CHECK POINT
RESEARCH

2018

ОТЧЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДОБРО ПОЖАЛОВАТЬ В БУДУЩЕЕ КИБЕРБЕЗОПАСНОСТИ

Check Point
SOFTWARE TECHNOLOGIES LTD

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

2017 год стал поворотным годом, удивившим многих в отрасли IT-безопасности. Мы становимся очевидцами перехода к пятому поколению кибератак — от широкого применения вымогательского ПО, бот-сетей «Интернета вещей», взломов данных и мобильных вредоносных программ к сложным многовекторным технологиям.

В контексте развития киберландшафта Всемирный экономический форум недавно назвал кибератаки одним из трех основных глобальных рисков на 2018 год. Действительно, сейчас мы можем наблюдать, как злоумышленники эффективно используют вымогательское ПО в качестве орудия нанесения ущерба крупным учреждениям, влияя на здоровье и жизнь населения целых стран, а также создавая проблемы в разных отраслях бизнеса.

В прошлом году в центре внимания были взломы данных, сопровождавшиеся шокирующими откровениями о компрометации данных клиентов. Более того, масштаб и частота таких атак, от Uber до Equifax, не показывают признаков их уменьшения.

Пробелы безопасности в мобильных устройствах, таких как Bluetooth, а также в магазинах мобильных приложений также означают, что многие варианты вредоносных программ продолжают свободно циркулировать. Фактически миллионы мобильных устройств по всему миру были заражены вредоносными приложениями, которые генерируют высокие доходы для тех, кто смог внедрить вредоносное ПО в магазины приложений.

Растущая популярность и стремительный рост стоимости криптовалюты, захлестнувшие мир, привели к значительному увеличению распространения криптомайнеров, которые быстро стали излюбленным вектором атак, приводящим к монетизации.

Утечка предполагаемых киберинструментов ЦРУ, созданная группами хактивистов, как было замечено, бросает длинную тень на глобальную экосистему информационной безопасности в целом. Стало больше доказательств того, что технологии, поддерживаемые государством, стоят за некоторыми из крупнейших глобальных кибератак – от предполагаемого взлома выборов до саботажа критической инфраструктуры.

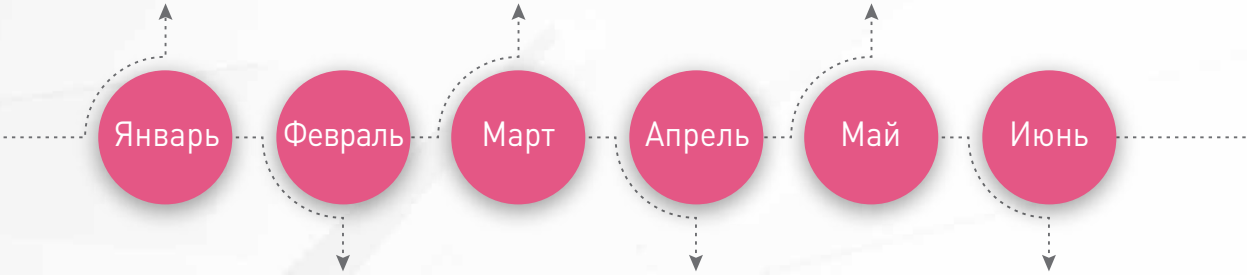
В этом отчете мы рассмотрим прошедший год и попытаемся проанализировать его события. Мы поймем, как ландшафт угроз в свете пятого поколения кибербезопасности теперь охватывает страны и отрасли по нескольким векторам сети, облаков и мобильных устройств и использует для этого технологии, спонсируемые государством. Анализируя недавние атаки, мы сможем понять, что 97% организаций не подготовлены к кибератакам. Затем мы более подробно рассмотрим, что может произойти в 2018 году и, самое главное, как лучше к этому подготовиться.

КАЛЕНДАРЬ ГЛАВНЫХ КИБЕРАТАК 2017 ГОДА

Принстонский университет оказался одной из 27 000 жертв, потерявших свои данные из-за уязвимости MongoDB.

Атаковано PoS решение Verifone, крупного производителя систем платежей дебетными и кредитными картами.

Попытка саботажа президентских выборов во Франции, когда у кандидата в президенты Эммануэля Макрона похитили 9ГБ конфиденциальной информации.



Утечка 2.5 миллиона учетных записей пользователей Xbox и PlayStation, включая имена, адреса эл. почты и персональные ID.

Взломано мобильное приложение New York Post и осуществлена массовоя рассылка оповещений о поддельных новостях.

Вслед за WannaCry в мае, Petya стал причиной массовых перебоев в работе FedEx, Maersk, WPP и многих других компаний по всему миру.

Мобильное вредоносное ПО CopyCat заразило свыше 14 млн. устройств Android по всему миру и за два месяца с помощью поддельных рекламных объявлений принесло злоумышленникам прибыль в 1.5 млн. долларов США.

EQUIFAX

У крупного кредитного агентства Equifax украдено 143 млн. записей о клиентах, включая номера социального страхования, данные кредитных карт и другую информацию.

UBER

57 млн. записей о водителях и клиентах Uber были похищены в результате захвата учетной записи AWS. Uber заплатил 100 000 долларов США для сокрытия взлома.

Июль Август Сентябрь Октябрь Ноябрь Декабрь

УКРПОШТА
ГОЛОВНА ПОШТА КРАЇНИ

Национальная почта Украины стала целью DDoS-атаки с целью нарушения ее работы в масштабе страны.

The National Lottery®

Массированная DDoS-атака вывела из строя Национальную лотерею Великобритании, не позволив миллионам приобрести ее билеты.

bitcoin

Платформа криптомайнинга NiceHash была скомпрометирована и потеряла 4700 биткоинов (70 млн. долларов США) в пользу хакеров.

ОСНОВНЫЕ КИБЕР-**ИНЦИДЕНТЫ 2017 ГОДА**

ШОКИРУЮЩИЕ ВЗЛОМЫ

ВЗЛОМ ДАННЫХ EQUIFAX

В сентябре 2017 одно из трех крупнейших кредитных агентств в США, Equifax, подверглось взлому, который затронул более 145 миллионов клиентов. Используя «дыру» в безопасности пакета программного обеспечения «Apache Struts», хакеры смогли украсть конфиденциальные данные, включая имена, адреса, даты рождения, номера кредитных карт, номера социального страхования и номера водительских удостоверений.

