интенсивной, чем в феврале, рекламой авиа- и железнодорожных перевозок. Заметный спад отмечается в медицинском секторе — 8,59% — однако стоит заметить, что просадка спроса и, соответственно, трафика в основном коснулась услуг платной косметологической медицины. На 1,70% также упал трафик сайтов недвижимости и на 1,88% – тематических и профессиональных социальных сетей.

Вслед за отменой (или переносом) большинства ключевых спортивных событий — от Олимпиады до автогонок в классе Формула-1 — снизился интерес к сервисам ставок на спорт (- 4,92%), при этом DDoS-атаки на эту категорию бизнеса выросли практически в три раза. Это, по всей видимости, является наглядной иллюстрацией того, как в условиях кризиса и сокращающегося рынка некоторые игроки прибегают в том числе к внерыночным методам конкурентной борьбы.

Аналогичная ситуация на рынке электронной коммерции и онлайн-магазинов — рост числа атак на 183%.

Более агрессивный рост числа атак, по сути, продемонстрировал только сектор онлайн-курсов и сервисов дистанционного обучения (почти в 4 раза). Это легко объясняется агрессивным нежеланием учеников продолжать свое образование в школах и высших учебных заведениях в онлайн-формате. Нагрузка на сайты онлайн-образования при этом увеличилась всего на 2,88%, даже в условиях того, что многие компании сделали свои уроки и программы бесплатными на время эпидемии. Рост трафика в секторе цифрового образования оказался не сравним с ростом развлекательного контента (5,32%).В условиях начавшегося кризиса и роста экономических рисков многие обратили свое внимание на валютные рынки. Вследствие этого сектор криптобирж и Forex продемонстрировал в марте существенный рост (+5,56% и +3,13%, соответственно). Ресурсы микрофинансовых организаций также стали пользоваться повышенным спросом среди населения.

Увеличился трафик кассовых аппаратов. В основном, рост был сконцентрирован в периоде с 1 по 21 марта (до 7%). Во-первых, на этот период пришелся ажиотаж в закупке продуктов первой необходимости; во-вторых, поскольку через наличные деньги может передаваться коронавирус, российские пользователи стали большее количество операций выполнять с помощью банковских карт — что, вероятно, увеличило налоговую нагрузку на ряд магазинов и все еще функционировавший в этом периоде ресторанный бизнес. В последнюю неделю марта трафик кассовых аппаратов снижался, оставаясь при этом по-прежнему выше февральского уровня. Естественным следствием закрытия ресторанов стал также общий спад в сфере купонного бизнеса.» ***(- 5.82%)… (Мария Нефёдова. Qrator Labs изучила DDoS-атаки и изменения трафика во время пандемии коронавируса // Xakep (https://xakep.ru/2020/04/13/corona-traffic/). 13.04.2020).***

***

«По мере распространения пандемии коронавируса растет и число атак, эксплуатирующих данную тему. В столь нелегкое время Управление радиотехнической обороны Австралии (Australian Signals Directorate, ASD) решило ужесточить борьбу с киберпреступниками, пытающимися нажиться на всеобщей проблеме.

Согласно заявлению ASD, в отношении киберпреступников, эксплуатирующих проблему COVID-19, регулятор будет использовать свои наступательные возможности, вплоть до ответных кибератак.

«Киберпреступники, прикрывающиеся киберпространством и международными границами для атак на австралийцев, находятся отнюдь не за пределами нашей досягаемости. Мы наносим ответный удар через Управление радиотехнической обороны, которому уже удалось успешно пресечь деятельность иностранных киберпреступников путем отключения их инфраструктуры и блокировки им доступа к похищенной информации. Некоторые киберпреступники даже выдают себя за представителей органов здравоохранения и пользуются

доверием австралийцев с целью заражения их компьютеров вредоносным ПО и похищения конфиденциальной информации», - сообщила министр обороны Австралии Линда Рэйнольдс.

Как пояснила министр, ASD уже использовало свои наступательные возможности для отключения инфраструктуры, используемой иностранными киберпреступниками.

По мнению главы ASD Рэйчел Нобл, киберпреступники и впредь продолжат эксплуатировать тему COVID-19 для обмана австралийских пользователей. «Мы только начали наступательные кибероперации, и мы продолжим наносить ответные удары по киберпреступникам за рубежом, пытающимся похитить данные и деньги австралийцев», - сообщила Нобл». ***(Австралийские власти контратакуют хакеров, использующих тему COVID-19 // SecurityLab.ru (https://www.securitylab.ru/news/506574.php). 09.04.2020).***

***

«С начала карантина из-за пандемии коронавируса COVID-19 Служба безопасности Украины разоблачила 154 агитаторов, которые в интернете распространяли фейки о коронавирусе. Об этом сообщает пресс-служба СБУ. подписчиков.

Оперативникам СБУ удалось выяснить, что восемь интернет-агитаторов целенаправленно действовали по заданию российской стороны. Такие вражеские агенты работали в Одессе, Днепре, Львове, Херсоне и Киеве. Их деятельность расследуется по статьям 109 и 110 Уголовного кодекса Украины - "действия, направленные на насильственное изменение или свержение конституционного строя или захват государственной власти, а также за посягательство на территориальную целостность и неприкосновенность Украины".

Информация о других 146 распространителях ложных новостей направлена в Нацполицию. Треть из них уже привлечена к административной ответственности за распространение ложных слухов, которые могут вызвать панику или нарушение общественного порядка.

СБУ заблокировала более двух тысяч "вредных" интернет-сообществ с общей аудиторией более 700 тысяч человек.

"Специалисты по кибербезопасности СБУ постоянно анализируют интернет-контент подобной тематики, который в основном распространяется с российского информационного пространства. Он направлен на создание искусственной паники или содержит призывы к нарушению условий карантина", - сказано в сообщении Службы». ***(СБУ РАЗОБЛАЧИЛА 154 РАСПРОСТРАНИТЕЛЕЙ ФЕЙКОВ О КОРОНАВИРУСЕ // Багнет (http://www.bagnet.org/news/accidents/423091/sbu-razoblachila-154-rasprostraniteley-feykov-o-koronaviruse). 14.04.2020).***

***

«NASA сообщило об увеличении кибератак, которые направлены на специалистов агентства, перешедших на удаленный режим работы. За последние несколько дней количество атак на системы NASA увеличилось вдвое, кроме того чаще начали фиксировать попытки фишинга.

Последний пункт, отмечают в NASA, вызывает особое беспокойство – он означает, что сотрудники агентства переходят по ссылкам на вредоносные сайты в два раза чаще, чем обычно.

Как происходят атаки и при чем здесь COVID-19

Попытки заставить пользователей зайти на сайт или открыть вредоносное приложение, вложенное в письмо, остаются одним из самых простых способов получить доступ к корпоративным сетям и персональным компьютерам работников агентства, заявляют в NASA. В меморандуме агентства отмечается, что для атаки злоумышленники часто используют информацию о коронавирусе.

Сотрудники NASA должны знать, что киберпреступники, которые пытаются получить доступ к конфиденциальной информации, логинам и паролям пользователей, активно используют пандемию COVID-19 как повод для атаки на электронные устройства и сети NASA. В письмах с вредными ссылками часто содержатся запросы на пожертвования, информация о распространении и передаче вируса, мерах безопасности, получении льгот, фейковые новости о вакцинах,

– отмечают в NASA.

Другие учреждения, которые пострадали от атак

NASA – не единственное учреждение, которое зафиксировало рост кибератак на фоне пандемии COVID-19. Ранее исследователи компании Abnormal Secutity сообщали о росте количества фишинговых атак, связанных с темой коронавируса.

Злоумышленники маскируют свои письма под официальные сообщения студентам от руководства университетов или письма от Всемирной организации здравоохранения с подробным описанием мер безопасности для предотвращения инфекции.

Кроме того, исследователи из охранной компании Sophos сообщили о десятках новых интернет-доменов со словом covid и о более чем 5 тысячах сертификатов HTTPS, которые ссылаются на коронавирус.

Также коронавирус стал причиной DDoS-атаки на сайт Министерства здравоохранения и социальных служб США. Атака вывела сайт из строя. Как сообщал портал Bleeping Computer, после вспышки COVID-19 количество людей, которые ищут информацию о коронавирусах, резко возросло. В связи с этим злоумышленники попытались сорвать распространение информации о вирусе, выполнив DDoS-атаку на веб-сайт HHS.gov.

Кроме того, в интернете начали распространяться слухи о "национальном карантине" на территории США. Позже Совет национальной безопасности США опубликовал в Twitter опровержение этих слухов. Как считают власти США, кибератаку осуществили иностранные хакеры, но подтверждения этому пока нет.

Как защитить себя и компанию

Информационный отдел NASA советует персоналу использовать для защиты от кибератак собственный VPN агентства, а также не пользоваться служебной электронной почтой в личных целях, а личные аккаунты, например, в социальных сетях, не использовать для работы.

Однако, как пишет ArsTechnica, использование VPN эффективно только для тех, кто подключается к корпоративным сетям.

Люди, которые работают из дома и имеют доступ к G Suites, Salesforce или другим облачным сервисам, получают значительно меньшую выгоду от VPN. Потребительские VPN обычно не обеспечивают дополнительную защиту от фишинг-атак и вредоносных программ, подчеркивает издание…» ***(Количество кибератак на NASA резко возросло из-за коронавируса // Телеканал новостей «24» (https://24tv.ua/techno/ru/kolichestvo_kiberatak_na_nasa_rezko_vozroslo_iz_za_koronavirusa_n1312579). 08.04.2020).***

***

«Киберпреступники, действовавшие в интересах иностранных правительств, взломали сети компаний и учреждений, исследующих COVID-19

Высокопоставленная сотрудница Федерального бюро расследований заявила в четверг, что хакеры, действовавшие в интересах иностранных государств, взломали сети американских компаний, проводящих исследования COVID-19 – тяжелого респираторного заболевания, вызванного коронавирусом.

Тоня Угорец, зампомощника директора ФБР по борьбе с киберпреступностью рассказала об этом участникам интернет-дискуссии, организованной вашингтонским Институтом Аспена.

По словам Угорец, ФБР недавно получило информацию о кибератаках на сети ряда медицинских и исследовательских учреждений, занимающихся изучением коронавируса и вызываемого им заболевания. Хакеры, как стало известно ФБР, действовали в интересах неких иностранных правительств. Угорец не уточнила названия хакерских группировок и государств, в чьих интересах действовали киберпреступники.

«Мы определенно зафиксировали разведывательную деятельность и несколько вторжений в [сети] некоторых учреждений, особенно тех, что публично заявили о проведении исследований, связанных с COVID», - заявила представитель ФБР.

Угорец отметила, что учреждения, которые работают над разработкой перспективной терапии или потенциальной вакцины, безусловно заинтересованы в публичном освещении своей деятельности. Тем не менее, по ее словам, в этом случае такими учреждениями начинают интересоваться «другие государства, заинтересованные в сборе подробностей» проводимых исследований и, возможно, даже в «краже конфиденциальной информации, которой обладают эти учреждения».

Представитель ФБР добавила, что хакерские группировки, поддерживаемые иностранными правительствами, часто атакуют биофармацевтическую промышленность, и подобные атаки только усилились с начала нынешнего кризиса, связанного с пандемией коронавируса…». ***(ФБР: иностранные хакеры заинтересовались исследованиями по лечению коронавируса // Голос Америки (https://www.golos-ameriki.ru/a/fbi-hackers-covid/5376008.html). 17.04.2020).***

***

«Киберпреступники атакуют военные организации в США с помощью фишинговых писем, эксплуатирующих тепу пандемии коронавируса. Согласно отчету Центра по борьбе с киберпреступностью при Министерстве обороны США, злоумышленники нацелились не только на оборонные предприятия – их главной целью является Пентагон.

Хотя киберпреступники уже в течение нескольких месяцев активно атакуют компании и частных лиц письмами на тему COVID-19, о подобных атаках на свои сети Минобороны США заявило впервые. Сообщение об атаках было опубликовано через платформу Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE), предоставляющую предприятиям оборонно-промышленного комплекса данные о киберугрозах.

Одна из компаний сообщила Минобороны о получении электронного письма якобы от Центра по контролю и профилактике заболеваний США. Указанная в письме ссылка вела на мошеннический сайт, предназначенный для похищения учетных данных.

Удалось ли злоумышленникам добиться желаемого и проникнуть в сети Пентагона, DCISE не сообщает…». ***(Хакеры атакуют Пентагон с помощью фишинговых писем на тему COVID-19 // SecurityLab (https://www.securitylab.ru/news/506956.php). 22.04.2020).***

***

«Исходный код мобильного приложения Covid19 Alert, предложенного правительству Нидерландов в качестве средства отслеживания случаев заражения коронавирусной инфекцией (COVID-19), не соответствует приемлемым стандартам безопасности, поскольку содержит пользовательские данные другой программы.

Covid19 Alert вошло в число приложений, представленных Министерству здравоохранения, социального обеспечения и спорта Нидерландов, сообщило информагентство RTL Nieuws. Исходный код мобильного приложения был опубликован в Сети для проверки, и вскоре в нем были обнаружены пользовательские данные, происходящие из другой программы.

Приложение содержало около 200 полных имен, адресов электронной почты и хэшей паролей пользователей, хранящихся в базе данных другого проекта, связанного с разработчиком Immotef.

По словам представителя Covid19 Alert, информация была «случайно помещена в Сеть» из-за спешки, поскольку команда хотела сделать исходный код доступным для анализа. Разработчики работают над улучшениями, но остается неизвестным, пройдет ли Covid19 Alert дальше в процессе отбора.

Это далеко не первый случай, когда приложение для обнаружения коронавируса уличили в проблемах конфиденциальности. Например, в марте нынешнего года власти Китая выпустили приложение Alipay Health Code, позволяющее пользователю проверить, необходимо ли ему находиться в карантине из-за контакта с людьми, зараженными коронавирусом. Как оказалось, приложение также передает эти данные в полицию». ***(В приложении для отслеживания***

COVID-19 обнаружена утечка данных // SecurityLab (https://www.securitylab.ru/news/506861.php). 20.04.2020).

***

«Ймовірно, нікого не здивує, що під час пандемії COVID-19 триває і навіть посилюється діяльність хакерів, які підтримуються державами, але, як повідомляється, США переконані, що одна з країн проводить масовану кампанію. Чиновники, які спілкувалися з журналістами CNN, стверджують, що зафіксована ціла хвиля кібератак проти американських урядових агентств і фармацевтичних фірм – американські фахівці пов'язують кампанію з Пекіном. Вважається, що Китай намагається вкрасти дослідження COVID-19, щоб просунути свої методи лікування або вакцинації.

У той час як атаки були нанесені по цілому ряду постачальників медичних послуг та фармацевтичних компаній, за даними CNN, міністерство охорони здоров'я і соціальних служб (яке управляє CDC) також стало свідком сплеску щоденних нападів зловмисників.

До сих пір Китай не відповів на звинувачення, і примітно, що інші країни були звинувачені в атаках, пов'язаних з пандемією. Наприклад, на початку квітня агентство Reuters стверджувало, ніби іранські хакери намагалися скомпрометувати облікові записи електронної пошти працівників Всесвітньої організації охорони здоров'я. Американською владою озвучувалася звинувачення і проти інших країн.

Проте, Китай сильніше інших хвилює чиновників в США. Китай, як повідомляється, активно включився в кампанію з дезінформації, щоб викликати хаос навколо COVID-19. У минулому чиновники також звинувачували китайських хакерів у зломи, пов'язаних з системою охорони здоров'я. З огляду на масштабні наслідки пандемії COVID-19 і карантинних заходів, не виключено, що звинувачення США проти Китаю будуть звучати все частіше, підливаючи масла у вогонь кілька затихлої торгової війни». ***(США звинуватили Китай у хакерських атаках, націлених на дослідження COVID-19 // Portaltele (https://portaltele.com.ua/news/officially/ssha-zvinuvatili-kitaj-u-hakerskih-atakah-natsilenih-na-doslidzhennya-covid-19.html). 26.04.2020).***

***

«Специалисты «Лаборатории Касперского» сообщили о стремительном росте брутфорс-атак на протокол RDP, связанном с переходом многих компаний на удаленную работу из-за пандемии COVID-19.

Резкий скачок числа брутфорс-атак на RDP (Bruteforce.Generic.RDP в терминологии ЛК) произошел ближе к середине марта, причем картина примерно одинакова по всему миру, отмечают в ЛК. Атаки осуществляются не точечно, а по площадям. Похоже, киберпреступники логично заключили, что в связи с экстренным переходом сотрудников по всему миру на удаленную работу возрастет число плохо настроенных RDP-серверов, поэтому увеличили количество атак.

По мнению специалистов ЛК, в ближайшем времени прекращения атак на инфраструктуру, связанную с удаленным доступом (а также на различные сервисы, используемые для совместной работы) ожидать не стоит.

Для защиты от атак на RDP компаниям рекомендуется использовать сложные пароли, сделать RDP доступным только через корпоративный VPN, использовать аутентификацию на уровне сети (Network Level Authentication, NLA) и включить двухфакторную аутентификацию. Если RDP не используется, рекомендуется выключить его и закрыть порт 3389». ***(В связи с пандемией COVID-19 резко возросло число брутфорс-атак на RDP // SecurityLab.ru (https://www.securitylab.ru/news/508005.php). 30.04.2020).***

***

«Страны ЕС в период пандемии коронавирусной инфекции зафиксировали многочисленные кибератаки. Об этом говорится в распространенном в четверг, 30 апреля, заявлении главы внешнеполитической службы Евросоюза Жозепа Боррeля.

«ЕС фиксирует кибернетические угрозы и вредоносную кибернетическую деятельность против государств сообщества и стран-партнеров, направленные в том числе против сектора здравоохранения», — сказал Боррель.

По данным компании Infosecurity a Softline Company, с переходом российских образовательных учреждений на дистанционное обучение, кибератаки на них участились в 4 раза. Подобные киберпреступления совершаются с целью кражи персональных данных и контактной информации учащихся с целью их дальнейшего использования, например, в социальной инженерии. Также учебные чаты и конференции подвергаются атакам пранкеров.

Исследовании компании Positive Technologies выявили, что злоумышленники в интернет-пространстве чаще всего продают доступы в компании из США, Великобритании, Италии, Германии и Бразилии.

13 марта эксперт по кибербезопасности Александр Урбелис, работающий в нью-йоркской компании Blackstone Law Group сообщил о хакерской атаке на системы Всемирной организации здравоохранения (ВОЗ). Никаких предположений относительно того, кто стоял за этой атакой, эксперт не выдвинул.

Для минимизации рисков эксперты, опрошенные «Известиями», советуют работодателям заранее проводить инструктаж сотрудников, установить на их компьютеры антивирусные программы и VPN-доступ с двухфакторной аутентификацией, а также обновить всё ПО и IT-оборудование, обеспечивающее работу компании». ***(Страны Евросоюза заявили об увеличении числа кибератак // Газета «Известия» (https://iz.ru/1006469/2020-04-30/strany-evrosoiuza-zaiavili-ob-uvelichenii-chisla-kiberatak). 30.04.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«У рамках “Тижня Азії” Міністр закордонних справ України Дмитро Кулеба 2 квітня зустрівся з Послом Японії в Україні Такаші Кураі.

Співрозмовники відзначили обопільну зацікавленість у розвитку співробітництва у сфері кібербезпеки та продовженні безпекового діалогу з наголосом на протидії гібридним загрозам…». ***(Україна і Японія розвиватимуть взаємодію з протидії гібридним загрозам та кібератакам // Офіційно https://oficiyno.com.ua/2020/04/02/ukrajina-i-japonija-rozvivatimut-vzaemodiju-z-protidiji-gibridnim-zagrozam-ta-kiberatakam-31152/). 02.04.2020).***

***

Світові тенденції в галузі кібербезпеки

«Министерство иностранных дел ФРГ, Сенат США и компания Google запретили своим сотрудникам использовать приложение Zoom для видеоконференций. Данные решения связаны с наличием в программе проблем с безопасностью и защитой данных, подвергающих пользователей риску атак.

Запрет МИД Германии не затрагивает приложение, установленное на рабочих системах с проводным подключением к интернету, сообщила газета Handelsblatt. Однако в подобном случае запрещается вести конфиденциальные разговоры. Также отмечается, что в министерстве не могут полностью отказаться от программы, поскольку ее используют иностранные партнеры немецких дипломатов.

Компания Google также ввела запрет на использование платформы телеконференций Zoom для своих сотрудников, сославшись на проблемы с безопасностью приложения. Google отправила электронное письмо сотрудникам, сообщив об отключении данного ПО на рабочих компьютерах.

«Мы давно придерживаемся политики не разрешать сотрудникам использовать неутвержденные приложения для работы вне нашей корпоративной сети. Наша команда безопасности проинформировала сотрудников, использующих Zoom Desktop Client, что приложение больше не будет работать на корпоративных компьютерах, поскольку не соответствует стандартам безопасности. Сотрудники по-прежнему могут использовать Zoom для поддержания связи с семьей и друзьями», — сообщил пресс-секретарь Google Хосе Кастанеда (Jose Castaneda) порталу BuzzFeed News.

Вслед за решением Google сенат США также запретил своим членам использовать Zoom, сообщила газета Financial Times. Парламентский пристав, в чьи обязанности входит управление правоохранительными органами и безопасностью в Капитолии, порекомендовал сенаторам найти альтернативные методы для удаленной работы, хотя и не ввел прямой запрет…» ***(Сенат США, МИД Германии и Google ограничили сотрудникам использование Zoom // SecurityLab.ru (https://www.securitylab.ru/news/506555.php). 09.04.2020).***

***

«9 апреля сервис Zoom сообщил о создании собственного Совета по кибербезопасности. К работе привлекли бывшего руководителя службы кибербезопасности Facebook Алекса Стамоса, сообщает socialmediatoday.com.

Также руководство компании разработало 90-дневный антикризисный план и привлекло, кроме Стамоса, еще нескольких экспертов по безопасности. В частности, к Совету присоединилдись Chief Information Security Officers таких компаний, как HSBC, NTT Data, Procore.

Решение о создании Совета безопасности было принято после того, как в сеть попали записи видеозвонков нескольких тысяч пользователей. Затем от услуг сервиса отказались в Google, а еще в марте пользоваться приложеним своим сотрудникам запретил Илон Маск. После этого акционер Zoom Video Communications Inc. Майкл Дриу подал иск против компании, в котором обвиняет ее в сокрытии уязвимостей программы.

Однако несмотря на неприятности, на торгах 8 апреля 2020 года акции компании выросли на 4%. Возможно это связано с положительной оценкой версии приложения для правительства — Zoom for Government, данной Министерством внутренней безопасности США, Агентством инфраструктурной безопасности и Федеральной программой управления рисками и авторизацией». ***(Zoom сформировал собственный Совет безопасности // Телекритика (https://telekritika.ua/zoom-sformiroval-sobstvennyj-sovet-bezopasnosti/).10.04.2020).***

***

Сполучені Штати Америки

«В сентябре 2018 года президент США Дональд Трамп утвердил национальную киберстратегию Америки (National Cyber Strategy of the United States of America). В ней перечислены меры по обеспечению безопасности интернета, схожие с введенными в 2019 году в России законопроектом о надежном Рунете. Однако, помимо этого, Соединенные Штаты в указанной стратегии определяют для себя роль контроллера процессов информационных потоков мировой сети, а также арбитра обеспечения свободы интернета с правом вмешиваться в сети иностранных государств.

РАПСИ публикует ключевые выдержки из национальной киберстратегии США, демонстрирующие важность и своевременность принятия в России мер по обеспечению надежной и при необходимости суверенной работы Рунета.

Структурно киберстратегия США подразделяется на четыре «принципа»: защита американского народа, Соединенных Штатов и американского образа жизни; обеспечение процветания США; сохранение мира методом принуждения; продвижение американского влияния.

Важнейшей задачей киберстратегии США утверждается защита национальной инфраструктуры интернета, что в точности соответствует содержанию российского закона о надежном Рунете. В Америке контроль за безопасностью IT-инфраструктуры концентрируется на федеральном уровне. Министерству национальной безопасности предоставляется доступ к информационным системам органов власти и полномочия по их защите.

Ключевым моментом в проекте обеспечения национальной кибербезопасности США является контроль органов власти за соответствие

закупаемых IT-продуктов нормам федерального сервиса оценки рисков. Большинству иностранных поставщиков попадает в «черный список» и не допускается к участию в государственных закупках. В частности, это произошло с «Лабораторией Касперского» (без каких-либо доказательств опасности программных продуктов компании). Также от процесса создания сети передачи данных нового поколения отстранены китайские подрядчики.

Как указано в аналитическом докладе Института исследования интернета (ИИИ) «в настоящее время… усиливается конфликт между, с одной стороны, персональными данными/данными личного характера, приобретающими все большую экономическую значимость и коммерческую ценность и, с другой стороны, их защитой и обеспечением конфиденциальности. Несомненно, средства, методы разрешения этого конфликта, а также меры правовой защиты и т.д. будут претерпевать радикальные изменения и варьироваться в зависимости от специфики национальных правопорядков государств.

В этом плане нельзя не обратить внимание на тот подход, который закреплен в киберстратегии США. Во-первых, содействие развитию жизнеспособной и устойчивой цифровой экономике выделено в самостоятельный раздел. Во-вторых, в разделе отмечается, что «ограничительные положения о локализации данных» нередко используется в качестве оправдания для цифрового протекционизма, подводятся под категорию национальной безопасности».

Однако основной ареной действия национальной кибербезопасности США является международная сеть. Одной из главных задач является предотвращение отказа от многосторонней модели управления интернетом и воспрепятствование национальным государствам осуществлять суверенитет в киберпространстве. Это делается с целью ограничить неамериканское влияние на развитие интернета.

В «Основополагающем элементе III» киберстратегии: «Сохранение мира посредством силы» в качестве ключевой цели, в частности, формулируется: «выявление, противодействие, пресечение, ослабление интенсивности, а также сдерживание действий в киберпространстве, которые дестабилизирует и противоречат национальным интересам США, с сохранением превосходства США в киберпространстве и посредством киберпространства».