ВЗЛОМ ДАННЫХ UBER

Благодаря тому, что хакеры получили учетные данные для доступа к информации, хранящейся на учетной записи Uber в AWS, были похищены персональные данные 57 миллионов клиентов и водителей. Усугубило ситуацию то, что Uber решила скрыть нарушение, заплатив злоумышленникам 100 000 долларов за удаление конфиденциальных документов без их опубликования.

СИСТЕМА ЗДРАВООХРАНЕНИЯ UNC

Более 1300 пренатальных пациентов системы здравоохранения Университета Северной Каролины пострадали от серьезного взлома данных. Похищенная информация включала полные имена, адреса, расовую принадлежность, этнические группы, номера социального страхования и разнообразную медицинскую информацию пациентов.

Рост облачных вычислений объясняется их большей гибкостью, простотой интеграции и меньшими затратами.

Однако основные проблемы безопасности облачных сервисов заключаются в том, что они открыты вовне. Это означает, что к ним можно получить доступ из любого места и с любого устройства. Более того, они имеют неэффективную встроенную защиту по умолчанию.

Мы прилагаем все усилия, чтобы побудить наших клиентов не полагаться исключительно на их поставщиков услуг, а взаимодействовать с ними в рамках модели взаимной ответственности, чтобы защитить как свои данные, так и любые средства, используемые для доступа к ним.

Йоав Даниели, руководитель отдела управления продуктами, облачная безопасность

78%

КОМПАНИЙ СЧИТАЕТ, ЧТО БЕЗОПАСНОСТЬ IAAS И SAAS БУДЕТ ИХ ОСНОВНОЙ ПРОБЛЕМОЙ [1]

64%

ОРГАНИЗАЦИЙ ПОДВЕРГЛИСЬ ФИШИНГОВЫМ АТАКАМ В ПРОШЛОМ ГОДУ [2]

УРОВЕНЬ ГОСУДАРСТВА

УТЕЧКА «VAULT 7»

В апреле группа хактивистов WikiLeaks опубликовала сведения о наборе инструментов взлома, которые, как полагают, принадлежат ЦРУ. Утечка показала вероятный объем использования технологий государственного уровня в кибератаках пятого поколения. Необычайная коллекция хакерских инструментов дает ее обладателю все хакерские возможности ЦРУ. Считается, что этот арсенал вредоносных программ и десятки инструментов для атак «нулевого дня» были нацелены на широкий спектр продуктов американских и европейских компаний, включая iPhone от Apple, Android от Google, телевизоры Samsung и Microsoft Windows.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА США

Правительство США предупредило, что «Dragonfly», группа передовых постоянных угроз (APT), предположительно поддерживаемая государством, использовало сочетание тактик и методов, чтобы попытаться получить доступ к жизненно важным системам управления технологическими процессами (СУ ТП) в энергетических компаниях США и других критических инфраструктурных организациях через сети их поставщиков и доверенных третьих сторон.

УРОВНИ АТАК В EMEA

Исследование Check Point показало, что атаки в режиме реального времени в регионе EMEA увеличились в два раза, с 28% в 2016 году до 48% в 2017 году из-за высокотехнологичного вредоносного ПО, которое теперь используется хакерами низкого уровня. Почти 20% организаций пострадали от вредоносного ПО Fireball, заразив более 250 миллионов компьютеров по всему миру. Кроме того, злоумышленники смогли создать хаос, вызванный WannaCry, путем использования высокотехнологичных инструментов и методов атаки, разработанных при содействии государства.

Хактивисты и киберпреступники теперь используют вредоносное ПО уровня государства, обладающее разрушительным эффектом.

Во многих случаях общим элементом является использование человеческого фактора в организациях государственного сектора.

При таких больших ставках, какими являются геополитика, не говоря уже о жизни людей, это область кибербезопасности требует серьезного отношения во всех правительственных учреждениях по всему миру.

Ричард Клейтон,
руководитель исследований APT

ИЗОЩРЕННЫЕ КРАЖИ КРИПТОВАЛЮТЫ

ВЗЛОМ YOUBIT

С кражей биткоинов на 120 млн. долларов США у Youbit, относительно неизвестной южнокорейской криптовалютной биржи, киберпреступники заявили о своем новом крупном криминальном увлечении. Вместо выполнения тяжелой работы по майнингу ценного цифрового актива киберпреступники часто предпочитают украсть его у других. Из-за стремительного роста курса криптовалют в прошлом году у отдельных лиц и бирж были украдены миллиарды долларов.

МОШЕННИЧЕСТВО CONFIDO

Стартап Confido на платформе Ethereum обманул тысячи участников рынка, а затем исчез из Интернета после того, как собрал 374 000 долларов США от инвесторов при первичном размещении криптовалюты (ICO). В то время как многие криптовалюты все еще пытаются найти для себя полезное приложение в реальном мире, Ethereum стала любимцем среди финансистов, потому что ICO позволяют стартапам привлекать огромные инвестиции в ходе молниеносных кампаний по привлечению финансирования.

КРАЖА ETHEREUM

Хакер сорвал второй по величине куш в истории кражи цифровых валют, используя критическую уязвимость в кошельке с несколькими подписями Parity в сети Ethereum, опустошив за считанные минуты три крупных кошелька Ethereum стоимостью более 31 000 000 долларов США. Нападавший мог бы украсть гораздо больше, если бы не быстрое действие «белых» хакеров, которые быстро организовали его блокировку.

59%

КОМПАНИЙ СЧИТАЕТ ВЫМОГАТЕЛЬСКОЕ ПО НАИБОЛЬШЕЙ УГРОЗОЙ[4]

Из-за своей анонимности киберпреступники были одними из первых пользователей криптовалют. Но если рыночная капитализация Bitcoin выросла с 1 миллиарда до 500 миллиардов долларов всего за год (ко времени публикации отчета), другим людям трудно не заметить бум электронных валют.

Преступникам больше не требуется пытаться совершить крупные банковские кражи. Вместо этого они сосредоточили свои усилия на разработке новых и творческих способов, с помощью которых можно украсть уникальные цифровые кошельки. Это не только приносит выгоду злоумышленникам, но также отнимает ресурсы у тех, кто законно владеет этими ценными цифровыми активами, все более растущими в цене.

Стив Джонсон, руководитель отдела предотвращения усовершенствованных угроз

СТРАШНЫЕ УДАРЫ ВЫМОГАТЕЛЬСКОГО ПО

WANNACRY

Тысячи отмененных операций и визитов пациентов в Национальной службе здравоохранения Великобритании (NHS), а также массовые сбои в работе тысяч компаний и общественных организаций по всему мире включая Telefónica и Немецкие государственные железные дороги, были вызваны печально известной атакой вымогательского ПО WannaCry. Атака вынудила организации вернуться назад к ручным и бумажным методам работы, поскольку вредоносное ПО заблокировало компьютерные системы компаний и потребовало выкуп в биткоинах для расшифровки и получения доступа к их файлам.

NOTPETYA

Компания Reckitt Benckiser, производитель Nurofen и Durex, потеряла более чем 100 миллионов долларов из-за нарушения процессов производства и поставок, вызванного вымогательским ПО NotPetya, ставшим причиной крупномасштабного хаоса во всем мире. Хотя оно было в первую очередь нацелено на Украину, оно затронуло компании по всему миру, от датской логистической компании Maersk до американской службы доставки FedEx и британской рекламной фирмы WPP. После захвата зараженного компьютера вредоносное ПО требовало заплатить преступникам выкуп в биткоинах в размере 300 долларов.

BAD RABBIT

В октябре была развязана еще одна новая крупномасштабная атака с использованием вымогательского ПО против критически важных инфраструктурных компаний, а также организаций в сфере здравоохранения, финансов, дистрибуции и выпуска программного обеспечения. В основном нападение было сосредоточено на Украине, где были атакованы Киевский метрополитен, Одесский международный аэропорт, а также и министерства финансов и инфраструктуры. На этот раз исполнители заблокировали компьютеры своих жертв и потребовали за их расшифровку выкуп в биткоинах, эквивалентный 280 долларам США.

19,494

ВИЗИТОВ К ВРАЧУ БЫЛИ ОТМЕНЕНЫ ВСЛЕДСТВИЕ АТАКИ ВЫМОГАТЕЛЬСКОГО ПО WANNACRY[5]

Вымогательское ПО появилось в поле зрения кибербезопасности с конца 1980-х годов. По прошествии тридцати лет мы видим, что оно находится в центре внимания.

Если в 1980-х годах основной его целью была система здравоохранения, то теперь вымогательское ПО имеет отношение к каждому бизнесу и индивидууму.

Пока оно по-прежнему является чрезвычайно эффективным методом получения финансовой выгоды, а организации остаются необразованными в области поддержания своего «здоровья» в смысле кибербезопасности, мы не должны удивляться тому, что эти постоянно развивающиеся атаки продолжатся в предстоящие годы.

Тал Эйснер, руководитель отдела маркетинга продуктов предотвращения угроз

УЩЕРБ ОТ DDOS-АТАК

ШАНТАЖ КОРЕЙСКОГО БАНКА

В обмен на то, что онлайн-сервисы семи южнокорейских банков не будут нарушены, группа, назвавшая себя «Armada Collective», потребовала выплатить около 315 000 долларов США в биткоинах, угрожая атакой типа «распределенный отказ в обслуживании» (DDoS). Южнокорейские финансовые институты привыкли к тому, что они становятся объектами кибератак, сталкиваясь с аналогичными угрозами с 2011 года.

БРИТАНСКАЯ НАЦИОНАЛЬНАЯ ЛОТЕРЕЯ

Миллионы клиентов были разочарованы тем, что не смогли купить свои еженедельные лотерейные билеты, поскольку сайт британской национальной лотереи был выведен из строя с помощью крупномасштабной атаки DDoS. Более того, организация была за месяц предупреждена о проведении такой атаки, в случае, если выкуп в биткоинах не будет оплачен.

АТАКА НА DREAMHOST

В августе компания веб-хостинга DreamHost перенесла мощную атаку DDoS, которая вывела из строя большинство ее сервисов, серьезно нарушив хостинг, веб-почту и виртуальные частные серверы, а также ухудшив производительность электронной почты. Нападение, которое быстро исчерпало ресурсы систем компании, предположительно исходило от идеологически мотивированных хактивистов.

24%

КОМПАНИЙ ПОДВЕРГЛИСЬ DDOS-АТАКАМ ЗА ПРОШЕДШИЙ ГОД.

За прошедший год атаки DDoS поражали цели, начиная от крупных медиасайтов и заканчивая критической инфраструктурой. Поскольку исполнители этих атак часто остаются в тени, понять точные мотивы их запуска еще сложнее. Хотя в первую очередь такие причины могут варьироваться от происков конкурентов до политического хактивизма.

Наши исследования показывают, что в последние годы широко распространено вовлечение устройств «Интернета вещей» (IoT), с помощью которых были реализованы многие недавние атаки DDoS. Это происходит главным образом из-за того, что эти онлайн-устройства обладают слабой аутентификацией и поэтому уязвимы для вторжения и манипуляций со стороны злоумышленников.

Ярив Фишман, руководитель отдела управления продуктами, вертикальные решения безопасности

АГРЕССИВНОЕ МОБИЛЬНОЕ ВРЕДОНОСНОЕ ПО

COPYCAT И EXPENSIVEWALL

CopyCat, мобильная вредоносная программа, заразившая более 14 миллионов устройств по всему миру, позволила собрать миллионы долларов, используя поддельные приложения на устаревших устройствах. Эта кампания принесла хакерам всего за два месяца примерно 1,5 миллиона долларов в качестве дохода за поддельную рекламу. Кроме того, в Google Play Store был обнаружен новый вариант вредоносного ПО для ОС Android, получивший название ExpensiveWall, который регистрировал пользователей мобильных устройств в платных сервисах без их разрешения. Вредоносная программа была размещена в магазине приложений Google Play и заразило не менее чем 50 приложений. Зараженные приложения были загружены от 1 до 4,2 миллионов раз, прежде чем Google удалил их.

ГРУППА LAZARUS ИДЕТ В МОБИЛЬНУЮ СРЕДУ

Был обнаружен новый кластер образцов вредоносных программ, нацеленных на устройства Samsung и носителей корейского языка, в том числе найденных в библейских приложениях на корейском языке. Предполагается, что за атакой, конкретно нацеленной на население Южной Кореи, стоит группа Lazarus, поддерживаемая Северной Кореей.

ПРЕДУСТАНОВЛЕННОЕ МОБИЛЬНОЕ ВРЕДОНОСНОЕ ПО

Наша команда по поиску мобильных угроз обнаружила, что в прошлом году каждая организация подверглась заражению вредоносным ПО для мобильных устройств, причем 89% испытывали по меньшей мере одно нападение «человек посередине» в сети Wi-Fi. Кроме того, всего в двух компаниях из нашего опроса нашлось 36 устройств Android, содержащих вредоносное ПО, которое было предварительно установлено где-то в цепочке поставки. Некоторые из вредоносных программ даже имели доступ к системным привилегиям, то есть они не могли быть удалены пользователем, и устройства пришлось повторно перепрошивать.