Более прозрачно поясняется, что имеется в виду под «открытым интернетом» и каковы цели США в другом разделе киберстратегии: «Многие страны все чаще прибегают к различным ограничениям для локализации данных и внедряют механизмы регулирования в целях реализации политики цифрового протекционизма под предлогом обеспечения национальной безопасности. Эти действия оказывают отрицательное воздействие на конкурентоспособность американских компаний».

Важно заметить, что программа международного сотрудничества, описываемая в киберстратегии, однозначно позиционирует Россию как оппонента или даже врага США со всеми вытекающими мерами и последствиями.

Во введении в киберстратегию США говорится: «Администрация признает, что Соединенные Штаты ведут постоянную конкуренцию со стратегическими противниками, государствами, не признающими международных норм, террористическими и криминальными сетями. Россия, Китай, Иран и Северная

Корея всецело используют киберпространство как средство для создания реальной угрозы Соединенным Штатам, их союзникам и партнерам, часто с безрассудством, которое они никогда не проявляли бы в других сферах деятельности. Эти противоборствующие стороны используют киберинструменты, чтобы подорвать нашу экономику и демократию, украсть нашу интеллектуальную собственность и посеять раздор в наших демократических процессах. Мы уязвимы перед кибератаками в мирное время на критическую инфраструктуру, а также растет риск того, что эти страны будут проводить кибератаки против Соединенных Штатов во время кризиса, близкого к войне. Эти противоборствующие стороны постоянно разрабатывают новое и более эффективное кибероружие».

В этой связи в киберстратегии определены следующие ключевые направления укрепления потенциала кибербезопасности, а также обеспечения защиты США от киберугроз: «усиление американского влияния за рубежом (выделение – прим. ред.) с тем, чтобы расширить основополагающие принципы открытого, функционально совместимого, интероперабельного, надежного и безопасного интернета».

Международное право в киберстратегии упоминается лишь косвенно, как отмечают эксперты, фактически оно замена «добровольной приверженностью (других стран – прим. ред.) факультативным нормам ответственного поведения государств в мирное время».

Кроме того, среди целей киберстратегии указано намерение добиваться присоединения как можно большего количества стран к конвенции Совета Европы по борьбе с киберпреступностью (Будапештская конвенция), которая разрешает её участникам без согласования действовать на территории иностранного государства. Важно заметить, что Россия не принимает нормы Будапештской конвенции.

На основании норм этой конвенции США намереваются применять для предотвращения «безответственного поведения государств в киберпространстве, влекущего ущерб США или американским партнерам» дипломатические, военные, финансовые, разведывательные методы, публичные заявления и «возможности правоохранительных органов».» ***(Национальная киберстратегия США. Справка // РАПСИ (http://rapsinews.ru/publications/20200406/305674519.html). 06.04.2020).***

***

«Министерство обороны США существенно (в некоторых случаях на несколько лет) отстает в реализации ряда инициатив по обеспечению внутренней кибербезопасности. Об этом сообщается в отчете Счетной палаты США под названием “Минобороны необходимо предпринять решительные действия для улучшения кибергигиены” (“DOD Needs to Take Decisive Actions to Improve Cyber Hygiene”), опубликованном в понедельник, 13 апреля.

Согласно отчету, Пентагон не реализовал базовые практики кибербезопасности, чем поставил себя под угрозу кибератак. “До тех пор, пока Минобороны не завершит инициативы по кибергигиене и не внедрит практики кибербезопасности, министерство будет подвергаться повышенному риску успешных кибератак”, - сообщается в отчете.

Специалисты Счетной палаты оценивали реализацию трех инициатив по кибербезопасности: “Инициативы Минобороны по повышению культуры и соответствия кибербезопасности” (DOD Cybersecurity Culture and Compliance Initiative, DC3I), “Плана реализации дисциплины в области кибербезопасности” (Cybersecurity Discipline Implementation Plan, CDIP) и учений по кибербезопасности.

Как оказалось, 11 пунктов инициативы DC3I должны были быть завершены к концу финансового 2016 года, однако 7 из них до сих пор не закрыты. Как сообщается в отчете, 7 пунктов не были завершены, поскольку управление информационного директора Минобороны не приняло меры по их реализации. В управлении заявили, что не знали о возложенной ответственности, хотя эти задачи были закреплены за ним еще в декабре 2016 года.

На момент составления отчета Счетной палаты из 17 задач инициативы CDIP также были реализованы не все. 4 из 10 пунктов, за выполнение которых было ответственно управление информационного директора, так и не были завершены. Статус еще 7 задач остается неизвестным, поскольку ответственные за их выполнение не были назначены.Что касается учений, то Пентагон до конца не одобрил программу учений за 2018 год». ***(Пентагон на несколько лет отстает по инициативам кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/506621.php). 14.04.2020).***

***

Країни ЄС

«Министерство иностранных дел Германии ограничило использование видео-сервиса конференц-связи Zoom для своих сотрудников, пишет в среду, 8 апреля, газета Handelsblatt. По данным издания, ведомство направило служебную записку, в которой пишет о рисках использования платформы для безопасности и защиты данных.

В служебной записке отмечается, что поскольку система широко используется международными партнерами министерства, в настоящее время невозможно полностью запретить ее использование, а в кризисных ситуациях сотрудники могут совершать рабочие звонки посредством приложения на своих персональных компьютерах.

Издание напоминает, что недавно компания SpaceX Илона Маска и американское космическое агентство NASA запретили сотрудникам пользоваться платформой Zoom из-за "значительных проблем с конфиденциальностью и безопасностью".

Во время пандемии коронавируса в мире Zoom значительно нарастил число пользователей. Суточная аудитория приложения с декабря 2019 года по март 2020 года выросла в 20 раз, достигнув 200 миллионов человек. Во время карантина в разных странах мира Zoom используют предприниматели, учителя, фитнес-тренеры, артисты. Однако одновременно появились жалобы пользователей на несанкционированное подключение нежелательных лиц к видеоконференциям.

Накануне один из акционеров Zoom Video Communications обратился в суд США с иском к компании, обвинив ее в сокрытии данных о безопасности приложения, что привело к падению стоимости акций.» ***(МИД Германии советует не использовать Zoom вырастут // Internetua (https://internetua.com/mid-germanii-sovetuet-ne-ispolzovat-zoom). 09.04.2020).***

***

Китай

«Китай объявил о введении с 1 июня новых правил кибербезопасности, призванных способствовать "созданию упорядоченного, безопасного и открытого киберпространства и обеспечению национальной безопасности".

Соответствующий документ, озаглавленный "Меры по обновлению кибербезопасности", опубликован Управлением по вопросам киберпространства КНР - главным регулятором сферы интернета в стране.

Как отмечают местные эксперты, новые меры призваны "устранить потенциальные риски в области кибербезопасности" и гарантировать здоровое развитие национальной интернет-индустрии. Предполагается, что они скажутся на деятельности как китайских, так и иностранных поставщиков информации и сетевых продуктов и услуг для таких стратегических отраслей, как телекоммуникации, радио и телевидение, энергетика, финансы, дорожное хозяйство и водный транспорт, железные дороги и гражданская авиация.

В документе, который излагает газета China Daily, говорится, что операторы "критически важной информации", которые хотят предоставлять сетевые продукты и услуги для областей, имеющих отношение к национальной безопасности, должны будут проходить соответствующую проверку. При этом должны быть обозначены потенциальные риски для кибербезопасности, связанные с данными продуктами и услугами, имея в виду, например, незаконный контроль над информационными сетями, повреждение их, а также утечку, потерю и повреждение ключевых данных.

"Ранее главным вызовом с точки зрения кибербезопасности была защита личной информации. Теперь интернет-технологии служат широкому кругу отраслей, включая ряд важнейших секторов, тесно связанных с национальной экономикой и общественным развитием", - приводит издание мнение неназванного представителя китайской компании Qi An Xin Group, работающей в сфере промышленной и сетевой безопасности.

Одновременно Управление по вопросам киберпространства КНР объявило о начале двухмесячной кампании борьбы со "злонамеренными аккаунтами" в соцсетях. "Любые аккаунты, которые будут уличены в нарушении закона и соответствующих уложений, будут закрыты, а их операторы - подвергнуты наказанию", - говорится на сайте ведомства.

Как полагают наблюдатели, меры китайских властей по ужесточению контроля в сфере интернета и соцсетей связаны, в частности, с опытом, приобретенным в период борьбы с эпидемией коронавирусной инфекции». ***(Китай вводит новые правила национальной кибербезопасности // ООО "ИКС-***

МЕДИА" (http://www.iksmedia.ru/news/5660909-Kitaj-vvodit-novye-pravila-nacional.html). 28.04.2020).

***

…Правительство планировало провести ряд реформ и трансформировать Госспецсвязь. В частности, была выдвинута идея о создании комплексной системы защиты информации на онлайн-платформах «Прозорро», «Трембита», EHealth и Mobileid. Однако сейчас мы наблюдаем совсем иную картину: во время карантина и экономического кризиса большинство украинских ресурсов остаются абсолютно незащищенными перед российской киберугрозой.

Если верить информации, просочившейся в российские СМИ, ФСБ начало разрабатывать программу «Фронтон», способную осуществлять кибератаки на устройства интернета вещей. Программа способна останавливать работу не только соцсетей и файлообменников, но и отключать интернет на несколько часов по всей стране.

…Директор компании Berezha Security г-н Косун является сторонником идеи полной перезагрузки Госспецсвязи, которая нашла поддержку со стороны нынешней власти. Однако, как показало время, реформа закончилась (как и большинство других) банальным переназначением главы госслужбы.

«Я бы не сказал, что Валентин Петров (председатель Госспецсвязи) - человек «зеленой команды». Он в свое время работал в аппарате СНБО и занимался вопросами кибербезопасности. Петров пытается двигаться в верном направлении, но ГСССЗИ очень тяжелая и неповоротливая советская система, которая не предназначена для быстрого реагирования, поэтому она не может быть быстро реформированной. Она построена на постсоветских и совковых принципах, которые изначально являются коррумпированными и неэффективными. Поэтому Петрову очень трудно противостоять всей этой мафии, не имея собственной профессиональной команды. Ведь один в поле не воин. Я считаю, что нет смысла тратить время и усилия на перестройку этой абсолютно устаревшей и трухлявой конструкции, которую уже невозможно спасти. Тем более, что ей уже никогда и никто не будут доверять. Следует создать новый институт на более современных и демократических принципах (выбирать персонал на конкурсных основах и с конкурентными зарплатами). И постепенно, не размахивая шашкой, передавать полезные функции Госспецсвязи новой структуре. То есть должна быть создана авторитетная организация, которая консультировала бы всех игроков в сфере кибербезопасности по ключевым вопросам. В общем, необходимо создать коллективно-совещательный орган на добровольных началах без каких-либо властных полномочий».

Г-н Корсун напомнил о том, что Госспецсвязь обеспечивала правительство необходимой связью, и лишь в начале двухтысячных ей добавили новые функции.

Но госслужба так и не научилась противостоять каким-либо киберугрозам (сетей, серверов, софта, оборудования) в кибервойне с Россией.

«Исходя из предыдущих неопровержимых доказательств, ГСССЗИ не способна обеспечить даже свою собственную кибербезопасность. В свое время их самая продвинутая команда Center UA держала на своем веб-сайте в открытом доступе пароли к собственной электронной почте. Там еще было несколько подобных «зашкваров», которые демонстрируют полную некомпетентность и неспособность защитить самих себя. А что уже говорить о сотнях тысяч других сетей, в том числе и критической инфраструктуры. Если в Украине только сети государственных учреждений превышает цифру в ста тысяч, не говоря уже о частных компаниях, которых в десятки раз больше».

Эксперт по кибербезопасности напомнил о вирусе Petya, который распространялся через серверы бухгалтерской компании M.E.Doc. Он считает, что это была всего лишь небольшая разминка по сравнению с тем, что русские могут сделать в любой момент. По его словам, государство не то что не усвоило предыдущие уроки - оно так и не смогло создать полноценную систему национальной кибербезопасности.

«Ни одного движения в сторону национальной кибербезопасности не сделано. Причем уже был неприятный прецедент в Прикарпатье, когда русские отключили облэнерго и более 60 тысяч человек, проживающих в этом регионе, сидели без света. Также русские не раз вмешивались в работу украинских аэропортов. Патриотически настроенные украинские хакеры находили многочисленные проблемы с кибербезопасностью в аэропортах, на атомных станциях, предприятиях тяжелой индустрии и в транспортных сетях. У нас просто огромные пробелы по кибербезопасности в критически важной инфраструктуре. Таких случаев уже зафиксировано около 200. Я вам больше скажу – при прошлом президенте ничего не делалось в этом направлении, а все лишь воровали. Новая власть пошла еще дальше - начали преследовать белых хакеров, фальсифицируя при этом уголовные дела. У нас чиновники, включая президента, очень нервничают, когда их критикуют».

По словам г-на Корсуна, русские боты сидят во всех ключевых объектах украинской критической инфраструктуры, ожидая команды из Кремля на совершение очередной диверсии. Однако России сейчас невыгодно осуществлять кибератаки против Украины по политическим и репутационным соображениям.

«Как защититься в случае кибератаки? Никак. Сейчас работает принцип “каждый за себя”. Государство не в состоянии кого-либо защитить и не сможет помочь в критический момент. Оно лишь может состряпать какое-то уголовное дело, провести обыски или оштрафовать. Защищаться, в первую очередь, нужно объектам критической инфраструктуры, большинство которых находится в частной собственности. Среди них необходимо постоянно и настойчиво проводить разъяснительную работу. В западных странах уже разработаны современные профили защиты для различных IT-продуктов: ОС, СУБД, Firewalls, смарт-карт и тому подобных». ***(Элина Сулима. Госспецсвязь не способна обеспечить даже свою собственную кибербезопасность // Internetua***

(https://internetua.com/gosspecsvyaz-ne-sposobna-obespecsit-daje-svoua-sobstvennuua-kiberbezopasnost-). 03.04.2020).

***

Інші країни

«Компания «Custodio Technologies», сингапурское подразделение предприятия «Israel Aerospace Industries ELTA», станет частью Национальной научно-исследовательской программы Сингапура по кибернетической безопасности.

К участию в этой же программе привлечены Управление оборонных разработок и технологий, а также Министерство внутренних дел. Двухгодовой проект под названием «SLADE: Smart Learning Analytics for Digital Crime» нацелен на разработку умной платформы для анализа, изучения и расследования преступлений, совершенных в цифровом пространстве. Соответственно, следователи получат больше возможностей для установления личностей и поиска преступников.

В рамках вышеупомянутого проекта будет оптимизирована и в максимальной мере использована платформа «CyVestiGO», являющаяся локальной разработкой компании «Custodio Technologies». ***(«IAI» займется проектом по кибербезопасности // ISRAland Online Ltd (http://www.isra.com/news/244445). 24.02.2020).***

***

Протидія зовнішній кібернетичній агресії

«Президент США Дональд Трамп продовжив дію виконавчих указів про введені в тому числі проти Росії санкції за кібератаки щодо Сполучених Штатів…

Так, указ 13694, вперше ухвалений президентом Бараком Обамою, передбачає обмеження проти країн, які становлять загрозу для США в кіберпросторі.

Рішення також дозволяє міністерству фінансів країни вводити санкції проти осіб, які здійснюють кібератаки проти США, зокрема, блокувати рахунки і будь-які активи підсанкційних осіб на території країни.

“Ця значна зловмисна діяльність в кіберпросторі досі несе надзвичайну загрозу національній безпеці, зовнішній політиці та економіці США”, – йдеться в документі». ***(Трамп продовжив санкції проти Росії за кібератаки // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/tramp-prodovzhyv-sanktsiyi-proty-rosiyi-za-kiberataky.html). 01.04.2020).***

***

«Злам сайту Польського університету військових досліджень, а також слідуюча за зламом кампанія з дезінформації, є прикладом системних російських кібератак проти армії Польщі. Про це пише в своїй статті на Forsa.pl оглядач Мачей Мілош.

«Хакери РФ атакували сайт Польського університету військових досліджень і спробували запустити кампанію з дезінформації щодо польської армії. І це лише крайній випадок атак російських хакерів проти армії Польщі», - пише автор.

«Ідеологія фашизму, яка знищила 6 мільйонів поляків відроджується під опікою польської держави. З важким серцем я повинен визнати, що подібні процеси виходять і від Міністерства оборони», - наводить автор статті цитату з повідомлення розміщеного на сайті Університету військових досліджень, нібито написаного його ректором генералом Рішардом Парафіановічем.

«У повідомленні також критикувався союз Польщі з Сполученими Штатами і фігурували попередження про те, що польські політики, нібито ведуть країну до катастрофи. Безумовно, лист є підробкою і був опублікований хакерами, які зламали сайт університету. Атака, в свою чергу, була оперативно виявлена, а фейкова сторінка видалена з сайту. Міністерство оборони Польщі відреагувало, спростувавши брехливу інформацію і попередило, що подібні атаки можуть посилитися, особливо ті, що направлені проти польської армії. Міністерство звернулося до громадян з проханням бути обережними, не поширювати неправдиві новини і використовувати надійні джерела інформації», - повідомляє оглядач.

«Атака на сайт університету далеко не перша. Три роки тому в Інтернеті було опубліковано фейкове інтерв'ю з польським командувачем, генералом Славоміром Войцеховським, в якому генерал, нібито заявив, що «польські платники податків будуть платити за "ілюзорну американську військову присутність" і що США нібито "душать розвиток власної армії Польщі". У тому фейковому інтерв'ю також повідомлялося, що присутність збройних сил США в Польщі, нібито є ознакою «васальної залежності і слабкості, а не доказом партнерства», - пише Мачей Мілош.

«Такі кампанії з дезінформації мають різні форми, як, наприклад, хакерська атака на сайт університету з розміщенням інформації, яка виглядає достовірною, відправляється нібито з адреси польського парламенту, щоб ввести аудиторію в оману. Також, одним з інструментів є створення ряду веб-сайтів, що посилаються один на одного для створення уявної достовірності. Спільною рисою подібних кампаній, спрямованих проти польських офіцерів або співробітників міністерства, є критика присутності американських військових в Польщі і позиціонування НАТО, як агресора, незважаючи на оборонний характер організації », - зазначає експерт.

«Найкраще дезінформація працює в час кризи, коли емоційність людей підвищена, так як сама дезінформація спрямована на існуючі конфліктні точки в суспільстві, а емоції підсилюють сприйняття. Майбутні президентські вибори (в Польщі - ред.) стануть хорошим майданчиком для кампаній з дезінформації, особливо в умовах пандемії коронавірусу», - підсумував аналітик». ***(Хакери РФ атакували сайт Польського університету військових досліджень // Агенція інформації та аналітики (https://galinfo.com.ua/articles/hakery_rf_atakuvaly_sayt_polskogo_universytetu_viyskovyh_doslidzhen_343008.html). 30.04.2020).***

***

«Финансируемые правительством хакеры проэксплуатировали уязвимость нулевого дня в эстонском сервисе электронной почты Mail.ee и взломали учетные записи ряда высокопоставленных лиц.

Как сообщается в опубликованном недавно отчете Полиции безопасности Эстонии (Kaitsepolitseiamet, KaPo), инцидент имел место в прошлом году, и с тех пор уязвимость была исправлена. «Уязвимость эксплуатировалась для взлома лишь небольшого количества электронных ящиков, принадлежащих лицам, которые представляют интерес для иностранного государства», - говорится в отчете. Широкому кругу пользователей сервиса беспокоиться не о чем, уверяет KaPo.

Согласно отчету, атака была осуществлена с помощью электронных писем с вредоносным кодом, выполнявшимся, когда получатель открывал письмо на портале Mail.ee. Достаточно было лишь, чтобы жертва открыла письмо, никаких других действий с ее стороны не требовалось.

Вредоносный код автоматизировал ряд действий и настраивал переадресацию писем. «С момента открытия электронного письма с вредоносным кодом все получаемые жертвой письма переадресовывались на учетную запись, подконтрольную атакующему», - сообщила KaPo.

Помимо взлома Mail.ee в отчете также сообщается о других кибератаках на компании и частных лиц в Эстонии. В частности, говорится об операциях с использованием целенаправленного фишинга, проводимых другими финансируемыми правительствами группировками, такими как Gamaredon и Silent Librarian». ***(«Правительственные» хакеры взломали почту высокопоставленных лиц Эстонии // SecurityLab.ru (https://www.securitylab.ru/news/507989.php). 30.04.2020).***

***

Створення та функціонування кібервійськ

«Специалисты ИБ-компании FireEye опубликовали статистику эксплуатации спецслужбами уязвимостей нулевого дня по всему миру за последние семь лет, представленную в виде карты и временнòй шкалы. За основу эксперты взяли данные, собранные как самой FireEye, так и другими исследовательскими организациями, а также сведения из базы данных Google Project Zero.

Специалистам удалось связать 55 уязвимостей нулевого дня с кибероперациями, финансируемыми правительствами. Более того, они даже смогли определить, с правительством какой страны связана та или иная операция. Карта и временнàя шкала показывают количество уязвимостей нулевого дня, эксплуатируемых правительствами разных стран, их идентификаторы CVE и годы эксплуатации.

Судя по карте, уязвимости нулевого дня есть в арсенале у спецслужб не только передовых стран, таких как США, но и у весьма неожиданных игроков,

таких как Узбекистан. По словам специалистов, это связано с ростом числа компаний, продающих уязвимости нулевого дня спецслужбам по всему миру. Если у страны есть деньги, она скорее купит хакерские инструменты, чем разработает сама, пояснили эксперты.

«Примерно с 2017 года ландшафт начал по-настоящему меняться. Мы считаем, что хотя бы частично это связано с ролью поставщиков инструментов, расширяющих наступательные возможности правительств в киберпространстве. Наибольшая преграда между уязвимостью нулевого дня и атакующим – это не умение, а деньги», – пишут исследователи.

В частности, специалисты называют такие компании, как NSO Group, Gamma Group и Hacking Team, поставляющие инструменты для взлома правительственным организациям. К примеру, услугами NSO Group пользуются хакерские группировки Stealth Falcon и FruityArmor, предположительно связанные с правительством ОАЭ, а также SandCat, связываемая исследователями с Узбекистаном.

Чем крупнее игрок, там меньше эксплоитов он использует. Так, судя по временно̀й шкале, за последние два года Китай использовал только две уязвимости, а Россия – ни одной. Как поясняют эксперты, большие страны предпочитают обращаться к другим, более эффективным хакерским техникам, в частности к фишингу, краденым учетным данным и так называемым одноразовым эксплоитам, предназначенным для конкретных уязвимостей в каждом конкретном случае». ***(Опубликована карта эксплуатации 0day спецслужбами по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/506459.php). 07.04.2020).***

***

«…Вильнюс возглавил специальные Кибернетические силы Евросоюза быстрого реагирования (CRRT). И эта структура может представлять реальную угрозу для безопасности России.

После того, как представители шести государств (Литва, Эстония, Хорватия, Польша, Румыния, Нидерланды) подписали в Загребе в начале марта меморандум о создании совместного подразделения, глава литовского военного ведомства Раймундас Кароблис торжествующе заявил, что «это четкий конкретный пример того, как страны ЕС невоенными средствами могут содействовать повышению безопасности Европы, поддерживать усилия в деле обороны и сдерживания». По мнению Кароблиса, уж «теперь сотрудничество в сфере кибербезопасности вышло на качественно новый уровень».

В меморандуме изложены принципы деятельности подразделения. Члены международных команд, среди которых предполагаются как военные, так и гражданские, будут находиться на дежурстве в стране пребывания – и «подключаться к нейтрализации инцидентов в виртуальном пространстве».

С самого начала создание Кибернетических сил Евросоюза быстрого реагирования (CRRT) шло под руководством Литвы. Вильнюс настаивал на необходимости такой структуры с 2017 года, предлагая сделать ее частью европейской программы Постоянного структурированного сотрудничества по вопросам безопасности и обороны (Permanent Structured Cooperation – PESCO) физически еще в 2017-м. В итоге Вильнюс сумел доказать Брюсселю, что ЕС остро

нуждается в подобном подразделении. По словам Раймундаса Кароблиса, он очень рад, что CRRT стала первым фактически реализованным проектом PESCO.

Свои собственные кибернетические силы Литва активно развивает уже в течение нескольких лет. Литовцы буквально помешаны на «кибернетической опасности». Власти страны утверждают, что Литва якобы чуть ли не каждодневно подвергается атакам неких враждебных хакеров. По словам руководителя литовской Ассоциации интернет-СМИ Айсте Жилинскене, в 2017 году эти хакеры, например, взломали систему агентства новостей BNS, разместив на сайте ложное сообщение об американских солдатах, отравившихся в Латвии ипритом. В последнее время испытали на себе DDoS-атаки литовские новостные порталы delfi.lt, lrytas.lt, 15min.lt, а также сайты, принадлежащие компании Diena media news

…член комитета Совета Федерации по обороне и безопасности Франц Клинцевич заявил, что на самом деле Литва, Эстония, Хорватия, Польша, Румыния, Нидерланды не боятся кибератак на свои военные структуры, потому что они у них незначительные. По мнению сенатора, с учетом того, что у данных государств «один и тот же хозяин, не исключено, что на территории этих стран будут расставлены специальные устройства, созданы специальные базы, которые будут заниматься радиоэлектронной борьбой, радиоэлектронными диверсиями в отношении России».

Клинцевич усматривает тут руку Вашингтона…

Действительно, в июле прошлого года стало известно, что в литовском Каунасе при поддержке США строится некий «Центр кибербезопасности». Пока что про это учреждение известно довольно мало. Минувшим летом руководитель группы по политике в области кибербезопасности и информационным технологиям минобороны Литвы Йонас Скардинскас сообщал, что учреждение в Каунасе находится в «фазе создания». «У нас такая цель, чтобы этот центр начал функционировать к концу 2020 года», – сказал Скардинскас. По его словам, официальные лица Литвы вели переговоры с американцами о возможности работы в центре специалистов по кибербезопасности из гвардии Пенсильвании (США). Американцы также обещали предоставить и часть оборудования…

Согласно плану, новый центр в Каунасе будет функционировать как подразделение литовского Национального центра кибербезопасности. Предполагается, что из Каунаса можно будет управлять и силами быстрого киберреагирования ЕС. Всего Вильнюс планирует в течение трех лет выделить 430 000 евро на создание системы «раннего оповещения» о кибератаках. Власти Литвы также планируют выделить в 2020 году почти 500 000 евро на создание специального армейского «батальона связи», который будет орудовать в киберпространстве.