Как отмечается в нашем Отчете по мобильным угрозам, каждая крупная компания в прошлом году испытала атаку мобильных вредоносных программ.

Наши исследования также показали, что даже самые надежные магазины приложений имеют уязвимости, которые эксплуатируются на регулярной основе, и в эти магазины постоянно выкладывают вредоносные приложения.

Пятое поколение киберландшафта дает преступникам более широкую поверхность атаки и, следовательно, больше возможностей воспользоваться ею. Кроме того, новые уязвимости, будь то через Bluetooth или Wi-Fi, означают, что как организации, так и потребители должны знать о рисках, которые создают мобильные устройства.

Джереми Кей, руководитель отдела мобильной безопасности

СВЫШЕ **300**

ПРИЛОЖЕНИЙ В GOOGLE PLAY STORE СОДЕРЖАЛИ ВРЕДОНОСНОЕ ПО, КОТОРОЕ БЫЛО ЗАГРУЖЕНО 106 МЛН. ПОЛЬЗОВАТЕЛЕЙ[7]

100%

ВСЕХ КОМПАНИЙ ПОДВЕРГЛИСЬ АТАКАМ МОБИЛЬНОГО ВРЕДОНОСНОГО ПО[8]

НАБОР В АРМИЮ БОТНЕТОВ

БОТНЕТ HAJIME

Как и печально известный ботнет Mirai, Hajime распространялся через незащищенные устройства, у которых был открыт порт Telnet и использовались пароли по умолчанию. Hajime достигла поразительного охвата в более 300 000 устройств, но его цель остается неизвестной. Хотя некоторые предполагают, что это операция по очистке «Интернета вещей» от ботнета Mirai, его можно легко использовать в злонамеренных целях.

BLUEBORNE

Был обнаружен новый вектор атаки, получивший название «BlueBorne», который работает с использованием восьми различных уязвимостей, влияющих на Android, iOS, IoT-устройства, Windows и Linux. Уязвимости BlueBorne являются «червеподобными», что означает, что они могут распространяться с одного устройства на другое без дополнительных команд от злоумышленника, создавая тем самым большие бот-сети. Этот вектор атаки не требует от пользователя никаких действий, никаких предварительных условий или ограничений, кроме активного Bluetooth.

IOTROOP BOTNET

Совершенно новый ботнет, получивший название IoTroop, распространился и захватил IoT-устройства в гораздо большем объеме и с большим потенциальным ущербом, чем ботнет Mirai 2016 года. IoTroop распространяется через дыры в безопасности в программном и аппаратном обеспечении IoT, и свидетельства показывают, что им были затронуты более миллиона организаций. Ботнет еще не начал свою атаку, но когда это случится, результаты потенциально могут быть катастрофическими.

1 из 5

ОРГАНИЗАЦИЙ ТРАТИТ ОТ ДВУХ НЕДЕЛЬ ДО ГОДА НА ПОЛНОЕ ВОССТАНОВЛЕНИЕ ОТ УГРОЗ[9]

ПОСЛЕДНИЕ ТЕНДЕНЦИИ В ЛАНДШАФТЕ КИБЕРБЕЗОПАСНОСТИ

ВРЕДОНОСНОЕ ПО ОСВАИВАЕТ КРИПТОВАЛЮТЫ

Разработчики вредоносных программ быстро осваивают новшества и имеют тенденцию следить за растущими тенденциями, чтобы достичь широкомасштабной и эффективной работы. Из-за такого резкого повышения стоимости в 2017 году криптовалюты стали той тенденцией, которой сейчас следуют злоумышленники.

На криптовалютной арене для киберпреступников существует несколько целей. Некоторые из них ориентированы на то, чтобы добывать криптовалюты путем кражи вычислительной мощности пользователей с помощью вредоносного ПО, известного как «криптомайнер». Мы видели, что оно доставляется через веб-браузеры, которые используют блокировщики рекламы, а также сайты загрузки Torrent.

Другой метод, используемый киберпреступниками, заключается в том, чтобы заявить о том, что они будут делиться любыми добытыми криптовалютами с пользователем. Фактически же их реальное намерение состоит в том, чтобы отображать незаконные объявления или вести другую злонамеренную деятельность.

Вместо того, чтобы тратить время и силы на майнинг криптовалюты, более сложные атаки проводятся с помощью более «традиционного» метода ограбления банка и направляются прямо на деньги, воруя их непосредственно из самих криптообменников. И если криптообменные системы слишком сложно взломать, всегда существует возможность незаконного получения учетных данных криптовалютного кошелька пользователя.

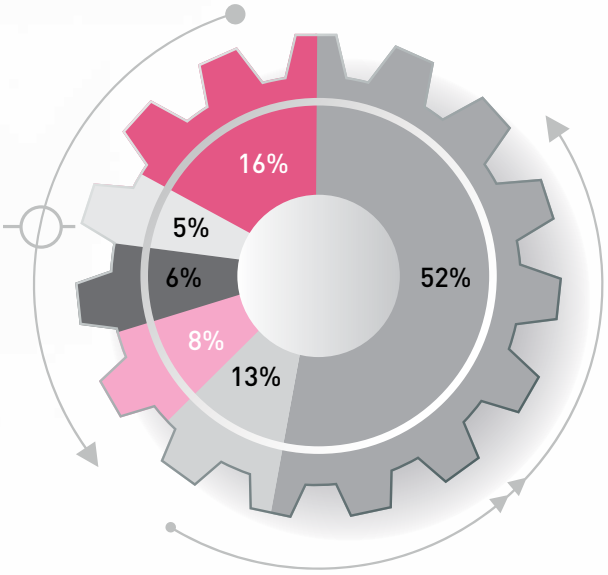


Рисунок 1: Наиболее популярное вредоносное ПО для криптомайнинга по относительному количеству атак. [10]

ВРЕДОНОСНОЕ ПО НАЦЕЛИВАЕТСЯ НА MAC OS

За последний год мы стали свидетелями увеличения количества атак, нацеленных на MacOS от Apple. Действительно, то, что когда-то было редким явлением, теперь превратилось в настоящую угрозу. К сожалению, разработчикам вредоносных программ удалось создать новые и творческие способы обойти защитные механизмы Apple и нацелить на пользователей Mac и iOS передовые вредоносные программы.

Однако растущее число вредоносных программ, разработанных для этой надежной операционной системы, имеет разные цели. Наиболее заметным является вредоносное ПО OSX/Dok, целью которого является перехват паролей пользователя и любой другой конфиденциальной информации путем контроля всех их сетевых соединений.

По иронии судьбы, то, что пользователи MacOS уверены в безопасности своей операционной системы, часто становится их слабым местом, когда они попадают под атаку. В отличие от других операционных систем, для MacOS существуют только ограниченные решения безопасности, и их использует еще меньшее количество пользователей. В результате, когда злоумышленнику удается обойти встроенные средства защиты, для него не остается никаких дополнительных преград.

Поскольку большое количество пользователей Mac — отличный стимул для хакеров, которые хотят расширить свою поверхность атаки, мы, скорее всего, продолжим в ближайшие годы наблюдать в отношении MacOS ту же тенденцию, которую мы видим в случае Windows. В свою очередь, это потребует от пользователей Mac обновить свою безопасность и использовать специальные технологии, способные предотвращать атаки «нулевого дня».

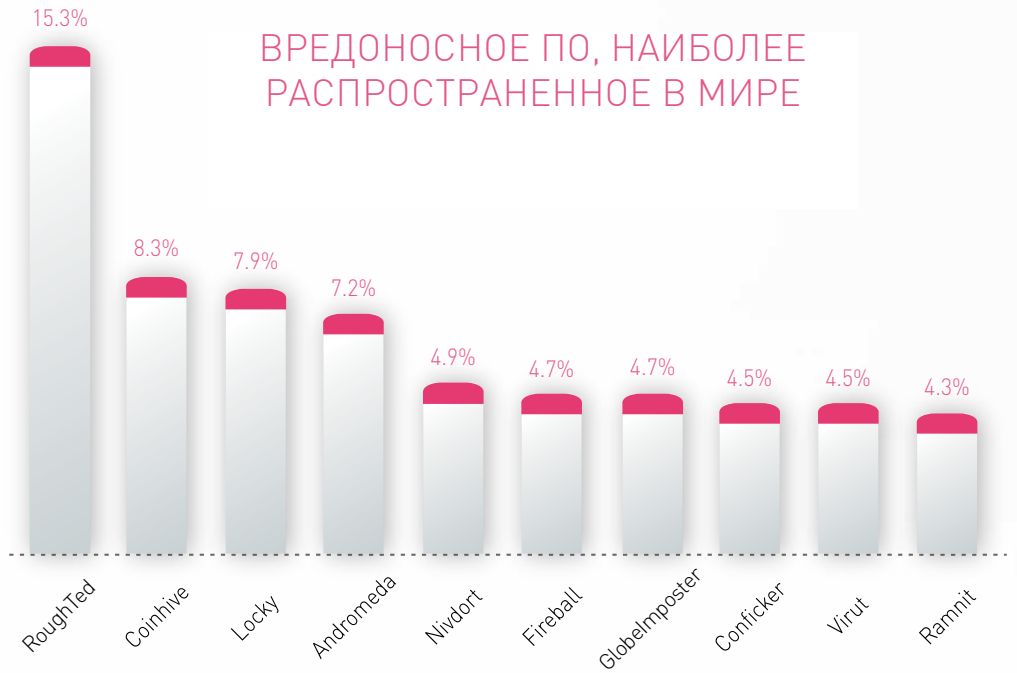


Рисунок 2: Наиболее распространенные в мире вредоносные программы: процент корпоративных сетей, подверженных каждому типу вредоносного ПО. [11]

МАССОВОЕ ВРЕДОНОСНОЕ ПО: РАСЦВЕТ ПРОМЫШЛЕННЫХ БОТНЕТОВ

Mirai, название печально известного ботнета 2016 года, вызвавшего хаос во всем мире, означает «будущее» на японском языке. В 2017 году, когда распространение ботнетов стало зловещим как по своим объемам, так и по целям, это «будущее» стало явью.

Кроме того, как в мире ПК, так и в мобильном мире, ботнеты стали обладать большими возможностями и стали более опасными, давая старт более крупным кампаниям, чем когда-либо прежде.

Прежде всего, в прошлом году мы обнаружили вредоносное ПО «Judy», рекламное ПО для автоматических кликов, которое оказавшись на уровне до 18,5 миллионов загрузок вполне может стать крупнейшей в мире мобильной вредоносной программой в Google Play.

Основная черта, общая для ботнетов, заключается в том, что все они ориентированы на создание критической массы для достижения своей цели. Будь то DDoS, криптомайнинг или массовая реклама, ключом является заражение как можно большего количества устройств, что делает практически невозможным противодействие атаке обычными средствами. Вместо этого требуется применять проактивные меры, используя более высокий уровень обнаружения и предотвращения вредоносного ПО.

РАЗРАБОТЧИКИ ВРЕДОНОСНОГО ПО УЧАТСЯ НА ЛУЧШИХ ОБРАЗЦАХ

Поскольку кибербезопасность часто является игрой «кошки-мышки», следующее поколение создателей вредоносных программ начинает использовать самые современные тактики, чтобы обойти меры безопасности и оставаться впереди преследователей. Они все чаще достигают этого, учась у самих «кошек» (служб безопасности).

Хорошим примером этого является атака вымогательского ПО WannaCry в мае 2017 года, которая использовала уязвимость «EternalBlue». В этом случае, как и во многих других, успех был достигнут за счет эксплуатации запоздалых патчей безопасности или отсутствия применения таких патчей. Первоначально обнаруженная АНБ США (NSA) атака использовала уязвимость для проникновения в сети и распространения внутри них. Организации, которые не смогли обновить свои системы безопасности, закончили тем, что заплатили за это высокую цену.

Аналогичное открытие было сделано и в случае утечки Vault 7, которая показала, что некоторые части кода, используемого ЦРУ для взлома мобильных устройств, были заимствованы из обычных вредоносных программ. Ключевым выводом для предприятий и пользователей здесь является то, что все киберугрозы связаны друг с другом, независимо от того, откуда они берут свое начало, и это следует учитывать при защите компьютерных сетей.