И тут стоит привести другие интересные сведения – три года назад, в 2017-м, в литовских СМИ появились публикации о том, что государство формирует из гражданских лиц команды кибернетических операций быстрого реагирования.

Замминистра обороны Литвы Эдвинас Кярза объявил, что в Вильнюсе создаются три такие команды. Чиновник сообщил, что в каждой из литовских «кибердружин» будет по двадцать человек, имеющих опыт работы в сфере IT. Он пообещал, что каждый «дружинник» при вступлении подвергнется тщательнейшей

проверке на предмет благонадежности. «Пятьдесят дней в году их можно будет приглашать на обучение, тренировки или осуществление вполне конкретных операций по киберзащите. Мы проводим эксперимент, чтобы посмотреть, как пришедшие в армию на добровольной основе профессионалы смогут сотрудничать в области кибербезопасности», – уверял Кярза. По его словам, кандидаты, преодолевшие все ступени отбора и прошедшие базовый курс обучения продолжительностью в несколько недель, стали военнослужащими в составе армии Литвы.

А еще годом раньше в Литве прошли первые национальные маневры «Кибернетический щит – 2016», продолжавшиеся три дня. В них участвовали свыше сотни представителей более чем сорока литовских государственных ведомств и научных организаций. «Посредством этих учений мы хотим наладить более тесное сотрудничество литовских структур в области кибернетической безопасности и обучить их представителей, чтобы они смогли применить полученный опыт в случае возникновения реальной угрозы», – заявил тогдашний министр обороны Юозас Олекас.

По его словам, в Литве решили уделить особое внимание данной сфере после того, как неизвестные хакеры взломали 10 июня 2015 года сайт Объединенного штаба вооруженных сил страны. Взломщики выложили на портале информацию о том, что целью начавшихся тем летом в странах Прибалтики и Польше учениях НАТО Saber Strike якобы является подготовка к аннексии Калининградской области. Позднее текст был удален. После этого с января 2016 года в Литве начал действовать Национальный центр кибернетической безопасности.

Также в стране узаконили возможность отключить любому человеку интернет при возникновении подозрений в «незаконной деятельности пользователя».

В 2016 году Литва пережила очередную крупную кибератаку, временно выведшую из строя сайты парламента и множества министерств. Власти привычно заявили, что за атакой «стоит Кремль». Но спустя год в прокуратуре вынуждены были признать, что порталы госведомств взломали дети: двое несовершеннолетних граждан Литвы и один датский подросток. А начале июля 2017 года Эдвинас Кярза и помощник генерального секретаря НАТО Сорин Дукару подписали в Брюсселе договор об укреплении сотрудничества в сфере кибербезопасности. Кярза тогда сказал, что «кибербезопасность является частью коллективной обороны, мы должны быть готовы вместе с союзниками в случае угрозы защищать это пространство».

Так закладывались первые кирпичики в воздвигнутое впоследствии здание Кибернетических сил Евросоюза быстрого реагирования. Однако есть сомнения в том, что функции CRRT будут чисто оборонительными...» ***(Андрей Винников. Прибалтика назначена ответственной за битву с «русскими хакерами» // Деловая газета «Взгляд» (https://vz.ru/world/2020/4/1/1031587.html). 01.04.2020).***

***

«Использование искусственного интеллекта поможет разведке Великобритании бороться с новыми видами угроз со стороны других государств.

Об этом говорится в отчете британского Королевского Объединенного института оборонных исследований (RUSI), сообщает Express.

«Использование искусственного интеллекта рекомендуется британской разведке для борьбы с новыми угрозами», – говорится в сообщении.

Согласно отчету RUSI, противники Британии могут использовать технологии на основе искусственного интеллекта для атак в киберпространстве и на политическую систему страны.

В частности, приводятся примеры таких атак в виде распространения обработанных по технологии «deep fake» фотографий и видео для манипулирования мнением и выборами.

По мнению экспертов, нужно уже начинать использовать искусственный интеллект, который сможет выявить и остановить онлайн кибератаки еще до того, как они появятся». ***(В Британии на борьбу с кибератаками могут "мобилизовать" искусственный интеллект // «Новости онлайн 24» (https://newsonline24.com.ua/v-britanii-na-borbu-s-kiberatakami-mogut-mobilizovat-iskusstvennyj-intellekt/). 28.04.2020).***

***

Захист персональних даних

«Издание ZDNet пишет, что в даркнете были выставлены на продажу личные данные 600 000 пользователей почтового провайдера Email.it. Представители провайдера уже подтвердили, что информация о компрометации правдива.

Взлом Email.it заметили в минувшие выходные, когда хакеры стали рекламировать в Twitter, сайт в даркнете, на котором они продают похищенные у компании данные. Интересно, что группировка, называющая себя NN (No Name) Hacking Group, утверждает, что сам взлом произошел более двух лет назад, в январе 2018 года.

«Мы взломали дата-центр Email.it более двух лет назад, и внедрились как APT. Мы изъяли все возможные конфиденциальные данные с их сервера, а затем решили дать им шанс ис править дыры [в безопасности], потребовав небольшую награду. Они отказались общаться с нами и продолжали обманывать своих пользователей/клиентов. Они не связывались со своими пользователями/клиентами после взломов!», — пишут злоумышленники.

Другой сообщение на сайте группировки, содержит чуть больше деталей. Согласно нему, еще 1 февраля 2020 года хакеры попытались вымогать у представителей Email.it деньги. Теперь представитель почтового провайдера сообщили ZDNet, что компания действительно отказалась платить вымогателям, и вместо этого уведомила о случившемся правоохранительные органы.

Теперь же хакеры пытаются монетизировать попавшую к ним информацию другим путем и продают пользовательские данные по цене от 0,5 до 3 биткоинов (от 3500 до 22 000 долларов). Группировка утверждает, что владеет 46 базами данных, которые были украдены у Email.it.

Похищенные БД содержат информацию о пользователях, которые имели бесплатные учетные записи электронной почты. Утверждается, что дамп содержит незашифрованные пароли, контрольные вопросы, содержимое электронной почты и вложения более чем для 600 000 человек, которые зарегистрировались и использовали сервис в период между 2007 и 2020 годами. Также хакерам якобы удалось заполучить SMS-сообщения, отправленные через службу SMS-рассылки Email.it.

Помимо содержимого дамп злоумышленники хвастаются и тем фактом, что им удалось удалить исходный код всех веб-приложений Email.it, включая приложения для администраторов и клиентов.

В ходе беседы с журналистами представители провайдера не опровергали заявления хакеров. В компании лишь подчеркнули, что на взломанном сервере не было никакой финансовой информации, а также данных платных клиентов. Сообщается, что брешь на ранее уязвимом сервере в настоящее время уже была закрыта». ***(Мария Нефёдова. Из-за взлома почтового провайдера данные 600 000 человек попали в продажу в даркнете // Xakep (https://xakep.ru/2020/04/07/email-it-hacked/). 07.04.2020).***

***

«Недавно Facebook подал иск против известной израильской компании NSO Group, разработчика шпионского ПО Pegasus, обвинив её в использовании уязвимости в приложении WhatsApp, владельцем которого является Facebook. Согласно иску, это привело к компрометации 121 пользователей WhatsApp в Индии. Неизвестные хакеры, получившие доступ к этой уязвимости, пробовали взломать доступ к аккаунтам 121 потенциальных жертв; аккаунты 20 пользователей были скомпрометированы в ходе осуществленных атак.

В ходе судебного разбирательства выяснилось, что ранее Facebook попытался купить шпионское ПО Pegasus. Об этом сообщил ответчик в суде.

Pegasus способен извлекать данные пользователей из облачных хранилищ Apple, Google, Facebook, Amazon и Microsoft. Данные экспортируются, предоставляя операторам ПО доступ к конфиденциальным данным пользователя. Собираемые данные включают в себя все сообщения и фотографии, учетные данные для входа в систему, а также информацию о местоположении устройства.

NSO Group имеет весьма неоднозначную репутацию, поскольку продает свои продукты не только правоохранительным органам, но и авторитарным правительствам, преследующим правозащитников и журналистов. Но по словам генерального директора NSO Group Шалева Хулио (Shalev Hulio), два представителя Facebook обратились к компании в октябре 2017 года и намеревались приобрести право на использование определенных возможностей Pegasus.

«По словам представителей компании, Facebook был обеспокоен тем, что его метод сбора пользовательских данных с помощью приложения Onavo Protect менее эффективен на Apple-устройствах, чем на Android. Facebook хотел использовать предполагаемые возможности Pegasus для мониторинга пользователей Apple-устройств и готов был заплатить за возможность мониторинга пользователей Onavo Protect», — сообщается в судебном документе.

В ответ на эти заявления представители Facebook заявили, что представители NSO неверно изложили суть переговоров. Согласно их позиции, NSO пытается сейчас ввести в заблуждение общественность, чтобы отвлечь от обсуждения фактов, связанных со взломом Pegasus.

В ответ представители израильской компании заявили, предоставляли доступ к Pegasus только для правоохранительных органов и спецслужб. С их слов, они отказали Facebook в покупке по причине того, что Facebook — это частная компания, поэтому она не удовлетворяет их требованиям.

Согласно отчету, Apple обязала Facebook удалить Onavo Protect из магазина приложений iOS App Store. Однако Facebook пошел дальше и удалил это приложение также из магазина Google Play». ***(Facebook судится с компанией, у которой соцсеть пыталась купить шпионский софт // РосКомСвобода (https://roskomsvoboda.org/57089/). 07.04.2020).***

***

«Сводная группа исследователей из Университета штата Огайо, Нью-Йоркского университета и Центра информационной безопасности CISPA Helmholtz провела масштабное исследование, изучив в общей сложности более 150 000 приложений. В том числе из Google Play (100 000 лучших приложений из магазина), приложения из альтернативных источников (20 000 приложений), и предустановленные на устройствах приложения (примерно 30 000 приложений, извлеченных из прошивок смартфонов Samsung).

Для проведения анализа эксперты создали специальный инструмент, получивший название INPUTSCOPE. Он предназначен для анализа контекста выполнения валидации user input, а также контента, вовлеченного в эту валидацию.

«Мы полагаем, что валидация ввода в мобильных приложениях может использоваться для раскрытия секретов, таких как тайные бэйдоры, секретные черные списки, а также скрытая функциональность, обеспечивающая доступ только к функциям администратора и связанная с input’ом, что широко распространено в приложениях для Android», — пишут эксперты в своем докладе.

Анализ, выполненный с помощью INPUTSCOPE, показал, что 12 706 приложений содержат различные бэкдоры, включая секретные ключи доступа, мастер-пароли и секретные команды. Все это, по словам аналитиков, может помочь злоумышленникам получить несанкционированный доступ к учетным записям пользователей. Кроме того, если злоумышленник имеет физический доступ к устройству, на котором установлено одно из таких приложений, он сможет предоставить доступ к устройству и третьим лицам, а также разрешить им запускать код на устройстве с повышенными привилегиями (благодаря скрытым секретным командам, присутствующим в полях ввода).

В общей сложности эксперты выявили более 6800 приложений со скрытыми бэкдорами и функциями в магазине Play Store, более 1000 в сторонних магазинах приложений и почти 4800 подозрительных приложений, которые были предварительно установлены на устройствах Samsung.

«Изучив несколько мобильных приложений вручную, мы обнаружили, что популярное приложение для удаленного управления (более 10 000 000 установок) содержит мастер-пароль, который способен разблокировать доступ даже при удаленной блокировке, установленной владельцем телефона в случае утери устройства», — рассказывают специалисты.

Также они обнаружили, что другое популярное приложение для блокировки экрана (5 000 000 установок) использует ключ доступа для сброса паролей произвольных пользователей, чтобы иметь возможность разблокировать экран и войти в систему.

Еще одно приложение для потокового вещания (5 000 000 установок) содержит ключ доступа для входа в интерфейс администратора, с помощью которого злоумышленник может изменить настройки приложения и разблокировать дополнительные функции.

И, наконец, популярное приложение для перевода (1 000 000 установок) содержит секретный ключ, который используется для обхода оплаты за расширенную функциональность, в том числе удаление рекламы в приложении…

Как видно из примеров, приведенных исследовательской группой, некоторые проблемы явно представляют угрозу безопасности пользователя и данных, хранящихся на устройстве, тогда как другие являются лишь безвредными «пасхалками» или отладочными функциями, которые случайно вошли в рабочую версию.

Еще до публикации доклада аналитики уведомили о своих изысканиях всех разработчиков приложений, в которых были обнаружены скрытое поведение или механизмы, похожие на бэкдоры. Увы, далеко не все разработчики ответили, хотя некоторые приложения все же были отредактированы и избавились от скрытой функциональности.

Также стоит отметить, что INPUTSCOPE анализировал поля ввода в приложениях, и побочным продуктом этого исследования стало обнаружение приложений, которые используют скрытые фильтры ненормативной лексики или политически мотивированные черные списки. В целом были найдены 4028 приложений для Android, которые обладают скрытыми черными списками для полей ввода. Черные списки предназначались для контента на китайском, английском и корейском языках и различались по размеру: от 7 до 10 000 пунктов в списке». ***(Мария Нефёдова. Тысячи Android-приложений содержат мастер-пароли, секретные ключи и команды // Xakep (https://xakep.ru/2020/04/06/inputscope/). 06.04.2020).***

***

«В Google Play появилось, и достаточно быстро исчезло приложение «Социальный мониторинг», однако пользователи и эксперты в области IT

успели проверить его на уязвимости, а также провести достаточно детальное исследование программы.

Первым внимание на приложение обратил Telegram-канал «Нецифровая экономика». Разработчиком программы указана подведомственная московской мэрии организация ГКУ «Информационный город».

«Правда, как выяснилось (здесь и далее – по информации телеграм-канала @itsorm) разработчиком числится некая компания «Гаскар», она же wokkalokka, — пишет Telegram-канал «Методичка». — Но разработчик – не главная проблема. В существующей версии приложение требует все возможные виды разрешений для установленных программ: от доступа к камере и местоположению до (по некоторым данным) привязки к приложению «Сбербанка». При этом передача данных происходит на сервер мэрии Москвы, а изображений – на мощности эстонского сервиса по распознаванию лиц identix.one, расположенные в Германии. Важно отметить — передаваемые данные незашифрованы и содержат сведения об идентификаторах смартфона и модуля связи (MAC/IMEI)».

Кроме этого, приложение требует дать доступ на передачу геолокации, доступ к управлению Bluetooth и носимым устройствам…

Исполнительный директор ОЗИ Михаил Климарёв заметил, что пользователи устроили в Google Play обвал `рейтинга данного приложения, ставя ему одну звёздочку, а также сопровождая это негативными комментариями. Он также посоветовал пользователям пожаловаться на нарушение программой приватности, чтоб Google удалил его из магазина приложений. Возможно, это стало причиной того, что сейчас программа недоступна, но это пока только наше предположение.

Достаточно детально приложение разобрал создатель TgVPN и владелец Telegram-канала «IT и СОРМ» Владислав Здольников, который представил промежуточные итоги изучения этой программы:

- Приложение получает доступ ко всей информации на телефоне: GPS, камера, местоположение, возможность звонить, просмотр любых данных, доступ к любым настройкам.
- Приложение передаёт собранную информацию на серверы мэрии в открытом виде без какого-либо шифрования. Это провал.
- Для распознавания лиц, приложение использует эстонский сервис identix.one — то есть, передаёт фотографии в эстонскую юрисдикцию и на серверы, расположенные в Германии. Обе страны входят в НАТО.
- Разработкой приложения занимается компания «Гаскар», подрядчик «Инфогорода».
- В QR-кодах зашифрованы MAC и IMEI (индивидуальные идентификаторы) устройства.
- На приложение было потрачено 180 млн рублей. Судя по его качеству, украдено было 99% бюджета.

«Это полнейший провал и позорище. ДИТ Москвы должен быть разогнан палками за такое», — считает он.

С ним согласен IT-специалист, разработчик Денис Евстигнеев, который дал РосКомСвободе свой комментарий: «Предположительно, приложение «Социальный мониторинг», разработанное компанией «Гаскар», подрядчикм

«Инфогорода» будет использоваться правительственными структурами Москвы для выдачи разрешения на выход из дома (вынести мусор, выгул собаки, покупка еды и т.д.). Из выложенного кода программы совершенно однозначно понятно: у Вас от правительство больше не будет НИКАКИХ секретов».

Разработчиком приложения для слежки указаны wokkalokka — некие ребята, которые делали приложение для детских смарт часов с трекингом. Ссылка на них же есть в privacy policy приложения.https://t.co/ornFU8btqk

— Vladislav (@unkn0wnerror) March 31, 2020

«Если вы что-то разработали, написали, всё будет доступно правительственным органам и множеству третьих лиц, — продолжает он. — С учетом объявления, что данные с сайта Госуслуг сегодня снова благополучно оказались доступны в сети Интернет рядовым пользователям. Во-первых, программа при установке требует ряд разрешений, которые дают возможность в произвольное время включить и выключать камеру, вести запись и отправлять это всё (по совершенно открытому протоколу) на сайт http://watch.telemetry.mos.ru (это можно увидеть при помощи программы tcpdump). Программа получает доступ ко ВСЕМ сетевым интерефейсам, Wi-Fi, BlueTooth. Т.е., телефон, подключённый в доме может преспокойненько «слить» данные о вашей домашней сети, о переговорах в мессенджерах и т.д. Сервис для распознавания лиц находится вообще в Эстонии (identix.one)! То есть наши данные отправляются за рубеж. На сайте https://github.com/iTaysonLab/gorkiy выложен исходный код программы. В QR-коде для слежки за жителями Москвы зашифрованы MAC/IMEI девайса».

Денис Евстигнеев тоже советует жаловаться администрации Google Play на данную программу как нарушающую приватность и не соответствующую мало-мальским требованиям безопасности:

«К сожалению, бесполезно ставить «звёздочки» (одну звёздочку), как это предлагалось изначально на некоторых каналах. Чтобы эту программу удалили с Google Play, нужно жаловаться.

Если этой программой нас заставят пользоваться, нет никакой гарантии, что эти данные не окажутся у третьих лиц. Перехватить такой трафик не составит никакого труда. Самое неприятное, что отказаться от установки этой программы мы не можем: это же разрешение на выход из дома.

И всё же, на телефон такую программу ставить НЕЛЬЗЯ. Она будет Вашим личным шпионом-доносчиком. Её нельзя ставить на телефон от слова «СОВСЕМ».

Московский власти, между тем, уже успели отреагировать на ту волну негодования, которая поднялась в Сети.

Приложение «Социальный мониторинг», контролирующее соблюдение режима самоизоляции, предназначено не для широкого пользования, а для пациентов с коронавирусом, которые будут лечиться на дому. Об этом в эфире «Эха Москвы» в среду заявил глава департамента информационных технологий (ДИТ) Эдуард Лысенко. По его словам, поскольку приложение будет работать не на всех платформах, больных на время самоизоляции обеспечат смартфоном, который после придется сдать. Полная версия приложения будет доступна в четверг. Сейчас оно больше недоступна в Google Play, куда тестовую выложили для сбора оценок со стороны экспертного сообщества.

С конца марта текущего года в Москве действует режим обязательной самоизоляции. Жителям запрещено покидать квартиру, исключение делается только для похода в магазин, выноса мусора или прогулки с собакой. В ближайшее время жителям столицы потребуется получать QR-код на сайте мэрии для каждого выхода из квартиры. Отслеживать передвижения жителей в режиме самоизоляции с помощью системы распознавания лиц на базе технологии NtechLab. Недавно в Сети были опубликованы «регламенты работы» после введения в столице пропускного режима. В частности, в одном из слайдов говорится о приложении «Социальный мониторинг» для «больных с домашним размещением»…». ***(Эксперты назвали приложение от правительства Москвы шпионской программой // РосКомСвобода (https://roskomsvoboda.org/56900/). 01.04.2020).***

***

«Эксперты сервиса мониторинга утечек данных Under the Breach обратили внимание, что один из популярнейших хакерских форумов в интернете, OGUSERS (он же OGU), сообщил о компрометации уже второй раз за последний год.

«Похоже, что кто-то сумел взломать сервер через шелл в загрузке аватаров в форумном софте и получил доступ к нашей текущей базе данных, датируемой 2 апреля 2020 года», — пишет администратор OGUSERS.

В итоге неизвестный злоумышленник похитил данные 200 000 пользователей, если верить официальной статистике пользователей, указанной на самом форуме. В настоящее время OGUSERS отключен и переведен в режим обслуживания.

Перед временным закрытием сайта администраторы уведомили пользователей о том, что сбрасывают пароли, а также призвали всех включить двухфакторную аутентификацию для своих учетных записей, чтобы похищенные в ходе атаки данные нельзя было использовать для взлома аккаунтов.

Напомню, что прошлый взлом OGUSERS произошел в мае 2019 года. Тогда атакующие проникли на сервер через уязвимость в одном из кастомных плагинов и получили доступ к бэкапу, датированному 26 декабря 2018 года.

Журналисты Vice Motherboard, изучившие копию украденной БД, подтверждали, что она подлинная. Также утечку исследовал известный ИБ-журналист Брайан Кребс (Brian Krebs), который тоже подтвердил подлинность данных и отметил, что дамп содержал информацию о 113 000 пользователей OGU. Похищенная у OGU база данных потом распространялась на других хакерских форумах.

UPD.

Утром 3 апреля 2020 года была замечено, что похищенная БД уже опубликована на конкурирующих хак-форумах, тогда так же, как и в прошлом году.

OGUSERS начинал свою работу как сайт, где продавали угнанные учетные записи на самых разных платформах и сервисах. Но если все начиналось с «интересных» аккаунтов в социальных медиа (Twitter, Instagram) с уникальными или короткими юзернеймами, то позже развилось в полноценный ресурс по

продаже любых аккаунтов, в числе которых были учетные записи пользователей PlayStation Network, Steam, Domino's Pizza и так далее…». ***(Мария Нефёдова. Хакерский форум OGUsers взломан второй раз за год // Хакер (https://xakep.ru/2020/04/03/ogusers-hacked/). 03.04.2020).***

***

«Только вчера мы писали о том, что специалисты компании IntSights обнаружили в продаже дамп, в который входят учетные данные пользователей Zoom (email, пароли), а также идентификаторы собраний, имена и ключи хостов. Тогда речь шла о сравнительно маленькой БД, содержащей лишь около 2300 записей. Теперь же эксперты компании Cybersecurity Cyble сообщили, что на хакерских форумах и в даркнете можно найти примерно 500 000 учетных записей Zoom, которые порой раздают вообще бесплатно.

О своей находке специалисты рассказали журналистам издания Bleeping Computer. Исследователи соглашаются с мнением коллег из IntSights и пишут, что найденные ими учетные данные – это результат атака типа credential stuffing. Таким термином обозначают ситуации, когда имена пользователей и пароли похищаются с одних сайтов, а затем используются против других. То есть злоумышленники имеют уже готовую базу учетных данных (приобретенную в даркнете, собранную самостоятельно и так далее) и пытаются использовать эти данные, чтобы авторизоваться на каких-либо сайтах и сервисах под видом своих жертв.

Торговлю аккаунтами Zoom эксперты заметили еще 1 апреля 2020 года. Они отмечают, что некоторые злоумышленники раздают взломанные аккаунты бесплатно, таким образом пытаясь завоевать себе репутацию в хакерском сообществе. Так, приведенный ниже пример демонстрирует список из 290 учетных записей, принадлежащих Университету Вермонта, Университету Колорадо, Дартмутскому колледжу, Университету Флориды и многим другим. Все они были опубликованы бесплатно.

Журналисты Bleeping Computer связались с несколькими пострадавшими из списка, используя указанные адреса электронной почты, и удостоверились, что такие учетные записи действительно существуют. Один из пользователей сообщил изданию, что приведенный в списке пароль был старым, то есть некоторые учетные данные, вероятно, были результатом более старых атак credential stuffing.

Заметив, что один из злоумышленников торгует учетными записями Zoom на хакерском форуме, специалисты Cyble связались с ним и договорились о покупке большого количества аккаунтов (чтобы предупредить своих клиентов о потенциальных проблемах). Таким образом Cyble удалось приобрести информацию примерно о 530 000 учетных записях Zoom по цене всего 0,0020 долларов за одну учетную запись

Купленные исследователями данные включали адреса электронной почты, пароли, URL-адрес собраний, а также ключи хостов (HostKey). Среди этих аккаунтов обнаружились учетные записи, принадлежащие таким известным компаниям, как Chase и Citibank, крупным учебным заведениям и не только. Кроме

того, исследователям удалось подтвердить подлинность части данных, проверив учетные записи, принадлежащие клиентам компании.

Специалисты напоминают, что повторное использование один и тех же паролей – это скверная идея, и рекомендуют пользователям, которые практикуют подобное, не рисковать и сменить пароли как можно скорее.» ***(Мария Нефёдова. Данные 500 000 аккаунтов Zoom продаются на хакерских форумах // Хакер (https://xakep.ru/2020/04/14/zoom-leaks/). 14.04.2020).***

***

«Учетные данные 3 954 416 пользователей торговой площадки Quidd были были опубликованы на общедоступном хакерском форуме.

Торговая online-площадка для продажи наклеек, карточек, игрушек и других предметов коллекционирования, стала жертвой взлома и теперь данные миллионов пользователей бесплатно распространяются на подпольных форумах.

Как сообщило издание ZDNet, похищенная информация включает логины пользователей Quidd, адреса электронной почты и хеши паролей. Пользователь форума под псевдонимом ProTag в прошлом месяце разместил копию данных Quidd на общедоступном хакерском форуме и с тех пор информацией начали обмениваться другие его участники. По его словам, первые объявления о продаже похищенных данных появились в узких преступных кругах еще в октябре 2019 года.

Об утечке впервые сообщили специалисты из компании Risk Based Security, которые также «после первоначального анализа подтвердили подлинность данных». Несмотря на тот факт, что пароли хранились в зашифрованном виде, злоумышленники уже начали работу над их расшифровкой. Один из них выставил на продажу доступ к более чем 135 тыс. взломанных паролей, а другой — к более чем одному миллиону.