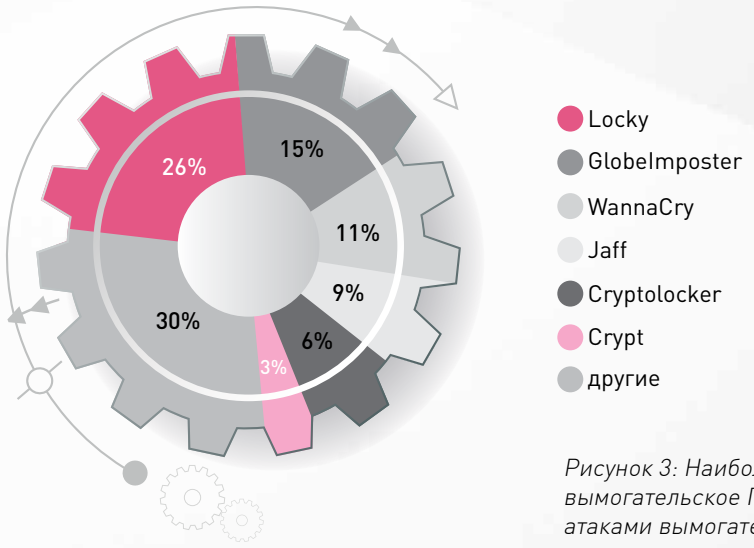


Рисунок 3: Наиболее распространенное вымогательское ПО по сравнению со всеми атаками вымогательских программ по всему миру. [12]

ПЯТОЕ ПОКОЛЕНИЕ МЕГА КИБЕРАТАК УЖЕ ЗДЕСЬ

Оглядываясь назад, легко идентифицировать различные поколения атак и продукты безопасности для защиты от них.

Однако тревожно, что скорость развития атаки намного опережает уровень безопасности, который используют организации.

Действительно, большинство из них оснащены только лишь системами, способными противостоять второму или третьему поколению угроз, в то время как атаки уже развились до пятого поколения.

Это большая проблема.

97%

ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ УСТАРЕВШИЕ ТЕХНОЛОГИИ КИБЕРБЕЗОПАСНОСТИ [13]

ОТЧЕТ **ПО ОТРАСЛЯМ ЭКОНОМИКИ**

ФИНАНСЫ: ЗАСТАВЛЯЯ МИР ВРАЩАТЬСЯ

ВВЕДЕНИЕ

Время биржевых брокеров и банковских клерков, выкрикивающих заказы под шум звонящих телефонов и пишущих машинок, давно прошли. Сегодня основой финансового мира являются компьютеры, а когда каждый день онлайн находятся сотни миллиардов долларов, атаки неизбежны.

Первичный мотив для кибератак финансового сектора очевиден — деньги. Однако деньги – это не всё, что поставлено на карту.

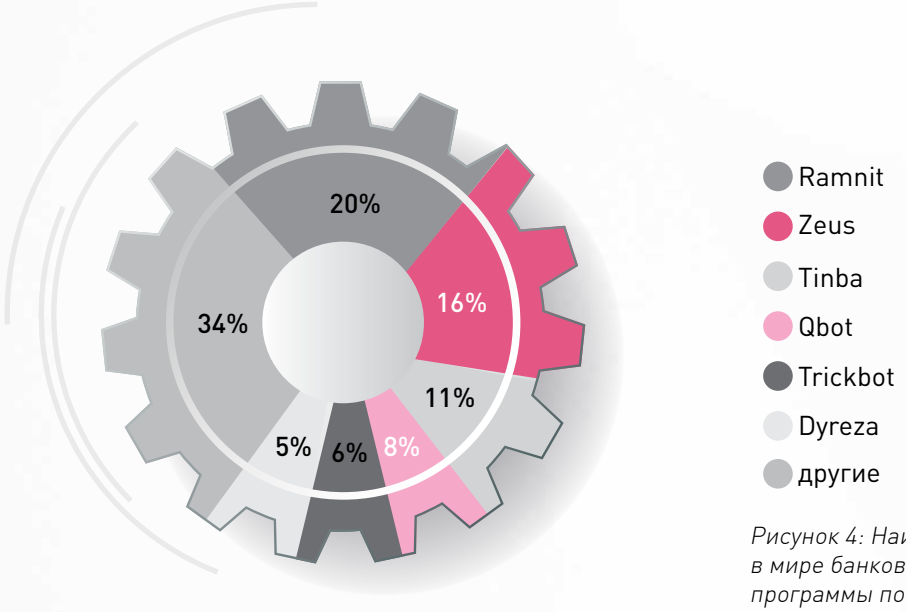


Рисунок 4: Наиболее распространенные в мире банковские вредоносные программы по отношению к общему количеству кибератак на банки. [14]

ПРОБЛЕМА

Финансовый сектор сталкивается с киберугрозами в трех основных областях: сеть SWIFT, вредоносное ПО для потребительского банкинга и кража информации.

Как доказала недавняя кража 60 миллионов долларов из Дальневосточного международного банка на Тайване, проприетарные банковские системы по-прежнему уязвимы для нападения. В этом конкретном случае специально созданное вредоносное ПО было внедрено не только на ПК и веб-серверы, но и в терминал SWIFT, используемый банком. После этого воры смогли получить учетные данные, необходимые для перевода платежей, и создали инструкции по переводу средств, производимых сетью SWIFT.

В результате многочисленных мер, предпринятых банками для обнаружения и предотвращения атак на счета своих клиентов, количество вредоносных программ в банках сократилось.

Это, однако, привело к тому, что разработчики вредоносных программ стали обращать свое внимание на более простые цели и избегать сложных механизмов защиты банков. Поскольку ворам больше не нужно взламывать банковский счет, чтобы получить деньги жертвы, это напрямую привело к увеличению вымогательских атак. В этом случае достаточно просто захватить компьютеры жертв для выкупа и вымогать у них деньги.

В то время как в мире ПК вредоносные программы перенацелились с банковских приложений на вымогательство, киберпреступления против мобильного банкинга продолжают оставаться популярными. Действительно, рост мобильного банкинга для удобства пользователей ввел новые риски, и эти пользователи, возможно, не знают об угрозах своим мобильным устройствам.

Другая арена киберпреступлений — это информация, которую хранят банки и кредитные агентства. В этом году мы получили неприятное напоминание об этом после взлома Equifax, который скомпрометировал конфиденциальную информацию почти половины граждан Соединенных Штатов.

И, наконец, в связи с тем, что блокчейн начинает выглядеть как будущее финансов, хакеры также устремили свой взгляд на эту новую тенденцию в финансовом секторе — криптовалюту. В декабре прошлого года Bitnex, крупнейшая в мире цифровая валютная биржа, была закрыта после массированной атаки «отказ в обслуживании». И это только один из недавних примеров в длинном списке атак, которые обрушились на этот рынок, приведя к убыткам, исчисляющимся многими миллионами долларов.