Quidd не сообщала ранее о каких-либо инцидентах безопасности, и неясно, знает ли компания о взломе. Пользователям Quidd рекомендуется сменить пароли к учетным записям как можно скорее.» ***(Данные 4 млн пользователей Quidd оказались в открытом доступе // SecurityLab.ru (https://www.securitylab.ru/news/506623.php). 14.04.2020).***

***

«Web-сайты SFOConnect[.]com и SFOConstruction[.]com международного аэропорта Сан-Франциско стали объектами кибератаки в марте 2020 года, в ходе которой преступники загрузили вредоносное ПО для хищения учетных данных пользователей. О данном инциденте сообщило руководство аэропорта на официальном сайте.

Неизвестно, удалось ли преступникам похитить какие-либо данные, но в противном случае украденные учетные данные могут предоставить злоумышленникам доступ к сети аэропорта. Как сообщается на сайте, «у некоторых пользователей, которые могли стать жертвой атаки, есть доступом к данным ресурсам за пределами сети аэропорта».

Руководство аэропорта после атаки отключило сайты и принудительно сбросило пароли. В настоящее время работа ресурсов восстановлена. Остается неизвестным, существовали ли какие-либо дополнительные средства защиты, такие как многофакторная аутентификация, для предотвращения взлома сайтов…» ***(Преступники взломали два web-сайта аэропорта Сан-Франциско // SecurityLab.ru (https://www.securitylab.ru/news/506618.php). 14.04.2020).***

***

«Боб Дьяченко, исследователь кибербезопасности в Украине, проводит часть своих дней в поисках на просторах Интернета множества данных, которые не защищены должным образом, чтобы найти уязвимые места и поставить защиту от хакеров.

В прошлом месяце Боб наткнулся на незащищенный сервер, хранящий информацию о 42 миллионах аккаунтов из Ирана, привязанных к мессенджеру Telegram.

Не было никаких прямых подсказок относительно того, кто получил данные и разместил их на сервере. Была только целевая страница, вся черная, с логотипом белого орла и посланием на фарси.

«Добро пожаловать в систему охоты», - говорится в сообщении на странице.

Дьяченко заявил, что уведомил иранское агентство по кибербезопасности, и вскоре после этого сервер был отключен.

Но прежде чем он исчез, другие киберлейты начали собственное расследование. В конечном итоге это привело их к хакерской группе с невероятным никнеймом - «Очаровательный котенок» (Charming Kitten – англ.) и поразительным выводом: Дьяченко наткнулся на шпионскую операцию иранского правительства.

«Уже более 10 лет я слежу за иранскими кибератаками и слежкой, и я никогда не видел ничего подобного», - сказал Амир Рашиди, иранский исследователь в области интернет-безопасности и цифровых прав, базирующийся в Нью-Йорке. «Они могли бы использовать это, чтобы преследовать моих родственников, моих друзей, мою семью».

Множество данных, части которых были просмотрены Bloomberg News, содержали имена пользователей, телефонные номера, биографии пользователей и уникальные коды - или «хэши» - связанные с учетными записями, хранящимися на сервере.

Неясно, были ли данные в основном от пользователей Telegram или от пользователей неофициальных версий приложения, которые стали популярными после того, как Telegram был запрещен в Иране в 2018 году. Некоторые неофициальные приложения, использующие тот же исходный код, что и Telegram, были ранее связаны с правительством Ирана.

В любом случае, эти данные могут быть использованы для клонирования учетных записей людей и отслеживания частных сообщений, идентификации пользователей, которые используют Telegram анонимно, или рассылки пропаганды или дезинформации, направленных на конкретные группы, говорит Дьяченко.

Рашиди сказал, что ранее было известно о том, что Иран избирательно взламывал аккаунты отдельных людей. Однако, «система охоты» показывает, что иранские власти используют новые и более агрессивные методы сбора и анализа огромных массивов данных о своих гражданах, говорит Амир.

«Это первый раз, когда я увидел доказательства того, что они пытаются проанализировать данные в широком масштабе», - сказал Рашиди.

В сообщении Telegram присланном Bloomberg по email говорится, что, по мнению компании, данные получены из неофициальных версий приложения, используемых в Иране, которые могли тайно собирать информацию о пользователях Telegram с телефонов людей.

«Образцы данных, которые мы смогли изучить, ясно показывают, что информация собиралась с использованием сторонних приложений, которые крали данные у их пользователей», - сказал Маркус Ра, представитель Telegram.

«Если один из ваших друзей, у которого есть ваш номер, использовал вредоносное приложение, ваш номер и имя пользователя могут оказаться в базе данных», например в «системе охоты», сказал Ра, «даже если вы сами не использовали это вредоносное приложение».

По крайней мере, некоторые из пользовательских аккаунтов в базе данных связаны с активными пользователями официального приложения Telegram на основе обзора, сравнивающего учетные записи на сервере и в приложении. Отметки времени показывают, что некоторые аккаунты пользователей Telegram были доступны только в марте 2020 года.

Кибер-полиция Ирана пока не комментирует ситуацию с утечкой данных. Амир Наземи, заместитель министра в министерстве связи и информационных технологий Ирана, заявил, что подал жалобу на нарушение данных в Генеральную прокуратуру Ирана. Он отказался комментировать, были ли киберполиция или другие правительственные учреждения вовлечены в «систему охоты».

Об обнаружении сервера Бобом Дьяченко было сообщено в компьютерной торговой публикации. Несколько иранских исследователей в области кибербезопасности продолжают изучать данные.

Один из них, Мохаммад Джорджанди, который живет и работает в США, обнаружил, что сервер, хранящий пользовательские данные, был зарегистрирован в офисе на северо-западе Тегерана человеком по имени Манучехр Хашемлу (Hashemloo).

Используя онлайн-записи Bloomberg News, Джорджанди установил, что Hashemloo использовал тот же адрес Gmail, который использовал известный хакер, связанный с иранским правительством. Хакер, который использует никнейм ArYaIeIrAN, был связан с предполагаемой хакерской группой, спонсируемой правительством Ирана, известной как «Очаровательный котенок», которая ранее атаковала иранских диссидентов, ученых, журналистов и правозащитников.

Джорджанди пришел к выводу, что люди, которые настроили сервер «системы охоты», вероятно, работали на правительство Ирана.

ClearSky Cyber Security также ранее обнаружила несколько хакерских операций, выполненных ArYaIeIrAN связанным с Hashemloo, и в отчете 2017 года

упоминается адрес Gmail хакера, который связан с операциями, выполняемыми «Очаровательным котенком».

Другой иранский исследователь безопасности сказал, что Hashemloo был «известным человеком в безопасности и хакерском обществе» в Иране, чье имя было во многих кибер-операциях правительства Ирана. Исследователь, который живет в Иране и просит анонимности из-за проблем безопасности, сказал, что «система охоты», вероятно, была порталом для иранского агентства кибер-полиции, которое было создано в 2011 году отчасти для целевых групп инакомыслящих и критиков правительства.

Взломы «Очаровательного котенка» были задокументированы исследователями в течение нескольких лет.

В своем отчете за 2017 год ClearSky задокументировал, что Charming Kitten создал поддельные новостные сайты, в том числе один с именем britishnews.com, и попытался взломать компьютеры журналистов, правозащитников и исследователей из Европы и Ближнего Востока.

В прошлом году ClearSky заявил, что та же группа хакеров попыталась взломать учетные записи электронной почты нынешних и бывших должностных лиц США, людей, связанных с нынешней президентской кампанией в США, журналистов, освещающих глобальную политику, и известных иранцев, живущих за пределами Ирана.

«У нас есть веские доказательства того, что Charming Kitten является хакерской группой, спонсируемой государством Иран», сказал Охад Зайденберг, ведущий исследователь компании в области кибер-разведки.

Зайденберг сказал, что он не смог узнать, кто стоит за «системой охоты». Но в прошлом, по его словам, группа Charming Kitten предназначалась для пользователей Telegram.

Ранее группа создала вредоносный веб-сайт, который был похож на страницу входа в Telegram, утверждает Зайденберг.

В течение многих лет иранцы использовали Telegram в качестве средства связи, используя шифрование для защиты личных сообщений. Приложение также позволяет пользователям присоединяться к группам, где они могут узнать о новостях, которые подвергаются цензуре со стороны государственных СМИ в стране.

После запрета на Telegram некоторые иранцы обошли его, используя программное обеспечение, такое как виртуальные частные сети, что позволило им обойти блокировку страны на веб-сайте Telegram, сообщает Рашиди.

Другие начали скачивать неофициальные версии Telegram, называемые Hotgram и Telegram Gold, которые используют тот же базовый код, что и официальное приложение, но не управляются Telegram.

Эксперты по кибербезопасности подозревают, что неофициальные приложения могли быть разработаны иранским правительством в качестве средства контроля за гражданами страны.

В мае 2019 года Нассролла Пежманфар, член парламента Ирана, подтвердил эти подозрения, заявив, что Telegram Gold и Hotgram были профинансированы

разведывательными и коммуникационными министерствами Ирана, которые, по его словам, потратили около $90 млн. на их создание.

«Было очевидно, что они связаны с властями Ирана», - говорит Махса Алимардани, исследователь, специализирующийся на Иране в Оксфордском интернет-институте. «Они подвергали цензуре контент на платформах и пытались централизовать контроль над пользователями».

Telegram предупредил иранцев против использования неофициальных приложений. В прошлом году они были удалены из Google Play Store по соображениям безопасности.

«К сожалению, несмотря на наши предупреждения, люди в Иране все еще используют непроверенные приложения», - сказал Ра, представитель Telegram». ***(Романов Роман. Украинский исследователь кибербезопасности обнаружил в Telegram шпионскую систему Ирана // InternetUA (http://internetua.com/ukrainskii-issledovatel-kiberbezopasnosti-obnarujil-v-telegram-shpionskuua-sistemu-irana). 18.04.2020).***

***

«Издание ZDNet сообщает, что у каталога приложений Aptoide произошла крупная утечка пользовательских данных. Согласно официальным данным, португальский магазин приложений используют более 150 миллионов человек по всему миру.

По информации журналистов и сервиса по мониторингу утечек Under the Breach, на известном хакерском форуме были опубликованы 20 000 000 записей, которые являются частью более крупного дампа, насчитывающего уже 39 000 000 записей. По словам хакера, эти данные были получены после взлома Aptoide, произошедшего ранее в этом месяце.

Дамп представляет собой экспортированную из PostgreSQL БД и содержит информацию о пользователях, которые зарегистрировались или использовали Aptoide в период с 21 июля 2016 года по 28 января 2018 года. Информация о пользователях включает в себя адрес электронной почты, хешированный пароль, настоящее имя, дату регистрации, IP-адрес регистрации, информацию об устройстве и дата рождения (если указана).

Также доступна различная техническая информация, такая как состояние учетной записи, токены регистрации, токены разработчика, данные о том, являлась ли учетная запись суперадминистратором или источником рефералов…». ***(Мария Нефёдова. Данные 20 млн пользователей каталога приложений Aptoide опубликованы на хакерском форуме // Xakep (https://xakep.ru/2020/04/20/aptoide-hacked/). 20.04.2020).***

***

«Злоумышленники выставили на продажу в даркнете более 267 млн профилей Facebook за £500 (примерно $620). Хотя ни одна из данных записей не содержит пароли, хранящаяся в них информация может позволить мошенникам организовать фишинговые атаки с целью кражи учетных данных.

В прошлом месяце эксперт в области безопасности Боб Дьяченко (Bob Diachenko) обнаружил открытую базу данных Elasticsearch, содержавшую более 267 млн записей Facebook. Большинство записей содержали полное имя пользователя, его номер телефона и уникальный идентификатор Facebook.

Интернет-провайдер, управляющий IP-адресом сервера, в конечном итоге отключил его, однако вскоре после этого к сети был подключен второй сервер, содержащий те же данные, а также дополнительные 42 млн записей. Сервер был незамедлительно атакован, при этом атакующие оставили его владельцам сообщение о том, что им необходимо позаботиться о защите своих серверов. 16,8 млн записей среди новых похищенных данных содержали адреса электронной почты пользователей Facebook, информацию о дате рождения и поле. Как предположил Дьяченко, серверы принадлежали криминальной организации, которая похитила данные с помощью API Facebook, прежде чем они были заблокированы, или использовала технологию web-скрейпинга для извлечения данных из профилей Facebook.

Как сообщил ресурс BleepingComputer, специалисты из ИБ-фирмы Cyble обнаружили злоумышленника, продающего базу данных за £500 на хакерских форумах. Исследователи приобрели базу данных для проведения анализа и добавили ее в свой сервис уведомления о нарушениях AmIbreached[.]com». ***(267 млн профилей Facebook выставлены на продажу в даркнете за $620 // SecurityLab (https://www.securitylab.ru/news/506906.php). 21.04.2020).***

***

«В конце апреля 2020 года Федеральный суд США вынес вердикт, согласно которому Facebook должна будет заплатить $5 млрд за утечку конфиденциальных данных, принадлежащих десяткам миллионов клиентов.

Помимо штрафа, постановление требует, чтобы Facebook усилила защиту конфиденциальных данных, предоставлял подробные квартальные отчеты о соблюдении соглашения и позволял контролировать свою деятельность независимому наблюдательному совету.

Некоторые активисты по защите конфиденциальности негативно отреагировали на судебное решение, утверждая, что американские власти позволили Facebook легко отделаться после скандала с Cambridge Analytica и похищением данных миллионов пользователей. Однако председатель Федеральной торговой комиссии США Джо Саймонс (Joe Simons) заявил, что он «доволен» решением суда, и отметил, что это самый крупный штраф, когда-либо выписанный агентством по защите прав потребителей.

«В то же время, суд требует от Facebook контролировать конфиденциальность данных на каждом этапе своей деятельности и обеспечивать существенно большую прозрачность и ответственность за решения своих руководителей, касающиеся конфиденциальных данных», - сказал Саймонс.

Соглашение выходит за рамки мер, обычно требуемых законодательством США, и должно «служить примером более строгого контроля защиты конфиденциальных данных», заявил в своем блоге директор по конфиденциальности Facebook Мишель Протти (Michel Protti).

«Мы надеемся, что это дело станет толчком к дальнейшему прогрессу в разработке соответствующего законодательства в США и других странах», - сказал Протти. По его словам, после суда Facebook создал десятки команд, которые занимаются вопросами конфиденциальности, и тысячи людей работают над проектами, связанными с ее защитой». ***(Facebook заплатит $5 млрд за утечку данных десятков миллионов клиентов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5660591-Facebook-zaplatit-5-mlrd-za-utechku.html). 27.04.2020).***

***

Кібербезпека Інтернету речей

«Для удобства использования люди зачастую подключают бытовую или офисную технику (мониторы, датчики или кухонные электроприборы) к беспроводным сетям. Интернет вещей выгоден тем, что позволяет эффективно управлять ресурсами, а также значительно экономить деньги и время. Именно поэтому различные организации активно пользуются данной технологией. Но любой продукт, подключенный к интернету, является мишенью для кибератак, если он не защищен. Обычно устройства из категории интернет вещей плохо или никак не защищены. Любую технику, подключенную к интернету, легко найти, и этим активно пользуются различного рода мошенники. Зачастую преступники используют интернет вещей для кражи личной информации или шантажа владельцев девайсов. Большинство из этих продуктов (а их насчитывается около 490 миллионов), уязвимы к, например, DNS-rebinding-у (атакам на веб-сервисы). Мы решили выяснить, может ли любой «умный» датчик или камера стать оружием в руках злоумышленника?

По словам народного депутата Александра Федиенко, любая технология или устройство, подключенные к сети интернет, уязвимы к атакам и утечкам информации.

«Необходимо, в первую очередь, работать над защитой любой системы или устройства. Проблема в том, что развитие интернета вещей происходило и происходит волнообразно, поэтому методы защиты только снйчас стали “подтягиваться”. Сначала на рынок было выброшено много решений, которые предназначались для общественного сектора (квартиры, дома, дач) и коммунальных услуг. Сейчас уже выходят технологии IIoT (индустриальный интернет вещей), которые перед их установкой следует обязательно проверить на безопасность и уязвимость. Сейчас во всем мире внедряются свои регламенты по интернету вещей. В Украине обычно происходит имплементация европейских стандартов в различных областях».

…директор компании Berezha Security Константина Косуна заявил, 90% интернет вещей уязвимы к любым атакам. То есть вся Wi-Fi техника, имеющая дефолтные логин и пароль (admin: admin), подвержена взлому.

«Вы подключаете холодильник к интернету с автоматическими настройками, нажимая перед этим по инструкции необходимую кнопку. Эти автоматические

настройки (по типу утюга, кофеварки, тостера и т.д.) является огромной проблемой, о которой говорят все эксперты. Когда вы подсоедините все эти предметы к вашей домашней сети, то в большинстве случаев, вам не потребуется в обязательном порядке менять заводские логин и пароль. Это, скорее, проблема производителя, который таким образом облегчает для пользователей настройку тех или иных приборов, чтобы они не прибегали к помощи каких-либо специалистов. Поэтому в инструкции они обычно пишут, что необходимо нажать те или иные кнопки».

Г-н Корсун отметил, что заводские настройки известны производителю, хакерам, преступникам и всевозможным мошенникам. Как только человек подключает что-то к сети они сразу же запускают автоматический сканер, который в автоматическом режиме обнаруживает все эти незащищенные девайсы.

«Вопрос лишь в том, как идентифицировать сетевые имена (страну или регион владельца прибора хакеры уже знают)? Для хакера очень сложно локализовать местонахождение устройства и привязать его к определенному человеку. Конечно, можно сразу выявить провайдера, который может работать в любом городе (Киеве, Харькове, Львове или Днепре). Возможно, он даже локализует, что провайдер находится в столице и работает на Печерске и Троещине. Но выявить конкретного человека, который пользуется этим незащищенным холодильником или тостером, очень сложная задача».

По мнению эксперта, хакеры не любят сложных задач, поскольку им надо как можно быстрее все монетизировать. Они ставят на все виды источников энергии майнеры, блокировщики, шифровальщики, рассылают спам и т. д. Эти устройства будут выполнять не очень корректные (и противоправные) действия, при этом пользователь девайса даже об этом не узнает. Если прибор оборудован еще и видеокамерой (как радионяня) или микрофоном (если он встроен в прибор), то к ним легко может получить доступ любой злоумышленник. Он сможет круглосуточно следить за всеми действиями владельца техники. И в случае необходимости может прибегнуть к финансовому шантажу. Поэтому на любое устройство, которое может подключаться к интернету, необходимо поставить свой пароль.

«Если говорить о промышленном интернет вещей, то теоретически хакеры могут взломать какие-то важные предприятия. Но практически это невозможно. Например, Запорожскую атомную электростанцию обвиняли в том, что у них в сети незащищенный интернет-периметр и ее можно легко сломать. Белые хакеры даже как-то нашли уязвимость и получили доступ к информационным системам критической инфраструктуры. При этом стоит вспомнить, что интернет сеть образует некий контур вокруг станции, но она физически отделена от системы управления электростанции. И так в большинстве случаев».

Г-н Корсун отметил, что в Украине уровень проникновения информационных технологий в управление производственными процессами относительно низкий. В этом отношении мы очень сильно отстаем от Европы, США, Японии и даже такой экзотической страны как Австралия. Доступ к сетям критической инфраструктуры в большинстве случаев не предоставляет прямой возможности что-то открыть, взорвать, остановить и т. д.

«Однако есть доступ в локальную сеть, которая несовместима напрямую с производственными процессами, позволяющая получить большой объем инсайдерской информации (о том, кто куда ходит, у кого, когда отпуск, какая зарплата, о неуплате налогов, коррупции). Таким образом можно найти компромат на любого сотрудника и начать его шантажировать для того, чтобы его завербовать. А человек инсайдер внутри атомной станции становится уже настоящей большой проблемой, которая способна наделать много беды»

Если воспользоваться международными исследованиями, как советует президента группы компаний «Адамант» Иван Петухов, то можно увидеть, что максимальный прирост кибератак в последние годы происходит как раз в IoT. Проблема тут комплексная и виноваты не только производители, которые недостаточно продумывают алгоритмы защиты, а и сами пользователи, что не задумываются о безопасности своих данных и защите личных устройств. В своем большинстве люди ставят пароли, которые легко взломать, не меняют их на роутерах и достаточно халатно относятся к безопасности информации.

«Наибольшие риски в интернет вещах - это утечка данных и использование туманных вычислений для развертывания бот-сетей. А вообще-то данная технология в Украине уже есть давно, но она не столь активно развивается как бы могла и связано это с неповоротливостью государства, которое долго внедряло 3G, 4G, 5G технологии, а также неготовностью ряда монополистов (Киевэнерго, водоканал, Киевгаз и т.д) устанавливать «умные» счетчики, они затраты на логистику привыкли перекладывать на потребителей и государственные органы, что призваны контролировать этот процесс находятся с ними в коррупционной связке. Поэтому у нас больше коррупционных рисков чем технических. Подходя ближе к теме внедрения IoT могу порекомендовать не экономить на кибербезопасности и для развертывания сетей обращаться в известные на рынке компании, которые в состоянии оценить угрозы и предложить оптимальные варианты решения», - отметил г-н Петухов». ***(Элина Сулима. По мнению специалистов, 90% объектов интернета вещей не устоят перед кибератаками // Internetua (https://internetua.com/po-mneniua-specialistov-90-ob-ektov-interneta-vesxei-ne-ustoyat-pered-kiberatakami). 03.04.2020).***

***

«Современные «умные» автомобили представляют угрозу безопасности. К такому выводу пришли специалисты британской организации Which?, занимающейся тестированием различных товаров и помогающей потребителям делать осознанный выбор.

Исследователи протестировали две марки автомобилей Ford (Focus Titanium Automatic 1.0L с бензиновым двигателем) и Volkswagen (Polo SEL TSI Manual 1.0L с бензиновым двигателем) и выявили проблемы с безопасностью. В частности, они обнаружили отсутствие эффективных мер защиты CAN-шин и информационно-развлекательных систем от вредоносного воздействия.

Специалистам британской ИБ-компании Context Information Security в свою очередь удалось получить доступ к информационно-развлекательным системам обоих автомобилей – дисплеям на приборной панели, отображающей

всевозможные данные, начиная от карты с GPS-навигатором и заканчивая радиостанцией и музыкальными плейлистами.

«Хотя автомобили взломать гораздо сложнее, чем многие другие подключенные продукты, исследователям Context удалось выявить уязвимости в безопасности и даже обнаружить пароль для сети Wi-Fi на заводе Ford», – сообщили исследователи.

Изучив используемые в автомобилях Ford CAN-шины и подключенные к ней элементы, эксперты выяснили, что информационно-развлекательная система подключена к трем отдельным шинам, в том числе к трансмиссии. По словам исследователей, в теории, благодаря этому злоумышленники могут получить доступ к управлению двигателем.

Как выяснилось, достаточно было просто «помахать перед машиной бэйджем Volkswagen», и открылся доступ к переднему радарному модулю, что теоретически дало бы злоумышленникам возможность вмешаться в работу системы предотвращения столкновений.

Системы беспроводной разблокировки в обоих автомобилях оказались уязвимыми к релейным атакам и атакам повторного воспроизведения». ***(Подключенные автомобили Ford и Volkswagen представляют угрозу безопасности // SecurityLab.ru (https://www.securitylab.ru/news/506583.php). 10.04.2020).***

***

Кіберзлочинність та кібертерроризм

«Специалисты Aqua Security сообщают об атаках, начавшихся в последние несколько месяцев. Неизвестные злоумышленники сканируют сеть в поисках серверов Docker, использующих порты API, которые открыты для всех желающих, без паролей. Такие незащищенные хосты в итоге подвергаются компрометации: на них устанавливают майнинговую малварь под названием Kinsing.

Исследователи пишут, что атаки начались еще в прошлом году и продолжаются до сих пор. Причем эти атаки являются лишь одним из пунктов в длинном списке вредоносных кампаний, нацеленных на Docker. Так как эти системы в случае взлома предоставляют хакерам беспрепятственный доступ к огромным вычислительным ресурсам.

По словам экспертов, когда хакеры находят экземпляр Docker с открытым портом API, они используют этот доступ для раскатки контейнера Ubuntu, куда загружают и устанавливают вредоносное ПО Kinsing.

Основная цель данной малвари — добыча криптовалюты на взломанном Docker, но малварь имеет и дополнительные функции. Так, среди них выполнение скриптов, которые удаляют другие вредоносные программы, могут работать локально, а также собирают локальные учетные данные SSH и пытаются продолжить распространение в контейнерную сеть компании, чтобы заразить и другие облачные системы все там же майнером Kinsing.

Так как атаки Kinsing продолжаются и сейчас, Aqua Security рекомендует компаниям проверить безопасность Docker и убедиться, что никакие административные API не доступны из вне. Такие эндпоинты должны находиться за брандмауэром или VPN (если так необходимо, чтобы они были доступы из интернета), а также отключаться, если они не используются». ***(Мария Нефёдова. Малварь Kinsing атакует серверы Docker // Хакер (https://xakep.ru/2020/04/06/kinsing-miner/). 06.04.2020).***

***

«Еще в конце марта 2020 года ИБ-специалист Джон Ветингтон сообщил журналистам издания ZDNet, что некто развернул масштабную кампанию по взлому плохо защищенных серверов Elasticsearch. Так, неизвестный злоумышленник взламывает плохо защищенные серверы Elasticsearch и пытается дефейснуть их или стереть все их содержимое. При этом вину за содеянное он пытается возложить на американскую ИБ-компанию Night Lion Security.

Первые атаки были замечены 24 марта 2020 года и, похоже, они автоматизированы: скрипт сканирует интернет в поисках незащищенных Elasticsearch, подключается к БД, пытается стереть их содержимое, а затем создает новый пустой индекс с названием nightlionsecurity.com. По какой-то причине атакующий скрипт срабатывает не во всех случаях, но индекс nightlionsecurity.com присутствует даже в тех БД, где контент в итоге остался нетронутым. Из-за изменчивой природы данных, хранящихся на серверах Elasticsearch, эксперты затрудняются определить точное количество пострадавших систем.