СОВЕТЫ И РЕКОМЕНДАЦИИ

Чтобы оставаться защищенными от эксплуатации уязвимостей в сетях SWIFT, финансовые учреждения должны внедрять не только стандартные меры безопасности, но и новейшие средства защиты, которые будут сдерживать даже самого искушенного злоумышленника.

Кражи из тайваньского банка можно было избежать, если бы использовались расширенные возможности криминалистического анализа для обеспечения видимости полной картины путем мониторинга и записи всех событий на конечных устройствах, включая зараженные файлы, запущенные процессы, изменения системного реестра и сетевой активности. Должно было быть развернуто решение, которое отслеживает шаги, предпринимаемые вредоносным ПО и блокирует попытку преступника замести свои следы.

Чтобы предотвратить доставку вымогательского ПО через вредоносные файлы финансовые организации должны иметь в своем распоряжении сложные механизмы для блокирования известных и неизвестных угроз. Система извлечения и эмуляции угроз, которая кроме того включает в себя мониторинг, протоколирование, отчетность и анализ событий для корреляции данных и предоставления информации о действительных атаках, также сэкономит драгоценное время команды IT-безопасности.

Финансовые учреждения должны понимать, что защита данных своих клиентов в облаке является общей ответственностью между ними и поставщиком облачных услуг. В рамках этой ответственности финансовые организации должны обеспечить немедленное применение патчей для всех известных уязвимостей, а также внедрение комплексных решений по предотвращению облачных угроз, которые обеспечивают защиту от атак «нулевого дня», а также гибкое и автоматическое управление доставкой, которое масштабируется в соответствии с их потребностями.

Хотя пользователи должны располагать собственным решением для защиты от вредоносных программ, реализованном на их мобильных устройствах, финансовым учреждениям было бы полезно внедрить передовые решения для мобильной кибербезопасности непосредственно в приложениях для банковских операций, которые используют их клиенты. Таким образом они могут защититься не только от угроз вредоносного ПО, попыток SMS-фишинга и проблем аутентификации, но также и от любых уязвимостей в самой мобильной операционной системе.

Хорошей новостью является то, что по мере того, как мониторинг и контроль безопасности становятся строже, атакующие становятся все более обескураженными своими результатами, как это видно из примера отмирания вредоносного банковского ПО для ПК.

Поскольку новые технологии, такие как блокчейн, быстро распространяются, банки должны внимательно следить за своей инфраструктурой безопасности и переходить к следующим поколениям технологий кибербезопасности. В этом случае они смогут не оставлять двери хранилищ открытыми и блокировать все попытки киберпреступников обогатиться за их счет.

ШОППИНГ В **РОЗНИЦЕ**

ВВЕДЕНИЕ

С данными о тысячах или даже миллионах кредитных карт и идентификаторах покупателей, расположенными глубоко внутри сетей компаний розничного сектора, у преступников есть все основания прилагать свои усилия на развитие вектора атак, нацеленного на этот сектор экономики.

На протяжении многих лет киберпреступники разрабатывали более сложные способы атак на терминалы Point-of-Sale (PoS) и взлома сетей розничных компаний, чтобы украсть идентификаторы клиентов и данные их кредитных карт. И действительно, охват и мощность этих атак только возрастают.

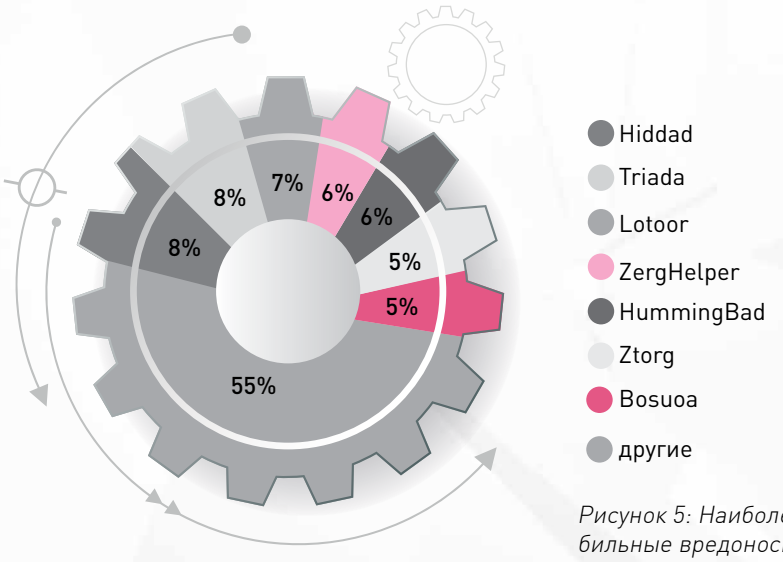


Рисунок 5: Наиболее известные в мире мобильные вредоносные программы. Поскольку все больше потребителей совершают свои покупки с помощью мобильных устройств, у разработчиков мобильных вредоносных программ появляется больше стимулов для обеспечения более широкого их распространения. [15]

ПРОБЛЕМА

В случае с киберпреступниками, целью которых является кража личных и финансовых данных клиентов, предоставленных в интернет-магазины, схемы цифрового маркетинга и лояльности, легко понять, почему более трети розничных компаний уже стали жертвами кибератак.

Стоимость украденных данных, продаваемых на черном рынке, теперь может достигать 20 долларов США за каждую запись, поэтому неудивительно, что информация о кредитной карте, а также личные контактные данные, даты рождения и информация о привычках покупателей являются наиболее распространенной целью киберкраж.

Примером этого был взлом данных GameStop в начале прошлого года. После кражи имен и адресов тысяч клиентов и данных их кредитных карт, включая номера CVV2, хакеры выставили их на продажу в «темном Интернете».

Кроме того, Forever 21 составил компанию другим розничным торговцам, таким как Chipotle, Kmart, Brooks Brothers, Target и T.J.Maxx, столкнувшись с атакой на пункты продаж. В этом случае хакеры получили доступ к платежной информации клиентов, отключив средства маркировки и шифрования, установленные продавцом всего за два года до этого.

Как показало наше исследование, помещенное на веб-сайте AliExpress, другой метод, используемый для получения доступа к информации о клиентах розничных торговцев,— это фишинг-атаки. В этом случае это фишинг в сочетании с атакой XSS, используемой для того, чтобы еще более убедить жертву в том, что ничего подозрительного не происходит. Действительно, в течение прошлого года крупные розничные компании, такие как Amazon, Best Buy, Walmart и Nike, были использованы в качестве приманки для покупателей, чтобы завлечь их в мошеннические схемы при покупках онлайн.