Основатель Night Lion Security Винни Тройя (Vinny Troia) отрицает, что его компания имеет какое-либо отношение к происходящему. В интервью DataBreaches.net, 26 марта 2020 года, Тройя заявил, что, по его мнению, эти атаки осуществляются хакером, которого он отслеживает последние годы и который является предметом его будущей книги.

Но если 26 марта атаки еще выглядели как чья-то шутка, то сейчас ситуация заметно ухудшилась. По данным поисковика BinaryEdge, в настоящее время индекс nightlionsecurity.com присутствует примерно на 15 000 серверах, тогда как в конце марта таковых насчитывалось лишь 150. При этом BinaryEdge в общей сложности «видит» лишь 34 500 серверов Elasticsearch, доступных из интернета.

Теперь Тройя сообщил ZDNet, что уже уведомил правоохранительные органы о происходящем. Также сами журналисты связались с командой безопасности Elastic, которая теперь тоже изучает эти атаки. В свою очередь Джон Ветингтон занят составлением списка серверов, на которые повлияли атаки, и пытается определить компании, которые из-за этого могли сталкиваться со сбоями в работе служб.

Хуже того, изучая эту кампанию, Ветингтон обнаружил еще одного хакера, который тоже атакует незащищенные серверы Elasticsearch. Этот злоумышленник оставляет на серверах послание, которое информирует, что сервер был взломан, и призывает его владельцев связаться с хакером по электронной почте. В настоящее время это сообщение обнаружено на 40 серверах». ***(Мария Нефёдова.***

Неизвестные дефейснули и стерли данные с 15 000 серверов Elasticsearch // Xakep (https://xakep.ru/2020/04/03/elasticsearch-hacks/). 03.04.2020).

***

«Компания Fortinet мировой лидер в области глобальных интегрированных и автоматизированных решений для обеспечения кибербезопасности представляет выводы исследования FortiGuard Labs Global Threat Landscape Report.

Исследования, проведенные в четвертом квартале 2019 года, показывают, что киберпреступники не только продолжают пытаться использовать любую возможность для атаки во всей цифровой инфраструктуре, но и максимизируют глобальные экономические и политические реалии для дальнейшего достижения своих целей.

Глобальные тренды показывают, что распространенность и обнаружение угроз могут различаться в зависимости от географии, но изощренность и автоматизация атак остаются неизменными повсюду. Кроме того, необходимость уделять первоочередное внимание кибер гигиене остается актуальной во всем мире, так как угрозы растут быстрее, чем когда-либо прежде…

«В гонке кибер вооружений у преступного сообщества зачастую было явное преимущество из-за растущего разрыва в кибер-навыках, расширения поверхности цифровых атак и применения социальной инженерии с эффектом неожиданности, чтобы использовать в своих интересах ничего не подозревающих людей. Чтобы вырваться из цикла все более изощренных и автоматизированных угроз, организациям необходимо использовать те же самые технологии и стратегии для защиты своих сетей, которые преступники используют для атаки на них. Это подразумевает использование интегрированных платформ, которые способны обеспечить защиту и прозрачность всей цифровой инфраструктуры с помощью ресурсов интеллектуального анализа угроз и готовых сценариев реагирования» – Дерек Мэнки, руководитель отдела безопасности и глобальных угроз, FortiGuard Labs.

1) Не очень уж миленький котенок. Исследования показывают значительный уровень активности в регионах, связанных с Charming Kitten, группой аффилированных с Ираном APT (advanced persistent threat) в 4 квартале. Группировка, действующая с 2014 года, провела многочисленные кампании по кибершпионажу. Недавняя активность свидетельствует о том, что интерес злоумышленников распространился на бизнес по срыву выборов. На это указывает серия атак на целевые учетные записи электронной почты, связанные с президентской предвыборной кампанией. Кроме того, было замечено, что Charming Kitten применяет четыре новые тактики против предполагаемых жертв, которые были разработаны, чтобы обманным путем заставить субъект расстаться с конфиденциальной информацией.

2) Рост угроз безопасности для устройств IoT. Устройства IoT продолжают сталкиваться с проблемами, связанными с уязвимым программным обеспечением, и это может повлиять на неожиданные устройства, такие как беспроводные IP-камеры. Эта ситуация усугубляется, когда компоненты и программное обеспечение

встраиваются в различные коммерческие устройства, продаваемые под разными торговыми марками, иногда разными поставщиками. Многие из этих компонентов и услуг часто программируются с использованием битов и кусочков заранее написанного кода из различных общих источников. Такие общие компоненты и заранее написанный код иногда уязвимы для эксплуатации, вот почему иногда одни и те же уязвимости появляются неоднократно в широком диапазоне устройств. Масштаб в сочетании с невозможностью легко исправить эти устройства является значительной проблемой, и подчеркивает трудности обеспечения безопасности цепочки поставок. Недостаточная осведомленность или доступность патчей, распространенность уязвимостей в некоторых устройствах IoT и документально подтвержденные попытки «поработить» эти устройства в бот-сетях IoT – все это способствовало тому, что эти эксплойты заняли третье место по объему среди всех IPS-обнаружений в течение квартала.

3) Старшие угрозы помогают младшим. В условиях постоянного давления, направленного на то, чтобы идти в ногу с новыми угрозами, организации иногда забывают о том, что у старых эксплойтов и уязвимостей действительно нет срока годности, злоумышленники продолжат использовать их до тех пор, пока они работают. В качестве примера можно привести EternalBlue. Вредоносная программа со временем адаптировалась для использования общих и основных уязвимостей. Она использовалась в многочисленных кампаниях, включая, прежде всего, атаки вымогателей WannaCry и NotPetya. Кроме того, в мае прошлого года был выпущен патч для BlueKeep, уязвимости, которая могла потенциально использоваться компьютерными червями, и которая могла бы распространяться с той же скоростью и в том же масштабе, что и WannaCry и NotPetya. И вот в прошлом квартале появилась новая версия трояна EternalBlue Downloader с возможностью использования уязвимости BlueKeep. К счастью, версия, находящаяся в настоящее время в обращении, не полностью отлажена, и заставляет целевые устройства аварийно завершать работу перед загрузкой. Однако, если посмотреть на традиционный цикл разработки вредоносного ПО, то, скорее всего, в ближайшем будущем у злоумышленников появится функциональная версия этого потенциально разрушительного вредоносного пакета. И хотя с мая был выпущен патч для BlueKeep, слишком многие организации до сих пор не обновили свои уязвимые системы. Продолжающийся и развивающийся интерес акторов угроз к EternalBlue и BlueKeep является напоминанием организациям о том, что их системы должны быть исправлены и как следует защищены от обеих угроз.

4) Среди трендов – новый взгляд на глобальную торговлю спамом. Спам остается одной из главных проблем, с которой сталкиваются организации и частные лица. Наш отчет объединяет объем спамового потока между странами с данными, показывающими соотношение отправленного и полученного спама, наглядно демонстрируя новый взгляд на старую проблему. Большая его часть, по-видимому, следует экономическим и политическим тенденциям. Например, к самым крупным «торговым партнерам» США относятся Польша, Россия, Германия, Япония и Бразилия. Кроме того, по объему экспортируемого спама из географических регионов Восточная Европа является крупнейшим нетто-производителем спама в мире. Большая часть крупных спамеров за пределами

этого региона – выходцы из азиатских субрегионов. Остальные европейские субрегионы лидируют по чистым отрицательным показателям спама, получая больше, чем отправляют, за ними следуют страны Северной и Южной Америки и Африки.

5) Отслеживание следов киберпреступников с целью узнать их дальнейшие действия. Просмотр обнаруженных в регионе IPS-триггеров не только показывает, на какие ресурсы нацелены атаки, но и может указать на то, на чем киберпреступники могут сосредоточиться в будущем, либо потому, что в конечном итоге достаточное количество таких атак было успешным, либо просто потому, что в некоторых регионах развернуто больше технологий определенного типа. Но это не всегда так. Например, подавляющее большинство внедрений ThinkPHP происходит в Китае, где, по данным shodan.io, их почти в 10 раз больше, чем в США. Предполагая, что компании исправляют свое программное обеспечение примерно с одинаковой скоростью в каждом регионе, если ботнет просто проверял уязвимые экземпляры ThinkPHP перед развертыванием эксплойта, число обнаруженных триггеров должно быть намного выше в Азиатско-Тихоокеанском регионе. Однако там было обнаружено только на 6% больше триггеров IPS из недавнего эксплойта, чем в Северной Америке, что указывает на то, что эти бот-сети просто разворачивают эксплойт на любой найденный ими экземпляр ThinkPHP. Кроме того, при аналогичном взгляде на обнаружение вредоносного ПО, большинство угроз, нацеленных на организации, представляют собой макросы Visual Basic for Applications (VBA). Скорее всего, так происходит потому, что они все еще эффективны и дают результаты. В общем, частота обнаружения вещей, которые не работают, не будет оставаться высокой в течение долгого времени, и если есть значительное количество обнаружений чего-то, кто-то становится жертвой этих атак.

Потребность в глобальной интегрированной и автоматизированной кибербезопасности

По мере распространения приложений и увеличения количества подключенных устройств по периметру, создаются миллиарды новых поверхностей атак, которыми необходимо управлять и защищать. Кроме того, организации сталкиваются со все более изощренными атаками, направленными на расширяющуюся цифровую инфраструктуру, в том числе некоторые из них вызваны искусственным интеллектом и компьютерным обучением. Для эффективной защиты своих распределенных сетей организациям приходится переходить от защиты только периметра безопасности к защите данных, распространяемых по новым границам сети, пользователям, системам, устройствам и критически важным приложениям. Только платформа кибербезопасности, разработанная для обеспечения комплексной видимости и защиты всей поверхности атак, включая устройства, пользователей, мобильные конечные точки, многооблачные среды и SaaS-инфраструктуры, способна обеспечить защиту современных быстро развивающихся сетей, основанных на цифровых инновациях…» ***(FortiGuard Labs Threat Landscape Report: новые политические и экономические намерения киберпреступников // AMC Ukraine (https://channel4it.com/publications/FortiGuard-Labs-Threat-Landscape-Report-***

novye-politicheskie-i-ekonomicheskie-namereniya-kiberprestupnikov-37219.html#). 06.04.2020).

***

«…тенденцией последних месяцев среди операторов шифровальщиков стала публикация в открытом доступе данных, похищенных у пострадавших компаний. Так, разработчики малвари призывают аффилированных лиц копировать данные жертв перед шифрованием, чтобы затем эту информацию можно было использовать в качестве рычага давления (а если это не поможет, обнародовать или продать). Собственные сайты для этих целей уже завели разработчики вымогателей Maze, DoppelPaymer, Sodinokibi (REvil) и другие. Такая информация может включать в себя финансовые документы компании, личную информацию сотрудников и клиентские данные.

Компания Visser Precision, пострадавшая от атаки DoppelPaymer, это один из крупнейших промышленных подрядчиков в США, в число клиентов которого входят промышленные предприятия, а также компании аэрокосмической и автомобильной промышленности (например, Lockheed Martin, SpaceX, Tesla, Boeing, Honeywell, Blue Origin, Sikorsky, Joe Gibbs Racing и многие другие).

По информации издания, DoppelPaymer атаковал Visser Precision в марте текущего года. Так как компания не заплатила выкуп в установленный срок (как правило, вымогатели требуют сотни тысяч или даже миллионы долларов за восстановление зашифрованных файлов), злоумышленники претворили свои угрозы в жизнь и опубликовали в открытом доступе подборку похищенных документов.

Утечка затронула данные таких клиентов Visser Precision, как Tesla, Lockheed Martin, Boeing и SpaceX. The Register пишет, что среди обнародованной документации можно найти закрытую информацию о военном оборудовании, разработанном Lockheed Martin, например, спецификации антенны для системы защиты от минометов. Также была опубликована финансовая документация, информация о поставщиках, отчеты об анализе данных и юридические документы…» ***(Мария Нефёдова. Хакеры опубликовали в открытом доступе документы Boeing, Lockheed Martin, SpaceX и Tesla // Хакер (https://xakep.ru/2020/04/10/visser-precision-hack/). 10.04.2020).***

***

«Старейший в мире итальянский банк Monte dei Paschi di Siena сообщил о взломе почтовых ящиков своих сотрудников. 30 марта в результате кибератаки злоумышленники отправили якобы от имени банка электронные сообщения с голосовыми вложениями…

Представители банка не упомянули о какой-либо утечке данных компании или пострадавших клиентах в результате кибератаки…». ***(Преступники взломали почту сотрудников итальянского банка // SecurityLab.ru (https://www.securitylab.ru/news/506609.php). 13.04.2020).***

***

«Крупная компания DESMI, специализирующаяся на разработке и производстве насосных решений для судов и промышленности, стала жертвой кибератаки.

Атака произошла ночью 9 апреля. В результате атаки были отключены все компьютерные системы компании. О характере кибератаки, а также использованном в ее ходе вредоносном ПО не сообщается.

Компания привлекла внешних IT-экспертов для расследования инцидента и в настоящее время работает над восстановлением систем. DESMI уже сообщила о происшествии властям и полиции Дании.

«Первая часть наших систем будет запущена через несколько дней, а остальные — через пару недель», — сообщил генеральный директор Хенрик Серенсен (Henrik Sørensen).» ***(Датский производитель насосов DESMI стал жертвой кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/506606.php). 13.04.2020).***

***

«Операторы вымогательского ПО DoppelPaymer похитили внутренние конфиденциальные документы, принадлежащие Lockheed Martin, SpaceX, Tesla, Boeing, у промышленного подрядчика и опубликовали их в Сети после отказа платить выкуп.

Похищенные данные включают подробную информацию о военном оборудовании, разработанном американской военно-промышленной корпорацией Lockheed Martin, сообщило издание The Register. Также были опубликованы платежные формы, информация о поставщиках, аналитические отчеты и документы партнерской программы SpaceX.

Файлы были похищены у компании Visser Precision операторами вредоноса DoppelPaymer, которые заразили компьютеры подрядчика и зашифровали его файлы. Когда компания не смогла заплатить выкуп к назначенному сроку, злоумышленники опубликовали документы на общедоступном web-сайте.

Visser Precision поставляет комплектующие для аэрокосмической, автомобильной и обрабатывающей промышленности. В число ее клиентов входят предприятия, занимающиеся аэрокосмической, автомобильной и заводской промышленностью: Lockheed Martin, SpaceX, Tesla, Boeing, Honeywell, Blue Origin, Sikorsky, Joe Gibbs Racing, Университет штата Колорадо, Кардиффская школа инженерии и пр.

Представители Visser Precision, Tesla, Boeing, SpaceX не предоставили комментарии относительно инцидента». ***(Вымогатели опубликовали документы Boeing, Lockheed Martin и SpaceX // SecurityLab.ru (https://www.securitylab.ru/news/506584.php). 10.04.2020).***

***

«Жорсткі карантинні заходи та тривога через стрімке поширення смертельно небезпечного вірусу стали причиною виникнення хвилі злочинності. Новітні шахраї експлуатують нові реалії життя в умовах пандемії.

Поліцейська служба ЄС провела комплексну оцінку цих правопорушень. Для того, щоб зрозуміти, яким чином пандемія впливає на внутрішню безпеку в державах-членах ЄС, Європол визначив причини, які створюють сприятливий ґрунт для здійснення злочинів. Серед них – високий попит на захисні засоби та фармацевтичну продукцію та зниження мобільності громадян. Окрім цього, страх перед хворобою зробив людей вразливими, а отже ними стало легше маніпулювати. А те, що громадяни, залишаючись вдома, почали набагато активніше використовувати електронні засоби комунікації, відкрило нові можливості для онлайн шахрайства.

За даними Європолу, кількість кібератак проти організацій та фізичних осіб за останній місяць стрімко зросла. Більшість роботодавців започаткувала практику дистанційної роботи шляхом з'єднань із системами своїх організацій. Через засоби електронної комунікації кіберзлочинці пропонують різні послуги, які є шкідливим спамом. Активізувалося поширення небезпечного для дітей контенту. Оскільки малеча більше часу проводить вдома за комп'ютером, а нагляд батьків за ними є недостатнім…». ***(Вікторія ВЛАСЕНКО. У країнах ЄС почастішали випадки кібератак і шахрайства в умовах пандемії COVID-19 // Урядовий кур'єр (http://ukurier.gov.ua/uk/news/u-krayinah-yes-pochastishali-vipadki-kiberatak-i-s/). 10.04.2020).***

***

«Представители GitHub предупредили пользователей об активной фишинговой кампании, получившей название Sawfish.

В последнее время пользователи все чаще получают фишинговые письма, с фальшивыми предупреждениями о подозрительной активности учтенной записи или странных изменениях, внесенных в репозиторий или настройки. Ссылки, приложенные к таким посланиям, ведут на поддельную страницу входа в GitHub, созданную специально для сбора учетных данных жертвы и передачи их злоумышленникам.

Специалисты GitHub отмечают, что эта кампания имеет несколько примечательных аспектов. Например, фишинговая страница способна перехватывать коды двухфакторной аутентификации, которые генерируются при помощи TOTP-приложения (time-based one-time password). Это позволяет злоумышленникам атаковать и учетные записи, защищенные 2ФА. При этом подчеркивается, что пользователи, использующие аппаратные ключи безопасности, проблеме не подвержены.

Фишинговые послания часто приходят с легитимных доменов (которые были взломаны). Так, список фишинговых доменов, замеченных экспертами GitHub, включает в себя git-hub[.]co, githb[.]co, glthub[.]net, glthubs[.]com и corp-github[.]com.

При этом атаки направлены не на всех подряд, но в основном на активных пользователей, работающих в крупных технологических компаниях. Очевидно, злоумышленники берут те email-адреса, которые разработчики использовали для публичных коммитов.

Также атакующие активно используют службы сокращения URL-адресов, чтобы скрыть конечный фишинговый адрес (порой они объединяют сразу нескольких служб сокращения URL-адресов, чтобы надежнее запутать следы). В некоторых случаях жертв и вовсе сначала направляют на взломанный легитимный сайт и лишь потом непосредственно на фишинговую страницу.

Если атака удалась и учтенные данные попали в руки злоумышленников, часто хакеры сразу же скачивают все содержимое приватных репозиториев, доступных скомпрометированному пользователю (в том числе принадлежащих организациям и другим сотрудникам).

Пользователей, которые пострадали от этих атак, просят немедленно сбросить пароль и коды двухфакторного восстановления, просмотреть свои токены доступа и принять дополнительные меры дял защиты своей учетной записи. В дополнение к аппаратным ключам или WebAuthn 2FA рекомендуется использовать менеджеры паролей». ***(Мария Нефёдова. GitHub предупредил пользователей о фишинговой атаке // Хакер (https://xakep.ru/2020/04/20/github-phishing/). 20.04.2020).***

***

«Издание Bleeping Computer обратило внимание, что в начале ткущей недели португальская транснациональная компания Energias de Portugal стала жертвой шифровальщика RagnarLocker. Теперь злоумышленники требуют выкуп в размере 1580 BTC (10,9 млн долларов или 9,9 млн евро).

Energias de Portugal представляет собой транснациональный холдинг, который занимается производством, распределением по сетям и сбытом электроэнергии, а также закупками, доставкой и сбытом природного газа. Energias de Portugal является самой крупной производственной компанией в Португалии, а также одним из крупнейших производителей ветряной электроэнергии в мире. Компания представлена в 19 странах и на 4 континентах, имеет более 11 500 сотрудников и обеспечивает энергией более 11 миллионов клиентов.

Операторы шифровальщика RagnarLocker утверждают, что во время атаки они похитили у компании более 10 Тб конфиденциальных файлов, и теперь угрожают их «сливом» в открытый доступ, если не будет выплачен выкуп. В качестве предупреждения злоумышленники уже обнародовали файл edpradmin2.kdb – БД менеджера паролей KeePass. В этой базе можно обнаружить информацию об именах пользователей, паролях, аккаунтах, URL-адресах и заметках сотрудников Energias de Portugal.

Согласно записке с требованием выкупа, оставленной в системах компании, злоумышленникам также удалось похитить конфиденциальную информацию о выставлении счетов, контрактах, транзакциях, клиентах и партнерах Energias de Portugal.

Также издание сообщает, что операторы Ragnar Locker издевались над сотрудниками компании через «чат для клиентов», который хакеры используют для общения со своими жертвами. В частности, атакующие просили пострадавших ознакомиться со статьей о компании на сайте, где публикуются утечки, и

интересовались, готова ли компания обнаружить свою личную информацию в новостях, технических блогах и на биржевых ресурсах.

Представители Energias de Portugal заверили журналистов Bleeping Computer, что данная атака не повлияла на критически важную инфраструктуру компании и энергообеспечение:

«В понедельник, 13 апреля, EDP стала жертвой компьютерной атаки на корпоративную сеть, которая является важной частью наших сервисов и операций. Но службы электроснабжения и критически важная инфраструктура компании не подверглись компрометации, и мы продолжаем работу в штатом режиме.

В настоящее время проводится оценка ситуации, а ряд команд уже занимается восстановлением нормального функционирования систем. Это будет сделано как можно скорее и является нашим главным приоритетом.

EDP уже сотрудничает с властями, которые были немедленно уведомлены об инциденте, и старается определить источник и природу атаки. На данный момент нам ничего неизвестно о предполагаемом требовании выкупа, мы видели лишь эту информацию, которая была опубликована в СМИ». ***(Мария Нефёдова. Энергетический гигант Energias de Portugal атакован RagnarLocker. Хакеры требуют выкуп 10 млн евро // Xakep (https://xakep.ru/2020/04/16/edp-ragnar-locker/). 16.04.2020).***

***

«В начале апреля текущего года мы рассказывали о странной вредоносной кампании: пользователи получали навязчивые предложения скачать приложение, якобы информирующее о COVID-19 и созданное ВОЗ. Как оказалось, роутеры этих людей были скомпрометированы, настройки DNS изменены, а под видом «коронавирусного» приложения распространялся троян Oski.

…во всех случаях пострадавшие были владельцами роутеров D-Link или Linksys, и неизвестные злоумышленники изменили на их устройствах настройки DNS. Однако было неясно, как именно атакующие получали доступ к маршрутизаторам, хотя несколько пострадавших признались, что доступ к их роутерам можно было получить удаленно, и они использовали слабые пароли.

Теперь же The Register пишет, что разработчики компании Linksys начали принудительное обнуление паролей от облачного сервиса Linksys Smart Wi-Fi, так как, судя по всему, именно с этим сервисом была связана недавняя атака. Сервис Smart WiFi позволяет владельцам устройств Linksys подключаться к своим маршрутизаторам и другому оборудованию через интернет для управления настройками. После смены пароля и входа на сайт, сервис автоматически проведет проверку безопасности подключенных маршрутизаторов, чтобы убедиться, что ни на одном из них не были изменены настройки DNS.

Представители компании Belkin (владеет Linksys с 2013 года) подтвердили журналистам, что злоумышленники получили доступ к чужим учетным записям Smart Wi-Fi, используя атаки типа credential stuffing. Этим термином обозначают ситуации, когда имена пользователей и пароли похищают с одних сайтов, а затем используют на других. То есть злоумышленники имеют уже готовую базу учетных

данных (приобретенную в даркнете, собранную самостоятельно и так далее) и пытаются использовать эти данные, чтобы авторизоваться на каких-либо сайтах и сервисах под видом своих жертв.

«Несколько факторов позволяют сделать вывод, что эти учетные данные были украдены в другом месте: большинство запросов на аутентификацию [в Smart Wi-Fi] содержали имена пользователей, которые никогда не регистрировались в нашей системе. Мы проверили адреса электронной почты с помощью таких сервисов, как haveibeenpwned.com, и выяснили, что списки учетных данных, которые использовали для наших систем, ранее фигурировали в различных утечках.

Было предпринято несколько попыток использования одного и того же имени пользователя, но с разными паролями. В этом не было бы необходимости, если бы наши собственные системы оказались скомпрометированы», — рассказали представители Belkin.

Сколько именно пользователей оказалось скомпрометировано таким образом в компании не говорят. На специальной странице, посвященной инциденту, представители Linksys пишут: «Если вы загрузили приложение COVID-19 Inform, ваша сеть заражена. Вам нужно как можно быстрее избавиться от него, чтобы предотвратить дальнейшее воздействие».

Интересно, что письма с информацией об инциденте и просьбой поменять пароли были разосланы пользователям не с адреса на linksys.com, из-за чего возникла путаница, и у многих встал вопрос, настоящие ли это послания. Позже компания подтвердила происхождение писем в своем Twitter, заверив пользователей, что все в порядке». ***(Мария Нефёдова. Linksys сбрасывает пароли от Smart Wi-Fi из-за атак с подменой DNS // Xakep (https://xakep.ru/2020/04/16/smart-wi-fi-hack/) 16.04.2020).***

***

«До початку спалаху коронавирусной інфекції ІС3 підрозділ ФБР, брало не більше 1 тис. скарг на хакерські дії в день. За останній місяць, коли велика частина населення населення планети перебувала на карантині через пандемії коронавирусной інфекції, число щоденних скарг на хакерські дії зросла до 4 тис. штук. Схоже хакери вирішили нажитися на простих користувачів.

Також експерти з кібербезпеки відзначають, що фішингові листи набирають популярність. Приміром, вам на скриньку потрапляє лист з інформацією, що людство винайшло ліки від вірусу, і вас просять заповнити анкету. При завантаженні анкети на комп'ютер, вірус з файлу завантаженого на пристрій починає красти дані, або знищувати їх, і вимагати викуп.

Крім того, велика кількість офісних працівників почали працювати з дому, тому зріс і обсяг зломів різних месенджерів і сервісів для віддаленої комунікації співробітників. При цьому в доповіді ІС3 не вказується точна кількість проведених зломів і шкоди від них». ***(Хакери масово атакують мільйони комп'ютерів, у всьому винна пандемія // Знай.ua (https://techno.znaj.ua/306875-hakeri-masovo-atakuyut-milyoni-komp-yuteriv-u-vsomu-vinna-pandemiya). 21.04.2020).***

***

«Кількість кібератак на портали Всесвітньої організації охорони здоров'я (ВООЗ) значно збільшилася з моменту початку пандемії коронавірусу. Про це йдеться в опублікованому в четвер прес-релізі організації…

Як стверджує ВООЗ, зараз кількість посягань на її інформаційну безпеку в п'ять разів перевищує кількість кібератак за аналогічний період минулого року. Почастішали випадки розсилок електронних листів від імені організації із закликами жертвувати кошти нібито в фонд по боротьбі з коронавірусом. Крім того, на цьому тижні стався витік близько 450 адрес електронної пошти і паролів ВООЗ. Бази даних при цьому не постраждали, однак збиток був нанесений внутрішньої мережі організації, яку використовують її колишні і нинішні співробітники, а також партнери.

ВООЗ підкреслила, що працює над посиленням безпеки своїх систем.

Раніше у Google повідомили, що тема пандемії активно використовується для кібератак по всьому світу». ***(Ілля Нежигай. Кількість кібератак на ВООЗ під час пандемії збільшилася в п'ять разів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1865557-kilkist-kiberatak-na-vooz-pid-chas-pandemiyi-zbilshilasya-v-pyat-raziv). 24.04.2020).***

***

«…"Компания по кибербезопасности Mimecast обнаружила около 700 подозрительных мошеннических сайтов, копирующих самый популярный в мире потоковый сервис, появившиеся между 6 апреля и Пасхой", – говорится в сообщении.

Netflix, который во вторник собирается обнародовать свой прогноз по результатам первого квартала в отношении 7 млн новых подписчиков во всем мире, является основной целью, поскольку миллионы новых потенциальных пользователей ищут развлечения, находясь дома

Более новый сервис Disney+, который начал свою международную трансляцию в прошлом месяце, запустив ее на основных рынках Западной Европы, включая Великобританию, был клонирован четырьмя новыми веб-сайтами за тот же недельный период.

Некоторые поддельные сайты могут выглядеть чрезвычайно убедительно, продавая подписки или бесплатные аккаунты с целью сбора личных данных и данных кредитных карт, хотя большинство из них плохо спроектированы и имеют языковые ошибки, которые выделяют их как подозрительные.

«Мы наблюдаем резкий рост числа подозрительных доменов, выдающих себя за множество потоковых гигантов в мошеннических целях», – сказал Карл Уирн, глава отдела электронных преступлений в Mimecast». ***(В СЕТИ ОБНАРУЖИЛИ БОЛЕЕ 700 САЙТОВ-ПОДДЕЛОК NETFLIX И DISNEY+ // «Новости онлайн 24» (https://newsonline24.com.ua/v-seti-obnaruzhili-bolee-700-sajtov-poddelok-netflix-i-disney/). 20.04.2020).***

***

«С каждым годом число кибератак и ущерб от них постоянно растет во всем мире. Одной из основных причин роста киберпреступности является низкая стоимость и высокая доступность готовых вредоносных программ, продаваемых на подпольных торговых площадках.

Как сообщил ресурс Cybernews, в настоящее время не нужно быть программистом или обладать специальными техническими знаниями, чтобы купить или создать вредоносное ПО. Будущим киберпреступникам достаточно лишь знать, где делать покупки. Банковские трояны, предназначенные для кражи учетных данных пользователей online-банкинга, часто предлагаются вместе с вымогательским ПО, современными модульными ботами или другими вредоносами пр.

Программы также идут в комплекте с технической поддержкой, которая предоставляется бесплатно или за небольшую дополнительную плату. Самыми популярными в даркнете категориями вредоносов являются:

Инфостилеры — одни из самых популярных вредоносных инструментов. Троянские программы для кражи данных способны похищать пароли, cookie-файлы, истории и данные кредитных карт, сеансы чатов из мессенджеров и изображения с web-камер. Средняя цена — от $50 до $150.

Трояны удаленного доступа (RAT) позволяют злоумышленнику перехватить контроль над системой жертвы, включая запуск и установку программного обеспечения, создание скриншотов, переключение web-камеры и слежением за действиями жертвы. Цена варьируется от $800 до $1 тыс. Некоторые RAT, такие как Imminent Monitor, часто рекламируются как легитимные инструменты удаленного администрирования для увеличения продаж.

Модульные вредоносные боты могут выборочно запускать различные вредоносные программы в зависимости от целей атаки — от кейлоггинга и похищения паролей жертв до кражи адресов криптовалютных кошельков из их буферов обмена. Цена ботов составляет около $2,5 тыс.

Банковские трояны маскируются под подлинное программное обеспечение, которое пользователи часто загружают и устанавливают со сторонних сайтов. После установки вредоносы могут получить доступ к банковским реквизитам пользователя и отправить их обратно злоумышленнику, предоставив ему доступ к счетам жертвы. Цена варьируется в пределах $5 тыс.

Вымогательское ПО зашифровывает содержимое компьютерной системы жертвы и требует выкуп в криптовалюте для восстановления данных. В то время как большинство злоумышленников в 2020 году продают свой продукт по бизнес-модели «вымогательское ПО как услуга» (Ransomware-as-a-Service , RaaS), программы для создания собственного вымогателя также доступны для покупки. Цена аренды на месяц составляет от $800, а пожизненной подписки — около $2,5 тыс.

Почти все продавцы высококачественных вредоносных программ предоставляют покупателям подробные руководства по использованию своих продуктов. Что касается дешевых программ, то обзоры на них и советы по настройке публикуются даже на YouTube». ***(Насколько легко в настоящее время***

купить вредоносное ПО? // SecurityLab.ru (https://www.securitylab.ru/news/507983.php). 29.04.2020).

***

Діяльність хакерів та хакерські угруповування

Киберпреступная группировка DarkHotel в марте нынешнего года организовала масштабную вредоносную кампанию, нацеленную на китайские правительственные учреждения и их сотрудников.

По словам специалистов из Qihoo 360, обнаруживших атаки, преступники эксплуатировали уязвимость нулевого дня в серверах Sangfor SSL VPN для получения удаленного доступа к корпоративным и государственным сетям.

Эксперты выявили более 200 VPN-серверов, взломанных в ходе данной кампании. 174 из этих серверов были расположены в сетях правительственных учреждений в Пекине и Шанхае, а также в сетях китайских дипломатических представительств, действующих за рубежом, в таких странах, как Италия, Великобритания, Пакистан, Киргизия, Индонезия, Таиланд, ОАЭ, Армения, Северная Корея, Израиль, Вьетнам, Турция, Малайзия, Иран, Эфиопия, Таджикистан, Афганистан, Саудовская Аравия и Индия.

Использовав уязвимость в целевых устройствах, преступники заменили файл SangforUD.exe на версию с ловушкой. Данный файл представляет собой обновление для настольного приложения Sangfor VPN, которое сотрудники устанавливают на свои компьютеры для подключения к серверам Sangfor VPN. Когда работники подключались к взломанным серверам Sangfor VPN, им предоставлялось автоматическое обновление для их настольного клиента, содержащее вредоносный файл, который позже устанавливал на устройствах бэкдор.

Sangfor подтвердила факт компрометации устройств с помощью уязвимости нулевого дня и выпустила необходимое исправление. Компания также планирует выпустить скрипт для обнаружения взлома VPN-серверов преступниками и инструмент для удаления файлов, развернутых DarkHotel». ***(DarkHotel взломала правительственные учреждения Китая // SecurityLab.ru (https://www.securitylab.ru/news/506456.php). 07.04.2020).***

***

«Группа, известная под названием FIN7 (другие названия Navigator Group и Carbanak Group), использует подарочные карты и милых плюшевых мишек в своей новой физической фишинговой кампании.

Жертвы получают обычной посылкой плюшевого медведя и подарочную карту якобы от крупной американской сети магазинов бытовой электроники. В сопроводительном письме говорится, что это подарочная карта на $50, которые можно потратить на покупки в магазине. Список того, что можно купить, находится на флешке, которая также прилагается.

Флешка, вставленная в компьютер, заражает его бэкдором под названием GRIFFON, написанным на JavaScript. Код, загруженный на компьютер, позволяет злоумышленникам удаленно управлять некоторыми процессами, а также выполняет нужные киберпреступникам действия автоматически». ***(Киберпреступники обманывают жертв с помощью плюшевых мишек // SecureNews (https://securenews.ru/cybercriminals-trick-victims-with-teddy-bears/). 06.04.2020).***

***

«Государственный департамент, минфин и министерство национальной безопасности США вместе с Федеральным бюро расследований опубликовали предупреждение об угрозе со стороны хакеров из КНДР. Особую опасность их действия представляют для банков и других финансовых компаний, утверждается в сообщении. Северокорейских хакеров давно обвиняют в атаках на финансовые организации. В сообщении упоминаются, среди прочих известных фактов, распространение вымогательской программы WannaCry 2.0, которая в 2017 году заразила сотни тысяч компьютеров в разных странах, и которую спецслужбы США, Великобритании, Австралии, Канады и Новой Зеландии считают созданной в КНДР, мошенничество с банкоматами по схеме FASTCash и другие атаки.

В сообщении говорится, что действия КНДР представляют существенную угрозу для стабильности мировой финансовой системы и предлагается ряд мер противодействия: обмен информацией о киберугрозах, сегментация сетей, регулярное резервное копирование данных, обучение методам защиты от социального инжиниринга и так далее. Другим странам рекомендуется как можно принять стандарты борьбы с отмыванием денег и противодействия финансированию терроризма и распространения оружия массового уничтожения, разработанные межправительственной комиссией по финансовому мониторингу (FATF)». ***(США предупреждают о новой угрозе со стороны северокорейских хакеров // Открытые системы (https://www.computerworld.ru/news/SShA-preduprezhdayut-o-novoy-ugroze-so-storony-severokoreyskih-hakerov). 21.02.2020).***

***

«Госдепартамент США, Министерство финансов США, Министерство национальной безопасности США и Федеральным бюро расследований выпустили совместный отчет, в котором предупреждают мир «серьезной киберугрозе» для банковских и финансовых учреждений, исходящей от правительственных северокорейских хакеров. Власти убеждены, что такие атаки представляют «существенную угрозу целостности и стабильности международной финансовой системы».

Документ содержит краткое описание недавних киберпреступлений Северной Кореи и основывается на прошлогоднем отчете Совета Безопасности ООН, в котором подробно описывалась тактика Пхеньяна, который часто использует хакеров для обхода международных санкций, а киберпреступления как способ для сбора средств. Так, по данным ООН, северокорейские хакеры прибегают к следующим тактикам:

- атаки на банки и других финансовые организации и кража средств;
- атаки на криптовалютные биржи и кража средств;
- криптоджекинг: хакеры компрометируют серверы по всему миру, чтобы добывать криптовалюту;
- вымогательские кампании: компрометация сети организаций и вымогательство выкупов; взлом сайтов на заказ для сторонних клиентов, и последующая эксплуатация целей; вынуждение жертв оплачивать «консультации», которые помогают предотвратить будущие атаки.

Многие из таких атак были направлены на финансовый сектор, откуда северокорейские хакеры похитили более 2 миллиардов долларов.

Однако власти США не только в очередной раз предупредили об опасности северокорейских хакеров. Также, в рамках программы Rewards for Justice, американские власти предложили вознаграждение в размере до 5 000 000 долларов США за любую информацию, которая поможет нарушить работу финансовых механизмов и частных лиц, «участвующих в определенных видах деятельности, поддерживающих Северную Корею». Под этими видами деятельности подразумеваются отмывание денег, уклонение от санкций, киберпреступность и разработка оружия массового уничтожения.

Чиновники надеются, что публикация совместного отчета улучшит безопасность и осведомленность компаний, а также поможет повлиять на «хакерские» прибыли Пхеньяна и, косвенно, на программу вооружений страны.

«Международному сообществу, сетевым защитникам и общественности жизненно важно сохранять бдительность и совместно работать над уменьшением киберугрозы, исходящей от Северной Кореи», — говорят представители США». ***(Мария Нефёдова. Власти США предлагают 5 млн долларов за информацию о северокорейских хакерах // Xakep (https://xakep.ru/2020/04/16/5-million-reward/). 16.04.2020).***

***

«Аналитики компании ESET сообщают, что русскоязычная хакерская группа Energetic Bear (она же DragonFly), взломала два сайта, принадлежащих международному аэропорту Сан-Франциско.

Судя по опубликованной представителями аэропорта информации, компрометация произошла в марте текущего года и затронула сразу два ресурса. Так, атаки злоумышленников были направлены на сайт SFOConnect.com, которым пользуются сотрудники аэропорта, а также на сайт SFOConstruction.com, использующийся строительными подрядчиками воздушной гавани. Сообщалось, что в обоих случаях злоумышленники взломали ресурсы и внедрили на них вредоносный код, который эксплуатировал уязвимость в Internet Explorer для кражи учетных данных.

Однако аналитики ESET пишут, что целью злоумышленников являлись не учетные данные посетителей скомпрометированных сайтов, но учетные данные пользователей Windows.

«Цель заключалась в том, чтобы собрать учетные данные Windows (имя пользователя, хеш NTLM), эксплуатируя функциональность SMB и префикс file://», — говорят исследователи.

Как известно, хеш NTLM можно взломать, чтобы в итоге получить пароль пользователя Windows в формате простого текста. То есть если бы хакеры имели доступ к внутренней сети аэропорта, они могли бы использовать эти учетные данные, похищенные у сотрудников, для бокового перемещения по внутренней сети, последующего проведения разведки, кражи данных или осуществления саботажа.

После инцидента сотрудники аэропорта принудительно сбросили все почтовые и сетевые пароли, связанные с SFO, так что похищенные хеши NTLM будут бесполезны для атак. Но оба сайта использовались и другими пользователями, которые не были сотрудниками аэропорта. Теперь их призывают тоже подумать о безопасности и срочно поменять пароли.

По мнению аналитиков ESET, за этими атаками стоит русскоязычная правительственная группировка Energetic Bear (она же DragonFly, Crouching Yeti), активная с 2010 года. Основными целями группы обычно являются организации в энергетическом секторе (отсюда происходит название Energetic Bear), расположенные на Ближнем Востоке, в Турции и США. Однако в последние годы группировка также атакует и другие цели, например, компании в аэрокосмической и авиационной отрасли.

Так, в отчете «Лаборатории Касперского» от 2018 года описаны watering hole атаки Energetic Bear, которые использовали тот же трюк с префиксом file:// для получения хешей NTLM от пользователей, посещающих взломанный сайт. Специалисты ESET подчеркивают, что данный метод атак используется группой уже много лет…». ***(Мария Нефёдова. Русскоязычная группировка Energetic Bear взломала сайты аэропорта Сан-Франциско // Xakep (https://xakep.ru/2020/04/15/energetic-bear-sfo-hack/). 15.04.2020).***

***

«Нещодавні кібератаки на чеські лікарні ймовірно є роботою російських хакерів - російська сторона це заперечує.

…про це у понеділок повідомили чеські ЗМІ

Зокрема, видання Lidové noviny із посиланням на два достовірні джерела заявило, що, на думку слідчих, Росія, ймовірно, стоїть за кібератаками на чеські лікарні.

За даними газети, цю інформацію надав представник слідчої групи, що обіймає високу посаду, та підтвердив член Ради держбезпеки.

"Це організовано іноземною державою. Починають з'являтись свідчення, що за цим може бути Росія. Туди ведуть IP-адреси", - заявило джерело видання.

Російське посольство у Празі у своєму Facebook заперечило публікації чеських ЗМІ, назвавши їх "вигадками, брудною антиросійською атакою і відкритою провокацією".

"Ми категорично відкидаємо подібні вигадки", - повідомили в посольстві РФ. За словами російських дипломатів, це чергова фейкова новина", єдиною метою якої є створення ворожого іміджу Росії, особливо серед місцевого населення.

Дві чеські лікарні минулого тижня зіштовхнулися зі спробами кібератак, але їх вдалося відбити. Державний секретар США Майк Помпео висловив занепокоєння з приводу нападів на чеську систему охорони здоров'я на тлі пандемії коронавірусу.

Ознаки хакерських атак нагадують Естонію в 2007, де, як і в Чехії, напередодні усунули радянський пам'ятник. Російські кібератаки після знесення "бронзового солдата" у Таллінні завдали Естонії помітної шкоди, але стали поштовхом для поліпшення цифрової інфраструктури». ***(Сліди кібератак на чеські лікарні ведуть до Росії, заявили у Чехії // Європейська правда (https://www.eurointegration.com.ua/news/2020/04/21/7108969/). 21.04.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«В ходе одной из вредоносных кампаний ПО Emotet отключило компьютерную сеть одной из неназванных организаций. Как сообщила Microsoft, сбой в работе был вызван увеличением максимальной нагрузки на ЦП устройствах под управлением Windows и отключением интернет-соединений.

«Вредонос избегал обнаружения антивирусными решениями благодаря регулярным обновлениям от C&C-сервера, контролируемого злоумышленниками, и распространялся по системам, вызывая перебои в работе сети и отключая основные службы на протяжении почти недели», — сообщила компания Microsoft.

Причиной компрометации стал один из сотрудников организации, который открыл фишинговое письмо с вредоносным вложением, тем самым передав учетные данные злоумышленникам. Через пять дней Emotet был загружен и запущен на системах организации. Вредоносная программа незаметно распространялась по сети, похищала учетные данные администраторов и аутентифицировалась на новых системах, которые впоследствии использовались для взлома других устройств.

Несмотря на усилия команды IT-специалистов организации, за 8 дней вся сеть вышла из строя из-за перегрева, зависаний и перезагрузок компьютеров, а также из-за замедления интернет-соединений.

Команда специалистов из Microsoft смогла остановить распространение заражения с помощью элементов управления ресурсами и буферных зон, предназначенных для изоляции активов с правами администратора. В конечном итоге она смогла полностью устранить Emotet после загрузки новых сигнатур антивируса и развертывания специальных решений для обнаружения и удаления вредоносных программ.

Microsoft рекомендует использовать инструменты фильтрации электронной почты, чтобы автоматически обнаруживать и останавливать фишинговые

электронные письма, распространяющие инфекцию Emotet, а также использовать многофакторную аутентификацию, мешая злоумышленникам воспользоваться украденными учетными данными». ***(Вредонос Emotet за 8 дней вывел из строя всю IT-сеть Китая // SecurityLab.ru (https://www.securitylab.ru/news/506451.php). 06.04.2020).***

***

«Лаборатория Касперского» обнаружила целевую кампанию, которая действует с мая 2019 года и направлена на пользователей в Азии. В ходе неё было заражено более десяти часто посещаемых потенциальными жертвами сайтов, связанных с религией, волонтёрскими и благотворительными программами. Такой тип атаки, позволяющий зловреду проникнуть на устройство сразу после посещения пользователем скомпрометированного ресурса, называется watering hole («атака на водопое»).

Кампания получила название Holy Water, в рамках неё злоумышленники используют нестандартные подходы, но их нельзя назвать технически сложными. Главные особенности — быстрое эволюционирование и применение широкого набора инструментов, в частности атакующие использовали хранилище GitHub и ПО с открытым исходным кодом.

Злоумышленники инфицировали сайты, которые принадлежат как отдельным людям, так и общественным организациям, благотворительным фондам и другим компаниям. На интернет-страницы внедрялся загрузчик, который позволял установить на устройства жертв бэкдор сразу после посещения ими скомпрометированного ресурса. Такое ПО открывает полный доступ к заражённому устройству: позволяет вносить изменения в файлы, собирать конфиденциальную информацию с устройства и данные о проводимых на нём действиях.

Кроме того, в ходе кампании использовался ещё один бэкдор, который позволяет обмениваться зашифрованными данными с удалённым сервером. Его задача — собрать информацию о посетителе и проверить, является ли он целью. Если да, то на его устройство загружается плагин, который провоцирует загрузку, показывая фейковое обновление Adobe Flash. Файл, который позволял исполнять фейковое всплывающее уведомление от Adobe Flash, хранился на GitHub. Он уже закрыт, но благодаря предоставленной GitHub возможности изучить его историю эксперты «Лаборатории Касперского» смогли получить уникальные данные о деятельности и инструментах злоумышленников.

Обнаружение кампании Holy Water стало возможным из-за её низкобюджетности и не полностью проработанного набора инструментов, который менялся несколько раз за несколько месяцев.

«Атака типа watering hole через узкоспециализированные сайты — это эффективный способ заражения устройств определённой группы людей. По сути, эта кампания ещё раз демонстрирует, почему так важно задумываться о приватности в интернете. Риски её нарушения особенно высоки, когда речь идёт о разных социальных группах и меньшинствах, потому что всегда есть злоумышленники, которые могут быть заинтересованы в такой информации», —

комментирует Юрий Наместников, руководитель российского исследовательского центра «Лаборатории Касперского». ***(Обнаружена целевая атака, жертвы которой заражались через часто посещаемые ими сайты // IKSMEDIA.RU (http://www.iksmedia.ru/news/5655044-Obnaruzhena-celevaya-ataka-zhertvy.html). 02.04.2020).***

***

«Эксперты глобального центра исследований и анализа угроз «Лаборатории Касперского» (GReAT) обнаружили целевую кампанию по распространению троянца Milum. Он позволяет получить дистанционное управление устройствами в различных компаниях, в том числе промышленных. Эта кампания, получившая название WildPressure, всё ещё активна. В данный момент большинство её жертв находится на Ближнем Востоке.

Целевые кибератаки (APT) – наиболее сложные и опасные угрозы. Зачастую злоумышленники тайно получают расширенный доступ к системе, чтобы препятствовать её нормальной работе или красть данные. Подобные кампании, как правило, создаются и разворачиваются людьми, имеющими доступ к крупным финансовым и профессиональным ресурсам. Именно поэтому WildPressure быстро привлёк внимание исследователей «Лаборатории Касперского».

На данный момент эксперты смогли получить несколько почти идентичных образцов троянца Milum, которые не имеют общего кода ни с одной известной ранее APT-кампанией. Все они обладают возможностями для удалённого управления устройствами. В частности, троянец имеет следующие функции:

загружать и выполнять команды от своего оператора;

собирать различную информацию с атакованной машины и отправлять её на командно-контрольный сервер;

обновляться до более новой версии.

Исследователи GReAT стали первыми, кто зафиксировал деятельность троянца Milum. В августе 2019 года эксперты «Лаборатории Касперского» впервые обнаружили это вредоносное ПО. Исследование показало, что первые три образца были созданы ещё в марте 2019 года. Используя имеющуюся телеметрию, эксперты сделали предположение, что большинство целей этой вредоносной кампании находятся на Ближнем Востоке.

Пока многое в отношении WildPressure остаётся неясным, в том числе точный механизм распространения троянца Milum.

«Каждый раз, когда промышленный сектор подвергается нападению, это вызывает беспокойство. Аналитики должны обращать внимание на подобные атаки, поскольку их последствия могут быть разрушительными. Пока у нас нет подтверждения, что у злоумышленников, стоящих за WildPressure, есть какие-либо намерения, помимо сбора информации из атакованных сетей. Однако эта кампания всё ещё активно развивается. Мы уже обнаружили новые вредоносные образцы, кроме трёх первоначально выявленных. Пока мы не знаем, что будет происходить по мере развития WildPressure, но будем продолжать следить за её активностью», – сказал Денис Легезо, старший антивирусный эксперт «Лаборатории Касперского»…» ***(Обнаружена ранее неизвестная вредоносная кампанию***

WildPressure // IKSMEDIA.RU (http://www.iksmedia.ru/news/5654994-Obnaruzhena-ranee-neizvestnaya-vred.html). 02.04.2020).

***

«Ботнет Hoaxcalls активно атакует устройства Grandstream UCM6200 через исправленную недавно уязвимость CVE-2020-5722. Проблема затрагивает HTTP-интерфейс систем IP PBX и является критической (9,8 балла по шкале CVSS3.1). С ее помощью злоумышленник может осуществить SQL-инъекцию через особым образом сконфигурированный HTTP-запрос и выполнить команду оболочки с привилегиями суперпользователя (в версиях до 1.0.19.20) или внедрить HTML-код в электронное письмо для восстановления пароля (в версиях до 1.0.20.17).

Функция восстановления пароля в web-интерфейсе устройств Grandstream UCM6200 принимает имя пользователя в качестве входных данных и проверяет его наличие в базе данных SQLite. Используя в качестве имени пользователя определенную строку кода, атакующий может осуществить SQL-инъекцию и создать обратную оболочку для удаленного выполнения кода или ввести произвольный HTML-код в отправленное жертве электронное письмо для восстановления пароля.

Как сообщают исследователи компании Palo Alto Networks, уже более недели операторы Hoaxcalls активно атакуют устройства через уязвимость CVE-2020-5722, добавляют их в свой ботнет и используют для осуществления DDoS-атак. Злоумышленники также атакуют маршрутизаторы Draytek Vigor через другую критическую уязвимость (CVE-2020-8515).

Вредоносное ПО Hoaxcalls создано на базе кода семейства Gafgyt/Bashlite и распространяется автоматически через уязвимости в устройствах Grandstream и DrayTek. Ботнет используется для осуществления разных видов DDoS-атак в зависимости от полученных с C&C-сервера команд.

Уязвимость CVE-2020-5722 в Grandstream полностью исправлена в версии 1.0.20.17, а CVE-2020-8515 в DrayTek исправлена в версии 1.5.1.» ***(Hoaxcalls атакует устройства Grandstream UCM6200 через исправленную уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/506601.php). 13.04.2020).***

***

«Аналитики компании Bitdefender предупредили, что шпионский вредонос Agent Tesla используется для атак на нефтегазовые компании.

Так, в одной из фишинговых кампаний злоумышленники выдавали себя за себя за египетскую государственную нефтяную компанию Enppi (Engineering for Petroleum and Process Industries), и нацеливали свои атаки на организации в Малайзии, Соединенных Штатах, Иране, Южной Африке, Омане и Турции и других странах.

В рамках другой кампании хакеры прикидывались сотрудниками транспортной компании и использовали подлинную информацию о нефтяном/химическом танкере, чтобы обмануть своих жертв на Филиппинах.

Интересно, что во время этой кампании хакеры продемонстрировали прекрасное знание отраслевого жаргона, из-за которого их письма казались настоящими.

В рамках первой кампании злоумышленники выдали себя за представителей Enppi, чтобы запросить закупку оборудования и материалов в рамках проекта Rosetta Sharing Facilities от имени газовой компании Burullus. Такие письма содержали вложенные архивы, предназначенные для доставки Agent Tesla на машины жертв.

Проникнув в систему, малварь собирала учетные данные и конфиденциальную информацию, а затем предавала их на управляющий сервер, расположенный по адресу smtp[:]//smtp.yandex.com:587.

По данным Bitdefender, пик атак пришелся на 31 марта 2020 года, хотя обычное ежедневное количество инцидентов по-прежнему не превышает пять. Малайзия, Ближний Восток, Северная Африка и Соединенные Штаты пострадали от этой кампании больше всего.

Вторая кампания, похоже, началась примерно 12 апреля 2020 года, и теперь целями Agent Tesla стали компании-перевозчики на Филиппинах.

Bitdefender отмечает, что атаки на нефтегазовую отрасль учащаются с октября 2019 года, и достигли максимума в феврале 2020 года. За это время от компаний энергетического сектора поступило более 5000 сообщений о попытках атак, и аналитики полагают, что эта активность может быть связана с колебаниями цен на нефть и нефтяным кризисом.

Исследователи подчеркивают, что это первый случай, когда Agent Tesla используется для атак на компании нефтегазовой отрасли. Дело в том, что сам инфостилер – совсем несложное по меркам экспертов решение. Его нетрудно приобрести на хакерских форумах и им пользуются многие злоумышленники…» ***(Мария Нефёдова. Малварь Agent Tesla атакует нефтегазовые компании // Xakep (https://xakep.ru/2020/04/22/oil-and-gas-industry/). 22.04.2020).***

***

«Крупный поставщик ИТ-услуг, американская компания Cognizant, стал жертвой шифровальщика Maze. Атака привела к перебоям в обслуживании некоторых клиентов.

Cognizant предоставляет локальные и облачные услуги для других компаний по всему миру, в том числе технологические, консалтинговые и операционные (специалисты компании дистанционно управляют машинами своих клиентов для установки исправлений, обновления ПО, предоставляют услуги удаленной поддержки и так далее). Штат компания насчитывает около 300 000 сотрудников по всему миру, она занимает 193 место в списке Fortune 500, а среди ее клиентов чистятся крупные банковские организации, компании из сферы здравоохранения, производства и многие другие.

В минувшие выходные ИТ-гигант подтвердил, что пострадал от атаки шифровальщика, сообщив, что системы компании оказались заражены вымогателем Maze. Пока не сообщается, сколько именно систем пострадало, но известно, что инцидент перевел к перебоям в обслуживании некоторых клиентов, а также, в теории, создал для них угрозу.

Представители компании уже обратились в правоохранительные органы и опубликовали индикаторы компрометации для своих клиентов, в том числе IP-адреса серверов и хэши файлов kepstl32.dll, memes.tmp и maze.dll. Перечисленные в этом списке IP-адреса и файлы уже использовались в предыдущих атаках Maze.

Опираясь эти данные, ИБ-эксперт Виталий Кремез подготовил правило Yara, которое можно использовать для обнаружения DLL шифровальщика Maze.

Журналисты издания Bleeping Computer сообщают, что операторы Maze отказались обсуждать с ними данную атаку и не взяли на себя ответственность за взлом Cognizant. Скорее всего, хакеры не готовы обсуждать этот инцидент, чтобы не осложнять ситуацию, пока идет обсуждения выкупа (подобные прецеденты уже были).

Также журналисты отмечают, что в злоумышленники, вероятно, присутствовали в сети Cognizant много недель и постепенно продвигались все дальше, компрометируя все больше систем. Кроме того, Bleeping Computer напоминает, что перед развертыванием шифровальщика операторы Maze всегда крадут файлы компаний, а затем используют похищенную информацию против пострадавших в качестве дополнительного рычага давления. Так, вымогатели угрожают обнародовать украденные данные, если жертва не заплатит. К сожалению, эти угрозы нельзя назвать пустыми, так как у группировки есть специальный сайт, где действительно публикуются данные компаний, которые отказались платить». ***(Мария Нефёдова. Компания Cognizant пострадала от атаки шифровальщика Maze // Xakep (https://xakep.ru/2020/04/21/cognizant-hacked/). 21.04.2020).***

***

«Специалисты китайской ИБ-компании QuoIntelligence (QuoINT) обнаружили новую малварь, нацеленную на внутреннюю сеть производителя игр Gravity (в частности разрабатывающего известную ММОРПГ Ragnarok Online).

Судя по всему, атаки на компанию имели место в начале 2020 года, и за ними стоит одна из крупнейших правительственных хак-групп Китая — Winnti (она же APT41, BARIUM, Blackfly). Пока неясно, удалось ли хакерам добиться успеха, и достигли ли атаки цели.

«Нам удалось извлечь файл конфигурации малвари и определить предполагаемую цель. В данном случае в конфигурацию была включена следующая строка: 0x1A0: GRAVITY. Основываясь на ранее известных фактах и целях группировки Winnti, мы считаем, что этот образец, вероятно, использовался для таргетированной компании против Gravity Co., Ltd., южнокорейской компании, выпускающей видеоигры», — пишут специалисты QuoINT.

Обнаруженной малвари дали название Winnti Dropper, то есть это разновидность вредоноса, которая первой заражает компьютер жертвы, а затем доставляет в систему другое вредоносное ПО.

По данным аналитиков QuoINT, направленная на Gravity кампания является последним на текущей момент инцидентом в длинной череде атак Winnti,

нацеленных на индустрию видеоигр в целом и на игровые компании из Южной Кореи и Тайваня в частности.

Представители Gravity пока никак не прокомментировали выводы специалистов QuoINT…». ***(Мария Нефёдова. Китайские хакеры атаковали компанию-разработчика Ragnarok Online // Хакер (https://xakep.ru/2020/04/21/winnti-vs-gravity/). 21.04.2020).***

***

«Эксперты компании BI.ZONE зафиксировали всплеск активности трояна Faketoken. Малварь похищает деньги у пользователей Android-устройств, маскируясь под приложение популярной торговой площадки.

Исследователи рассказывают, что Faketoken образца 2020 года способен перехватывать SMS на устройстве, передавать сообщения на сервер преступников, а также отображать фишинговые окна поверх легитимных приложений (для сбора данных банковских карт). Отличительной особенностью последней версии трояна стала способность препятствовать удалению малвари с устройства с использованием антивирусных программ. Впрочем, эксперты отмечают, что удалить Faketoken все же возможно — для этого необходимо перевести ОС в безопасный режим.

Специалисты BI.ZONE связывают нынешнюю активность трояна с массовым переходом россиян на удаленную работу из-за пандемии коронавируса. Люди сидят дома, растет популярность онлайн-торговли, а злоумышленники не упускают шанс и пользуются этим.

В настоящее время в ботнет Faketoken входит более 10 000 зараженных устройств. Для распространения вредоносного ПО злоумышленники ежедневно регистрируют до семи новых фишинговых доменов.

Эксперты пишут, что большинство заражений происходит по стандартной схеме. Пользователь размещает объявление на торговой площадке и получает SMS или сообщение в мессенджере со ссылкой на фишинговую страницу. Он переходит по ссылке и скачивает установочный .apk файл, который внешне неотличим от настоящего приложения данной онлайн-площадки.

После запуска .apk и предоставления прав вредоносному приложению, злоумышленники получают возможность управлять зараженным устройством. Далее, когда жертва заходит в целевое легитимное приложение (например, мобильный банк или сервис такси), троян под вымышленным предлогом запрашивает ввод данных банковской карты и перехватывает SMS-коды от банка. С помощью этой информации преступники похищают денежные средства пользователя.

«Faketoken очень быстро распространяется — ежедневно троян заражает более 2000 устройств. Чтобы не стать жертвой преступников, мы рекомендуем не переходить по ссылкам из подозрительных источников, устанавливать приложения только из официальных магазинов и не отключать защитный сервис Google Play Protect. Использование антивируса и своевременное обновление антивирусных баз также поможет снизить риск заражения», — прокомментировал Евгений Волошин, директор по безопасности компании BI.ZONE…» ***(Мария Нефёдова. Старый***

троян Faketoken активизировался из-за COVID-19 // Xakep (https://xakep.ru/2020/04/20/faketoken-2/). 20.04.2020).

***

«ИБ-исследователи из компании ReversingLabs сообщили об обнаружении 725 вредоносных библиотек, похищавших содержимое буфера обмена, в официальном репозитории RubyGems…

Вредоносные пакеты были загружены в RubyGems в период с 16 по 25 февраля 2020 с двух учетных записей: JimCarrey и PeterGibbons. Исследователи пишут, что малварь была удалена из RubyGems еще 27 февраля, через два дня после того, как ReversingLabs уведомила разработчиков о своей находке.

Все обнаруженные вредоносны были клонами различных легитимных библиотек. Они использовали технику typosquatting, то есть имели нарочито похожие на оригиналы имена, и даже работали по назначению, но также содержали дополнительные вредоносные файлы.

Дополнительный файл, встроенный в каждый такой пакет, носил название aaa.png. Несмотря на расширение, этот файл не был изображением PNG. На самом деле он представлял собой исполняемый файл Windows PE. Установка любой из вредоносных библиотек вызвала цепочку следующих действий:

- PE-файл создавал Ruby-скрипт с именем aaa.rb, содержащий интерпретатор Ruby и все необходимые зависимости для запуска;
- этот скприт создавал скрипт Visual Basic с именем oh.vbs;
- скрипт создавал в реестре ключ для автозапуска;
- ключ автозапуска выполнял второй скрипт Visual Basic каждый раз, когда копмьютер запускался или перезагружался;
- второй скрипт перехватывал данные, отправленные в буфер обмена, и искал среди них шаблоны, похожие на адреса криптовалютных кошельков, и подменял их на кошелек злоумышленника.

ReversingLabs пишут, что эти библиотеки были загружены тысячами пользователей. Однако судя по Bitcoin-адресу злоумышленника, за все время активность кампании ему так и не удалось перехватить какие-либо платежи, подменив адрес на собственный.

Исследователи полагают, что за этой атакой стоит тот же человек или группировка, которая загружала вредоносные библиотеки в RubyGems ранее, в 2018 и 2019 годах. Оба инцидента отличались использованием схожих методов, а целью тоже была кража криптовалюты у пользователей». ***(Мария Нефёдова. В репозитории RubyGems обнаружено более 700 вредоносных библиотек // Xakep (https://xakep.ru/2020/04/17/rubygems-malware/). 17.04.2020).***

***

«Специалисты компании Cisco Talos сообщили о новой вредоносной кампании против правительственных учреждений и промышленных предприятий Азербайджана, в ходе которой злоумышленники используют тему коронавируса с целью заражения сетей трояном для удаленного доступа (RAT).

По данным исследователей, вредонос предназначен для атак на использующиеся в электроэнергетическом секторе SCADA-системы, в частности на ветротурбинные системы, производитель которых пока еще не определен.

Злоумышленники рассылают вредоносные документы Microsoft Word, загружающие на атакуемую систему написанный на Python ранее неизвестный троян PoetRAT. Свое название вредонос получил из-за многочисленных отсылок к сонетам Уильяма Шекспира.

PoetRAT оснащен всеми функциями, характерными для RAT. Он может похищать конфиденциальные документы, нажатия клавиш на клавиатуре, пароли и даже изображения с web-камер, а также предоставляет своим операторам полный контроль над скомпрометированной системой.

Как именно вредоносные документы Microsoft Word попадают на систему, неизвестно. Однако, поскольку они доступны для загрузки по обычной ссылке, исследователи предположили, что злоумышленники рассылают фишинговые письма или вредоносные URL.

Атаки начались в феврале нынешнего года, и с тех пор исследователи зафиксировали три волны. Некоторые поддельные документы были якобы от правительственных учреждений Азербайджана или от Организации оборонных исследований и разработок Индии. Некоторые файлы назывались C19.docx и не имели никакого содержимого.

Встроенный в документ макрос Visual Basic Script записывает вредоносное ПО на диск в виде архива smile.zip, состоящего из интерпретатора Python и самого трояна. Вредонос проверяет, не запущен ли он на виртуальной машине, и в случае выявления песочницы автоматически удаляется с системы». ***(Новый RAT атакует SCADA-системы в Азербайджане // SecurityLab (https://www.securitylab.ru/news/506863.php). 20.04.2020).***

***

«Imperva, яка спеціалізується на кібербезпеці, випустила черговий звіт з даними по інтернет-трафіку. Зокрема, компанія відзначила, що активність шкідливих ботів в інтернеті значно збільшилася і досягла 24%, що є рекордним показником. Такі боти зазвичай застосовуються для накрутки трафіку, передплатників, розсилки спаму або крадіжки паролів і персональних даних.

У порівнянні з минулим роком, трафік шкідливих ботів виріс на 18%. Частка «хороших» ботів при цьому скоротилася на 25% і тепер становить всього 13%. Сумарно трафік всіх ботів становить 37%. Решта (63%) – це інтернет-користувачі, частка яких збільшилася всього лише на 1%.

Найбільш уразливими до «поганих» ботів, на думку авторів дослідження, є фінансові послуги. За ними йдуть сфера освіти і науки, а також IT-послуги. Ринок нерухомості і дослідження ринку практично не цікавлять творців шкідливих роботизованих програм.

Imperva вважає, що зростання трафіку ботів пояснюється тим, що багато з них використовують просунуту систему заходів з різних підмереж (APBs). Щоб обдурити системи розпізнавання ботів і видати себе за людину, вони випадковим

чином змінюють IP-адреси і використовують анонімні проксі-сервери. Більшість таких ботів розробляються під браузер Google Chrome.

Якщо говорити про географію походження «поганих» ботів, то найбільша кількість трафіку (майже 46%) надходить з США. Далі йдуть Нідерланди та Канада. Однак найчастіше блокується бот-трафік з Росії (21,1%) і Китаю (19%)». ***(Чверть усього інтернет-трафіку складають шкідливі боти // ВСВІТІ (http://vsviti.com.ua/news/113902). 23.04.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Власти Нидерландов сообщают, что на прошлой неделе были закрыты сразу 15 сервисов для осуществления DDoS-атак по найму. В этой масштабной операции приняли участие представители веб-хостинговых компаний, регистраторы доменов, сотрудники Европола, Интерпола и ФБР.

Названия закрытых сервисов пока не раскрываются. Зато известно, что в Нидерландах был арестован 19-летний подозреваемый, устраивавший DDoS-атаки на правительственные сайты. Так, по его вине два голландских правительственных ресурса не работали на протяжении несколько часов 19 марта 2020 года.

Один из атакованных правительственных сайтов — Overheid.nl. Ресурс содержит информацию обо всех услугах и данных государственных организаций в стране, и в последнее время, из-за пандемии COVID-19, его часто посещают голландские граждане.

Другой сайт, MijnOverheid.nl, представляет собой платформу, которая позволяет получать цифровые услуги от правительства Нидерландов, в том числе связанные с налоговыми сборами, детскими пособиями и так далее…». ***(Мария Нефёдова. Голландская полиция закрыла 15 DDoS-сервисов за неделю // Xakep (https://xakep.ru/2020/04/13/dutch-police-vs-ddos/). 13.03.2020).***

***

Технічні аспекти кібербезпеки

«Больше половины из ТОП 1 млн самых популярных web-сайтов по Alexa используют протокол HTTPS, однако далеко не весь зашифрованный трафик является безопасным. Киберпреступники все чаще полагаются на SSL-сертификаты с целью вызвать у жертв ложное чувство безопасности при переходе по вредоносным ссылкам.

Как сообщили специалисты из компании Menlo Security, в 2019 году HTTPS-протокол использовало около 52% из 1 млн популярных сайтов. Почти все (96,7%) online-посещения, инициированные пользователями, осуществлялись по HTTPS-протоколу, однако только 57,7% URL-адресов в электронных письмах являлись

HTTPS-ссылками. Таким образом прокси-серверы и межсетевые экраны следующего поколения, на которые полагаются многие компании, могут пропустить угрозы на вредоносных web-сайтах, если проверка SSL не включена.

В ходе анализа киберугроз на web-сайтах с HTTPS специалисты выяснили, что 47,1% из них используют уязвимое серверное программное обеспечение, например, более старые версии Apache, Drupal или WordPress. 41,5% сайтов с HTTPS не классифицированы, а 10,7% являются фишинговыми. Почти 67% не браузерного трафика, генерируемого конечными точками во время загрузки обновлений, проходит по SSL.

«Преступнику намного проще размещать фишинговые ссылки или вредоносные файлы по SSL-протоколу, поскольку его практически не проверяют», — пояснили специалисты.

Некоторые организации избегают проверки SSL-сертификатов из соображений конфиденциальности, другие — из-за проблем с производительностью. Как отметили эксперты, пропускная способность локальных прокси-серверов и межсетевых экранов уменьшается как минимум в пять раз при включении SSL-шифрования. При том же количестве сотрудников, пользующихся интернетом, бизнесу потребуется в пять раз больше устройств для поддержания одинаковой пропускной способности. В данной ситуации предприятия подвергают себя гораздо большему риску атак, чем даже несколько лет назад». ***(Преступники скрывают вредоносные сайты за SSL-сертификатами // SecurityLab.ru (https://www.securitylab.ru/news/506579.php). 10.04.2020).***

***

«Специалисты компании RACK911 Labs продемонстрировали , как с помощью символических ссылок (directory junction на Windows и symlink на macOS и Linux) можно превратить практически любое антивирусное решение в инструмент для самоуничтожения.

Большинство антивирусных решений работают по одной схеме: при сохранении неизвестного файла на жесткий диск компьютера антивирус сканирует его в реальном времени. Если файл признается подозрительным, он либо отправляется в «карантин» - защищенное место, где ожидает дальнейших действий пользователя, либо удаляется. В связи с характером проводимых операций антивирусное ПО как правило обладает на системе наивысшими привилегиями, что, по словам специалистов RACK911 Labs, «открывает двери для широко спектра уязвимостей в безопасности и неопределенностей параллелизма» (так называемое «состояние гонки» или race condition).

Как сообщают исследователи, в большинстве антивирусных решений не учитывается небольшой зазор времени между сканированием файла и дальнейшими действиями с ним. Локальный злоумышленник или вредоносное ПО может вызвать неопределенность параллелизма с помощью символических ссылок и, воспользовавшись привилегированным статусом действий с файлом, отключить антивирусное ПО или сделать его полностью бесполезным.

Исследователи смогли успешно удалить важные файлы антивирусного ПО на компьютерах под управлением Windows, macOS и Linux, сделав его бесполезным, и

даже удалить ключевые системные файлы и тем самым вызвать серьезные повреждения, потребовавшие переустановки ОС.

По словам исследователей, осуществить представленную ими атаку очень просто, и бывалый хакер справится с ней без труда. Самое сложное – определить точное время, когда нужно выполнить directory junction или symlink. В данной атаке тайминг играет ключевую роль, поскольку опоздание даже на одну секунду сделает эксплоит бесполезным. Однако в случае с некоторыми антивирусными решениями тайминг не имел никакого значения, и для запуска их самоуничтожения было достаточно закольцевать запуск эксплоита.

Компания RACK911 Labs начала рассылать уведомления затронутым вендорам осенью 2018 года, и большинство из них, за небольшим исключением, уже исправили уязвимость». ***(Представлен способ превращения антивирусов в инструмент для самоуничтожения // SecurityLab (https://www.securitylab.ru/news/506939.php). 22.04.2020).***

***

«Команда специалистов Университета имени Давида Бен-Гуриона в Негеве (Израиль) под руководством Мордехая Гури продемонстрировала , как с помощью кулера компьютера можно похищать данные с физически изолированных систем. Исследователям удалось заставить вентилятор создавать контролируемые вибрации, позволившие им извлечь данные из атакуемой системы.

Атака получила название AiR-ViBeR. В отличие от атаки Fansmitter, представленной специалистами университета Бен-Гуриона несколько лет назад, AiR-ViBeR базируется не на генерируемом кулером шуме, а на вибрациях.

Исследователи внедрили в физически изолированный компьютер вредоносное ПО, позволяющее менять скорость вращения вентилятора. Путем ускорения и замедления вращения специалисты управляли частотой производимых вибраций, создавая из них определенные комбинации, которые передавались в окружающую среду (в частности, через стол).

Как пояснил Гури, находящийся поблизости такого компьютера злоумышленник может зафиксировать эти вибрации с помощью акселерометра, которым оснащены все современные смартфоны, выявить комбинации колебаний, расшифровать их и восстановить передаваемую информацию.

Зафиксировать вибрации можно двумя способами. К примеру, злоумышленник может положить свой смартфон рядом с атакуемым компьютером и регистрировать колебания без необходимости даже прикасаться к компьютеру. Если у атакующего нет доступа к месту, где находится целевая система, он может заразить вредоносным ПО смартфон сотрудника, у которого такой доступ есть. Вредонос будет фиксировать вибрации и передавать злоумышленнику, а владелец смартфона останется в полном неведении. По словам Гури, это очень легко сделать, поскольку в современных мобильных устройствах доступ к акселерометру может получить любое приложение, и разрешение пользователя для этого не нужно.

Правда, на получение данных с помощью AiR-ViBeR потребуется очень много времени. По факту, атака является самой медленной из всех такого рода – 0,5

бит/с, и ее использование в реальной жизни весьма маловероятно». ***(Представлен способ хищения данных через вибрации кулера компьютера // SecurityLab (https://www.securitylab.ru/news/506774.php). 17.04.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Компания Oracle выпустила обновления безопасности, устраняющие в общей сложности 405 уязвимостей в различных продуктах. 286 проблем могли быть проэксплуатированы удаленно.

13 продуктов Oracle, включая Oracle Financial Services Applications, Oracle MySQL, Oracle Retail Applications и Oracle Support Tools содержат ряд критических уязвимостей, самые опасные из которых получили оценку в 9,8 балла по шкале CVSS.

В общей сложности в семействе программного обеспечения Fusion Middleware исправлено 56 проблем, затрагивающих почти 20 связанных служб, включая Identity Manager Connector (версии 9.0), Big Data Discovery (версии 1.6) и WebCenter Portal (версии 11.1.1.9. 0, 12.2.1.3.0, 12.2.1.4.0). 49 уязвимостей могли быть использованы удаленно неавторизованным злоумышленником.

Обновление устраняет уязвимости в платформе Java Platform, Standard Edition (Java SE), используемой для разработки и развертывания Java-приложений. 15 проблем получили оценку в 8,5 балла по шкале CVSS и могли быть проэкслуатированны удаленно неавторизованным злоумышленником.

Также были исправлены 34 критические уязвимости в Oracle Financial Services Applications, 45 ошибок в Oracle MySQL, 9 в Oracle Server Database Server». ***(Oracle исправила 405 уязвимостей в своих продуктах // SecurityLab.ru (https://www.securitylab.ru/news/506611.php). 14.04.2020).***

***

«В сервисе VMware Directory Service (vmdir) обнаружена и исправлена опасная уязвимость (CVE-2020-3952), позволяющая злоумышленникам получить доступ к содержимому всей корпоративной виртуальной инфраструктуры.

VMware Directory Service является компонентом утилиты VMware vCenter Server, обеспечивающей централизованное управление виртуальными хостами и виртуальными машинами с одной консоли. Согласно описанию продукта, «один администратор может управлять сотнями приложений». Эти приложения управляются с помощью технологии единого входа (single sign-on, SSO).

VMware Directory Service является центральным компонентом vCenter SSO (наряду с сервером администрирования Security Token Service и сервисом vCenter Lookup Service). Кроме того, vmdir используется для управления сертификатами приложений, управляемых vCenter.

По системе оценивания опасности CVSS v.3 уязвимость CVE-2020-3952 получила максимальные 10 баллов. Проблема связана с плохой реализацией технологии управления доступом, позволяющей злоумышленнику обойти механизм аутентификации. Злоумышленник с сетевым доступом к уязвимой установке vmdir может извлечь конфиденциальную информацию, позволяющую взломать vCenter Server.

Уязвимость затрагивает установки vCenter Server 6.7 до версии 6.7u3f, если они были обновлены с предыдущих веток 6.0 или 6.5. Проблема не затрагивает «чистые» установки vCenter Server 6.7». ***(Уязвимость в VMware открывает хакерам доступ к корпоративной информации // SecurityLab.ru (https://www.securitylab.ru/news/506608.php). 13.04.2020).***

***

«Издание Bleeping Computer обратило внимание, что разработчики Microsoft выпустили строчные патчи для устранения уязвимости удаленного выполнения кода в библиотеке Autodesk FBX, которая интегрирована в Microsoft Office и Paint 3D.

В прошлом месяце разработчики Autodesk выпустили обновления для своего продукта Autodesk FBX SDK. Патчи устранили уязвимости удаленного выполнения кода, а также уязвимости, приводящие к отказу в обслуживании (DoS), которые можно было эксплуатировать при помощи специально созданных файлов FBX.

Так, специально созданный вредоносный файл FBX будет эксплуатировать переполнение буфера и хипа, разыменование нулевого указателя, а также проблемы type confusion, use-after-free и integer overflow, чтобы в итоге осуществить DoS-атаку или удаленное выполнение произвольного кода.

Но дело в том, что библиотека Autodesk FBX интегрирована в Microsoft Office 2016, Microsoft 2019, Office 365 и Paint 3D. И в связи с этим разработчикам Microsoft пришлось выпустить внеочередные патчи для свих продуктов, исправляя найденные в Autodesk FBX баги.

В опубликованном бюллетене безопасности специалисты компании разъясняют, что открытие вредоносных файлов FBX в приложениях Office может привести к удаленному выполнению кода. Пользователей простят установить обновления как можно быстрее». ***(Мария Нефёдова. Microsoft выпустила внеочередной патч для опасной уязвимости в Microsoft Office // Xakep (https://xakep.ru/2020/04/22/autodesk-fbx-rce/). 22.04.2020).***

***

«Специалисты из компании ESET обнаружили критические уязвимости в трех разных контроллерах «умного» дома — Fibaro Home Center Lite, eQ-3 Homematic Central Control Unit (CCU2) и ElkoEP eLAN-RF-003. Эксплуатация проблем позволяет злоумышленнику удаленно выполнить код, похитить данные и осуществить MitM-атаки.

Home Center Lite представляет собой компактный контроллер для управления «умными» устройствами, Homematic CCU2 предназначен для управления функциями программирования и логики в устройствах Homematic, а eLAN-RF-003

является «умным» коммуникатором для управления сетями через мобильные устройства.

В ходе анализа версии прошивки Fibaro Home Center (HC) Lite 4.170 были обнаружены проблемы, связанные с отсутствующей проверкой сертификата в TLS-соединениях, эксплуатация которых позволяет осуществлять MitM-атаки и внедрять команды. Также с помощью брутфорса преступник может узнать встроенный пароль прошивки, создать SSH-бэкдор и получить права суперпользователя для перехвата контроля над устройством. Доступ к встроенному модификатору входа хэш-функции (соль) можно было получить через web-интерфейс Fibaro.

Анализ версии прошивки контроллера Homematic CCU2 3 2.31.25 выявил уязвимость удаленного выполнения кода в CGI-скрипте контроллера. Версии прошивки устройства ELAN-RF-003 2.9.079 содержала проблемы, связанные с отсутствием реализации SSL-шифрования, некорректными проверками подлинности, которые позволяли выполнять команды без авторизации, и отсутствием cookie-файлов.

Специалисты сообщили о своих находках Elko и eQ-3 в феврале и марте 2018 года, однако рассказали о данных проблемах только сейчас. Elko исправила в мае 2018 года проблемы в версии прошивки 3.0.038, но отсутствие шифрования связи через web-интерфейс осталось до сих пор. EQ-3 исправила уязвимость удаленного выполнения кода в июле, а Fibaro устранила в августе все уязвимости, кроме встроенной соли, которая по-прежнему используется для создания хешей паролей». ***(Уязвимости в «умных» хабах подвергают дома риску удаленных атак // SecurityLab (https://www.securitylab.ru/news/507674.php).***

***

«Главный исследователь Agile Information Security и известный багхантер, регулярно участвующий в таких хакерских состязаниях, как Pwn2Own, Педро Рибейро опубликовал на GitHub детали четырех уязвимостей нулевого дня, касающихся корпоративного инструмента безопасности IBM Data Risk Manager (IDRM).

Сама компания IBM описывает этот продукт, как «центр управления рисками утечки данных, который позволяет руководителям и любым другим сотрудникам без специальной подготовки выявить, проанализировать и визуализировать риски утечки данных, а также предпринять необходимые действия для защиты бизнеса».

Рибейро подчеркивает, что IDRM — это корпоративный инструмент, который имеет дело с крайне конфиденциальной информацией. То есть компрометация такого продукта может привести к полной компрометации всей компании, поскольку у IDRM есть учетные данные для доступа к другим инструментам безопасности, не говоря о том, что IDRM содержит информацию о критических уязвимостях.

Рибейро пишет, что обнаружил четыре ошибки в IDRM и активно сотрудничал со специалистами CERT/CC, стремясь донести информацию о багах до инженеров IBM через официальную программу раскрытия уязвимостей. Однако,

невзирая на всю серьезность обнаруженных ошибок, IBM отказалась принимать отчет специалиста, прислав странный ответ:

«Мы оценили этот отчет и закрываем его как выходящий за рамки нашей программы раскрытия уязвимостей, поскольку данный продукт предназначен только для «расширенной» поддержки, оплачиваемой нашими клиентами. Это указано в правилах https://hackerone.com/ibm. Чтобы получить право участвовать в этой программе, вы не должны быть связаны контрактом на выполнение тестирования безопасности для корпорации IBM, ее дочерних компаний или клиентов IBM на протяжении шести месяцев до подачи отчета».

Рибейро признается, что до сих пор не понял, что означает этот ответ. Исследователь задается множеством вопросов: почему IBM отказалась принять его бесплатный отчет об уязвимостях, составленный по всем правилам? Означает ли это, что в данном случае компания принимает отчеты только от своих клиентов? Или, быть может, этот продукт не поддерживается? Но в таком случае, почему его все еще продают новым клиентам, и почему компания ведет себя столь безответственно?

«Это просто невероятный ответ от IBM, многомиллиардной компании, которая продает корпоративные продукты безопасности и консультирует по вопросам безопасности огромные корпорации по всему миру», — пишет Рибейро.

Так и не добившись ответа и реакции от IBM, исследователь опубликовал информацию о проблемах в открытом доступе, чтобы компании, использующие IDRM, могли принять меры для предотвращения атак. Все найденные экспертом уязвимости могут использоваться удаленно и заключаются в следующем:

- обход механизма аутентификации IDRM;
- возможность инъекций команд в одном из API IDRM, что позволяет атакующим запускать собственные команды в приложении;
- жестко закодированные учетные данные: a3user/idrm;
- уязвимость в API IDRM, которая позволяет удаленным злоумышленникам скачивать любые файлы.

Помимо детального описания проблем были опубликованы и два модуля Metasploit, которые эксплуатируют обход аутентификации и обеспечивают удаленное выполнение кода, а также загрузку произвольных файлов.

Лишь после того как информация о четырех 0-day вчера попала на страницы СМИ, представители IBM наконец обратили внимание на Рибейро и найденные им проблемы. В компании сообщили, что произошла ошибка: исследователь не должен был получить столь странный ответ, а обнаруженные им уязвимости не должны были остаться без внимания.

Теперь компания сообщает, что уязвимость, связанная с инъекциями команд, угрожавшая IBM Data Risk Manager версий 2.0.1, 2.0.2 и 2.0.3, была устранена в версии 2.0.4. Также эта версия решила проблему загрузки произвольных файлов, представлявшую угрозу для версий 2.0.2 и 2.0.3.

Жестко закодированные учетные данные, активные «из коробки», по-прежнему присутствуют в IDRM, но компания напоминает, что их нужно сбросить и сменить при первой установке, согласно руководству.

Также сообщается, что инженеры компании изучают проблему, связанную с обходом аутентификации в IDRM. Специалисты обещают выпустить патчи и обновить рекомендации по снижению рисков в самом скором времени.

Рибейро прокомментировал запоздалую реакцию компании журналистам издания The Register:

«Весьма грустно, что мне приходится публично раскрывать информацию о 0-day и публично стыдить их, чтобы заставить исправить критические уязвимости, тогда как они рекламируют себя как элитную компанию, предоставляющую услуги безопасности.

Как я уже писал в своем отчете, я лишь хотел сообщить им [о проблемах] и не просил взамен ничего, кроме упоминания об устранении уязвимости. И к слову об этом: я считаю весьма печальным и тот факт, что IBM, компания с многомиллиардным доходом, не способна наскрести несколько долларов, чтобы платить ИБ-исследователям, хотя она представлена на HackerOne».

Последний упрек эксперта связан с тем, что программа вознаграждения за уязвимости IBM не подразумевает никаких денежных вознаграждений, лишь почет и благодарность». ***(Мария Нефёдова. Раскрыты детали четырех 0-day уязвимостей в IBM Data Risk Manager // Xakep (https://xakep.ru/2020/04/22/ibm-0days/). 22.04.2020).***

***

«Киберпреступники атакуют больницы и правительственные учреждения в США с помощью вымогательского ПО, используя учетные данные Active Directory, похищенные путем эксплуатации критической уязвимости в VPN-серверах Pulse Secure.

Уязвимость CVE-2019-11510, позволяющая удаленно выполнить код, была исправлена Pulse Secure в августе прошлого года. Первые попытки ее эксплуатации зафиксировал исследователь безопасности Кевин Бомон (Kevin Beaumont) 22 августа 2019 года. Кроме того, в прошлом году уязвимость активно эксплуатировалась киберпреступными группировками, финансируемыми иранским правительством. Тем не менее, несмотря на это, многие установки Pulse Secure до сих пор остаются уязвимыми.

На прошлой неделе Агентство по кибербезопасности и защите инфраструктуры США (Cybersecurity and Infrastructure Security Agency, CISA) в очередной раз призвало организации как можно скорее обновить уязвимые версии Pulse Secure с целью предотвратить возможное проникновение злоумышленников в их сети и хищение учетных данных администратора домена.

Согласно уведомлению CISA, заполучив учетные данные, злоумышленники проникают в сетевую среду организации через уязвимые установки Pulse Secure VPN. В целях избежать обнаружения при подключении к VPN-серверу жертвы киберпреступники используют прокси, в частности инфраструктуру Tor и виртуальные выделенные серверы (VPS).

Одна из обнаруженных CISA киберпреступных группировок после похищения учетных данных через уязвимую установку Pulse Secure VPN смогла заразить вымогательским ПО сети нескольких больниц и госучреждений в США и

зашифровать хранящуюся в них информацию. Тем не менее, в 30 случаях попытки проникновения в сетевую среду оказались безуспешными, после чего группировка выставила похищенные учетные данные Active Directory на продажу.

Уязвимость CVE-2019-11510 позволяет удаленному неавторизованному атакующему скомпрометировать VPN-серверы, получить доступ к незашифрованным учетным данным всех активных пользователей и выполнить произвольные команды, если пользователи не сменили свои пароли.

Установившие обновление организации по-прежнему могут оставаться уязвимыми, если патч был применен уже после того, как злоумышленники проникли в сети. В связи с этим CISA выпустило утилиту с открытым исходным кодом check-your-pulse, позволяющую организациям находить индикаторы взлома и решать, нужно ли сбрасывать пароли Active Directory». ***(Хакеры заражают больницы вымогательским ПО с помощью учетных данных AD // SecurityLab (https://www.securitylab.ru/news/506831.php). 20.04.2020).***

***

«З'ясувалося, що в iOS вже 8 років є серйозний пролом, скористатися яким можна через додаток «Пошта». Про це заявила американська фірма ZecOps, що працює у сфері кібербезпеки. У доповіді фахівців також говориться, що невідоме угруповання хакерів використовувало уразливість в особистих цілях. Під загрозою потенційно опинилися всі пристрої з iOS 6 і вище.

Хакери розсилали своїм жертвам листи, які запускали шкідливий код через стандартний поштовий додаток iOS. Що цікаво, користувачам навіть не потрібно було відкривати шкідливе повідомлення, бо «Пошта» працює в фоні. Це дозволило зловмисникам отримати повний контроль над пристроями. На даний момент вже відомо про шість випадків використання уразливості по всьому світу: від Північної Америки до Саудівської Аравії. Apple відмовилася коментувати ситуацію, але закрила пролом в свіжій бета-версії iOS 13.4.5.

Втім, користувачі стабільних збірок системи, яких більшість, все ще залишаються під загрозою. Єдиним варіантом захиститися від хакерської атаки до виходу патча є використання сторонніх поштових клієнтів». ***(Уразливість «Пошти» від Apple ставить під загрозу всі пристрої на iOS // ВСВІТІ (http://vsviti.com.ua/news/113898). 23.04.2020).***

***

«Вразливість у програмі Microsoft Teams, яка використовується для проведення відеоконференцій, дозволяла зламати її за допомогою одного GIF-зображення. …під загрозою була не тільки конкретний обліковий запис, зловмисники могли взяти під контроль "весь список облікових записів команд".

Наголошується, що уразливість зачіпала всі версії програми для ПК і веб-браузерів. Проблема полягала в тому, як Microsoft обробляє токени аутентифікації для перегляду зображень у командах — спеціальні файли, які підтверджують, що "законний" користувач отримує доступ до облікового запису команди. Ці токени обробляються Microsoft на її сервері, розташованому за адресою teams.microsoft.com, або на будь-якому піддомені за цією адресою. Фахівці

компанії CyberArk виявили, що існувала можливість захопити два з цих піддоменів — aadsync-test.teams.microsoft.com і data-dev.teams.microsoft.com.

Експерти з'ясували, що якщо хакери можуть змусити користувача відвідати захоплені піддомени, то токени будуть передані на сервер зловмисників. Простим способом змусити користувача відвідати скомпрометовані піддомени була класична фишинговая атака, коли зловмисники надсилають посилання і змушують клацнути по ній.

Але фахівці з CyberArk пішли іншим шляхом і створили GIF-зображення з Дональдом Даком, що при простому перегляді змусило б обліковий запис команди жертви відмовитися від свого сертифіката аутентифікації і, отже, власних даних. Це відбувалося тому, що джерелом GIF був скомпрометований піддомен, і додаток автоматично зв'язувався з ним для попереднього перегляду зображення. За словами фахівців з кібербезпеки, хакери могли використовувати уразливість, створивши черв'яка і поширивши атаку від одного користувача до іншого, формуючи масове "зараження".

Компанія Microsoft виправила вразливість 20 квітня. Як довго існувала помилка у програмі, невідомо…» ***(Експерти з кібербезпеки знайшли спосіб зламати аналог Zoom від Microsoft за допомогою "гіфки" // Зеркало недели. Украина (https://dt.ua/TECHNOLOGIES/eksperti-z-kiberbezpeki-znayshli-sposib-zlamati-analog-zoom-vid-microsoft-za-dopomogoyu-gifki-346069_.html). 28.04.2020).***

***

«Исследователи из компании Pen Test Partners обнаружили на посвященном защите информации сайте GDPR.eu уязвимость, позволявшую любому пользователю Сети извлечь логин и пароль для базы данных MySQL.

Ресурс GDPR.eu представляет собой консультативный сайт для организаций, которым необходимы советы по соблюдению требований «Общего регламента защиты данных» (The General Data Protection Regulation, GDPR). Сайтом GDPR.eu управляет швейцарская корпорация Proton Technologies AG, владеющая защищенной почтовой службой ProtonMail.

Проблема была связана с тем, что папка .git на сайте была доступна для чтения любому пользователю в интернете. Это достаточно распространенная проблема, возникающая из-за отсутствия правильной конфигурации. Многие web-разработчики используют инструмент разработки Git с открытым исходным кодом для создания страниц для отслеживания всех изменений, внесенных в файлы проекта. Папка .git может содержать исходный код, ключи доступа к серверу, пароли базы данных, размещенные файлы, встроенный модификатор входа хэш-функции (соль) и пр.

В репозитории сайта GDPR.eu находилась копия wp-config.php, ключевого файла, содержащего информацию, нужную для работы сайтов на WordPress. В данном файле в том числе содержались настройки управления базой данных MySQL (имя, локальный хост, логин и пароль). Злоумышленник с доступом к данному файлу мог переписать содержимое сайта или вовсе удалить его.

Специалисты проинформировали Proton Technologies о своих находках, и компания вскоре исправила уязвимость. По словам представителей компании, сайт

размещается на независимой сторонней инфраструктуре, не содержит никаких пользовательских данных, а информация в папке git не могла привести к дефейсу gdpr.eu, поскольку доступ к базе данных ограничен». ***(Посвященный защите информации сайт допустил утечку данных // SecurityLab.ru (https://www.securitylab.ru/news/507981.php). 29.04.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания RevBits представила новый набор инструментов Cybersecurity Suite, обеспечивающий защиту от кибератак.

Как отмечается, RevBits Platform была создана с одной целью - "предоставить комплексное технологическое решение, позволяющее выявлять, противодействовать и защищаться от инцидентов в сфере кибербезопасности, способных наносить вред правам интеллектуальной собственности наших клиентов".

"По мере роста уровня угроз в киберпространстве с тревожным увеличением числа компаний, сообщающих о случаях взлома и хакерских атак, стало совершенно очевидно, что основное большинство имеющихся на рынке решений не справляются с задачей обеспечения адекватной защиты, - прокомментировал генеральный директор Дэвид Шиффер (David Schiffer). - Наш новый пакет поможет значительно снизить риски и потери наших клиентов, одновременно гарантировав им улучшенную защиту и важную предоставив важную аналитическую информацию об их сетях".

В пакет RevBits Cybersecurity Suite входят следующие модули:

RevBits Email Security

RevBits Endpoint Security

RevBits Deception Technology

RevBits Privileged Access, Password, Key and Certificate Management…» ***(RevBits представила Cybersecurity Suite // Компьютерное Обозрение (https://ko.com.ua/revbits_predstavila_cybersecurity_suite_132487). 02.04.2020).***

***

«Компания NWU, дистрибьютор решений Netscout Systems в Украине, сообщила о новой инициативе этого поставщика средств обеспечения качества сервисов, безопасности и бизнес-аналитики.

Netscout Systems объявила о запуске Cyber Threat Horizon -бесплатного портала аналитики угроз, который предоставит наилучшую видимость атак DDoS в реальном времени.

Cyber Threat Horizon собирает данные о прошлых и возникающих угрозах DDoS, анализирует их, назначает для каждой уровень опасности и распространяет эту информацию в удобном визуальном представлении, демонстрирующем: тип

атаки, страну происхождения и страну назначения, масштабы атаки, её продолжительность и целевой сектор индустрии.

В своей работе портал опирается на систему активного анализа уровня угроз Arbor ATLAS, которая отслеживает примерно треть глобального интернет-трафика. Сведения в Cyber Threat Horizon поступают из множества различных источников, включая данные от глобальной инсталлированной базы продуктов Arbor Smart DDoS Protection , трафик ботнетов и Тёмный Веб. Отмечается, что используются только анонимизированные данные.

DDoS-атаки представляют собой серьезную угрозу доступности инфраструктуры и сервисов, обеспечивающих работу из дому для миллионов людей в условиях вспышки пандемии COVID-19. С Cyber Threat Horizon организации приобретают ситуационную готовность к DDoS-атакам – способность обеспечить защиту до того, как будет затронут столь важный сейчас удаленный доступ.

После бесплатной регистрации на портале, пользователь получает доступ к историческим данным вплоть до 2003 года. Кроме того, регистрация даёт возможность настраивать представление информации, используя разнообразные контекстные фильтры, и создавать отчёты по регионам, отраслевым вертикалям и интервалам времени, помогающие понять, как атаки DDoS могут повредить конкретным сетям.» ***(Новый бесплатный портал Netscout визуализирует ландшафт DDoS-угроз // Компьютерное Обозрение (https://ko.com.ua/novyj_besplatnyj_portal_vizualiziruet_landshaft_ddos-ugroz_132510). 06.04.2020).***

***

«Amazon Web Services сообщила, что анонсированный в декабре на конференции re:Invent сервис безопасности Amazon Detective становится общедоступным. До этого он три месяца функционировал в ознакомительном режиме.

Amazon Detective использует искусственный интеллект, статистический анализ и теорию графов для повышения эффективности работы систем оповещения о прорывах защиты. Он предоставляет детальную информацию о масштабах и серьёзности проблем и помогает клиентам реконструировать методы и цели хакерских атак. Это, в свою очередь, позволяет клиентам ускорить расследование и избавляет их от необходимости собирать журналы различных источников данных.

«Детективный» сервис может анализировать триллионы событий на основе таких данных, как трафик IP, журналы VPC Flow Logs, а также служб AWS CloudTrail и GuardDuty. В итоге он генерирует постоянно обновляемое интерактивное визуальное представление ресурсов, пользователей и их взаимодействий. Такой подход даёт возможность точно идентифицировать выявленную вредоносную активность и выработать наилучшие меры противодействия.

Стоимость пользования новым сервисом, по информации Amazon, зависит от количества данным, получаемых от AWS CloudTrail, VPC Flow Logs и AWS GuardDuty. Максимально, Detective способен использовать сводные данные,

которые охватывают период в 12 месяцев. На данный момент, Detective доступен в регионах Amazon US East (Северная Виргиния), US East (Огайо), US West (Орегон), Europe (Франкфурт), Europe (Ирландия), Europe (Лондон), Europe (Париж), Europe (Стокгольм), Asia Pacific (Мумбаи), Asia Pacific (Сеул), Asia Pacific (Сингапур), Asia Pacific (Сидней), Asia Pacific (Токио), и South America (Сан-Паулу). В дальнейшем географический охват сервиса будет расширяться». ***(Служба AWS по расследованию инцидентов безопасности стала общедоступной // Компьютерное Обозрение (https://ko.com.ua/sluzhba_aws_po_rassledovaniyu_incidentov_bezopasnosti_stala_obshhedostupnoj_132489). 03.04.2020).***

***

«Разработчики Google адаптируют машинное обучение для борьбы с мошенниками, киберпреступниками и правительственными хакерами, которые активно используют тему пандемии коронавируса для фишинговых атак.

Компания сообщила, что только на прошлой неделе заблокировала более 18 000 000 фишинговых писем, связанных с COVID-19 и нацеленных на пользователей Gmail. Такой «коронавирусный» фишинг составляет примерно 2,5% от 100 000 000 фишинговых писем, которые Google блокирует ежедневно. Также разработчики сообщают о блокировании 240 000 000 ежедневных спам-сообщений, связанных с COVID-19.

Такой всплеск фишинговой активность на тему коронавируса побудил специалистов Microsoft и Google скорректировать стратегии по защите клиентов. Дело в том, что общее число фишинговых атак не увеличилось, просто злоумышленники следуют за трендами и настраивают свои сообщения в соответствии с обстановкой в мире.

«Мы внедрили упреждающий мониторинг для вредоносных программ, связанных с COVID-19, и фишинга в наших системах и рабочих процессах. Во многих случаях эти угрозы не новы, но представляют собой известные вредоносные кампании, которые обновили, чтобы эксплуатировать повышенное внимание к теме COVID-19», — пишут разработчики Google.

К примеру, Google будет обнаруживать фишинговые письма, в которых злоумышленники выдают себя за Всемирную организацию здравоохранения (ВОЗ), чтобы обманом заставить людей пожертвовать средства или распространять малварь.

Похожую тактику стали применять и инженеры Microsoft, которые тоже заметили, что старые и известные компании «перепрофилировались» и теперь эксплуатируют тему пандемии. «Мы наблюдаем смену приманок, но не всплеск новые атак», — пишет корпоративный вице-президент Microsoft 365 Security. Компания сообщает, что хотя SmartScreen ежедневно обнаруживает и обрабатывает более 18 000 вредоносных URL-адресов и IP-адресов, связанных с COVID-19, они составляют менее 2% от общего объема угроз…». ***(Мария Нефёдова. За неделю Gmail блокировал 18 млн фишинговых писем о COVID-19 // Xakep (https://xakep.ru/2020/04/17/covid-spam/). 17.04.2020).***

***

«Предприятия не могут (и не должны) следить за каждой из тысяч уязвимостей, ежегодно обнаруживаемых в ПО. Электроэнергетической компании вряд ли стоит беспокоиться об уязвимостях в браузерах, а бухгалтерской конторе незачем опасаться уязвимостей в АСУ ТП. Однако многие предприятия испытывают трудности с оценкой возможного влияния на них той или иной уязвимости. Новый проект компании Rapid7 призван решить эту проблему.

В среду, 15 апреля, компания представила платформу Attacker Knowledge Base (AttackerKB), позволяющую специалистам в области кибербезопасности проводить оценку возможного влияния уязвимостей на их предприятия. С помощью платформы безопасники могут узнавать, что дает злоумышленнику эксплуатация уязвимости, насколько сложно ее проэксплуатировать и какой уровень доступа к корпоративным сетям она предоставляет.

Данные об уязвимостях в AttackerKB будет вносить само ИБ-сообщество. То есть, платформа станет своего рода «Yelp для уязвимостей» (Yelp – популярный сервис для поиска услуг на местном рынке, например ресторанов или парикмахерских, с возможностью добавлять и просматривать их рейтинги и обзоры).

Для того чтобы опубликовать в AttackerKB анализ уязвимости, можно авторизоваться через GitHub, а открытый API позволяет пользователям экспериментировать с данными.

Проект базируется на системе оценивания уязвимостей Common Vulnerability Scoring System (CVSS).

«Хотя CVSS помогает в приоритизации уязвимостей, с ее помощью невозможно уточнять и контекстуализировать модели рисков индивидуально для каждой компании и каждого специалиста. При объяснении потенциального риска человеку более понятен не отраслевой стандарт, а рассказ тестировщика безопасности об эксплуатации связки из двух уязвимостей с низкими баллами CVSS для получения привилегированного доступа к критическим активам компании. В AttackerKB мы не стремимся к консенсусу, а хотим подчеркнуть ценность индивидуального опыта», – пояснила директор по разработке ПО Rapid7 Кэйтлин Кондон (Caitlin Condon)». ***(Новая платформа поможет предприятиям приоритизировать угрозы // SecurityLab (https://www.securitylab.ru/news/506748.php). 16.04.2020).***

***

«Компания Zyxel Networks совместно с компанией McAfee выпустила интегрированное универсальное решение для защиты сетей, специально разработанное для малого и среднего бизнеса.

Согласно исследованию 2019 Verizon Data Breach Investigations Report, сегодня более 40% кибератак нацелены на компании малого бизнеса, поэтому небольшим компаниям требуются мощное, простое в развертывании и управлении решение информационной безопасности, соответствующее масштабу их сетей. Интеграция решения McAfee для защиты от вирусов в семейство межсетевых

экранов старшего класса ATP предоставляет СМБ универсальный межсетевой экран с лучшими в своем классе технологиями обнаружения вредоносного кода, производительностью и расширенными функциями сканирования веб-контента.

«Потребности небольших компаний в эффективной киберзащите постоянно растут. Компания McAfee обеспечивает защиту сетей СМБ и позволяет сосредоточиться на ведении бизнеса. Отрадно, что благодаря партнерскому соглашению с Zyxel мы поможем их клиентам лучше защитить свои конфиденциальные данные», - заявил глобальный руководитель направления Enterprise Product Strategy and Alliances компании McAfee Джавед Хасан.

Пополнение в семействе ATP: защищающем от атак «нулевого дня»

Также сегодня Zyxel также представила две новые модели межсетевых экранов: ATP100W и ATP700 из предназначенной для СМБ серии межсетевых экранов Advanced Threat Protection. В этих решениях «все-в-одном» интегрирована масштабируемая облачная «песочница» с несколькими дополнительными уровнями безопасностями, обеспечивающими обнаружение и блокировку известных и неизвестных угроз.

Начиная с версии прошивки ZLD 4.5, увидевшей свет в феврале 2020 года, межсетевые экраны ZyWALL ATP могут одновременно выполнять сканирование на наличие вредоносного кода в режимах как Express, так и Stream. В режиме Express используется постоянно расширяющаяся облачная база данных с искусственным интеллектом, которая обеспечивает уникальный уровень информированности об угрозах, а в режиме Stream с помощью базы сигнатур обеспечивается локальное гранулярное и углубленное сканирование. Новый гибридный режим сочетает преимущества обоих подходов к сканированию, максимально повышая безопасность за счет всеобъемлющего и углубленного сканирования. Это позволяет защищать сети от инсайдерских угроз и помогает бизнесу отразить быстро эволюционирующие кибератаки…». ***(Zyxel и McAfee защитят средний и малый бизнес от неизвестных киберугроз // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5660508-Zyxel-i-McAfee-zashhityat-srednij.html). 27.04.2020).***

***