Ущерб, нанесенный репутации бизнеса, а также финансовые затраты могут быть огромными. По некоторым оценкам, средний ущерб компании составляет 172 доллара США за украденную запись. Это включает в себя затраты на восстановление после атаки, стоимость потерянного бизнеса из-за простоев, штрафы регуляторов и судебные издержки. Кроме того, наши опросы показали, что до 20% покупателей не вернутся в розничный онлайн-магазин, который стал жертвой кибератаки. Это высокая цена за то, что в принципе можно было бы предотвратить.

20%

ПОКУПАТЕЛЕЙ ГОВОРЯТ, ЧТО ОНИ НЕ ВОЗВРАТЯТСЯ В МАГАЗИН, КОТОРЫЙ СТАЛ ЖЕРТВОЙ КИБЕРАТАКИ [16]

1 из 3

РОЗНИЧНЫХ КОМПАНИЙ УЖЕ ПОДВЕРГЛАСЬ КИБЕРАТАКЕ [17]

СОВЕТЫ И РЕКОМЕНАЦИИ

В мае 2018 года ожидается введение Общих правил защиты данных (GDPR) ЕС, которые будут иметь далеко идущие последствия для розничных торговцев во всем мире. Чтобы избежать последствий взлома, компании должны внедрить решения безопасности с динамической архитектурой, которые обновляются в режиме реального времени.

Во-первых, требования PCI DSS должны быть реализованы по умолчанию, как часть общей стратегии безопасности. Это может происходить путем активного мониторинга элементов контроля безопасности для обеспечения эффективного и правильного рабочего процесса. Кроме того, политики аудита безопасности должны работать в режиме реального времени, а также гарантировать правильную настройку и работу таких элементов контроля безопасности, как межсетевой экран, антивирус, системы IPS (предотвращения вторжений) и DLP (предотвращения потери данных).

Розничные компании, которые используют устройства PoS, также должны предоставлять сквозное шифрование для всех операций с кредитными картами для защиты данных клиентов. Крайне важно также рассматривать защиту сети как задачу защиты диапазона множественных точек доступа, а не только лишь периметра.

Жизненно важно также использовать многоуровневый подход, который включает в себя обеспечение применения мер безопасности, контроль и управление. Мы рекомендуем создать план защиты шлюзов и конечных точек, который идентифицирует и блокирует вредоносное ПО, предназначенное для заражения компьютеров, а также сбора и извлечения информации о клиентах. При определении администратором политики безопасности автоматическая защита должна быть установлена с правилами, которые конкретно определяют политики контроля доступа и политики безопасности данных с точками их применения.

Наконец, в случае нападения предприятиям нужен план реагирования, чтобы обеспечить контроль над целостностью бизнеса, его репутацией и операциями. Этот план должен быть хорошо отрепетирован, при этом все участники должны знать свои роли и то, как взаимодействовать с другими членами команды реагирования.

ЛЕКАРСТВО БЕЗОПАСНОСТИ **ДЛЯ ЗДРАВООХРАНЕНИЯ**

ВВЕДЕНИЕ

С точки зрения кибербезопасности, возможно, наиболее уязвимой отраслью является здравоохранение, которое не только имеет дело с уязвимыми людьми, но и сама чрезвычайно уязвима.

Как часть отрасли, на которую общественность полагается буквально в деле спасения своих жизней, поставщики медицинских услуг являются легкими целями для вымогательства. Утечки конфиденциальной информации или остановка операций не является приемлемым вариантом.

ПРОБЛЕМА

В отрасли здравоохранения часто отказываются устанавливать обновления на оборудование, следуя регулирующим указаниям производителя, а также стремясь всеми способами обеспечить максимальное время беспрерывной работы медицинского оборудования.

К сожалению, это привело к тому, что один из самых тяжелых ударов от атаки WannaCry, который был нанесен в мае прошлого года, привел к выводу из строя большей части Национальной системы здравоохранения Великобритании (NHS). В ходе атаки компьютеры, необходимые для осуществления различных функций, включая сканеры МРТ, лабораторные тестовые установки и фармацевтическое оборудование, были выведены в офлайн, что привело к отмене тысяч визитов к специалистам и запланированных операций.

Индустрия здравоохранения также избрана целью хакеров, которые хотят украсть большое количество конфиденциальной информации, будь то для кражи идентификационной информации, мошеннических схем или продажи в «темной сети». Так было и в случае с Системой здравоохранения им. Генри Форда в Детройте в прошлом году, из которой было похищено более 18 000 записей уникальных данных о пациентах.

И наконец, еще один угрожающий вектор, который стал более заметен в прошлом году,— это уязвимости в самих медицинских устройствах.

Действительно, в то время как атака вымогательского ПО WannaCry затронула более 200 000 систем Windows в Великобритании, она также заразила радиологическое оборудование Bayer Medrad как на местном уровне, так и в США. Ущерб, наносимый через эти устройства, часто может быть невидимым, но тем не менее перебои в аппаратных средствах такого рода увеличивают потребности в ресурсах, вносят задержки в уход за пациентами и вызывают больше клинических ошибок.

Это так же страшно, как это и выглядит. Предоставление хакерам возможности подвергать опасности здоровье пациентов путем использования существующих уязвимостей, безусловно, представляет собой угрозу, которая должна быть устранена и устранена до того, как такие атаки будут реализованы.

СОВЕТЫ И РЕКОМЕНДАЦИИ

Для обеспечения того, чтобы пациенты получали необходимые экстренные сервисы, организациям необходимо решение, которое не только обнаружило бы дополнительные угрозы для своей сети, но в конечном итоге вообще помешало им проникнуть внутрь. Это означает наличие решения, включающего межсетевой экран, IPS, контроль приложений, антибот и возможности защиты от спама, а также технологии эмуляции угроз и извлечения угроз.

Поставщики медицинских услуг, безусловно, должны гарантировать, что у них есть возможности обнаружения эксплоита на уровне процессора. Это позволит им доставлять получателю очищенный документ, в то время как файл проходит проверку в фоновом режиме без каких-либо затрат для бесперебойной работы организации. Таким образом они смогут блокировать вредоносное ПО, предназначенное для обхода обычных технологий «песочницы», а также обеспечить свою защиту от передовых угроз, таких как WannaCry.

Кроме того, поставщики медицинских услуг должны стараться минимизировать сложность своих сетей и пытаться свести к минимуму различные версии программного обеспечения и отслеживать их из одного пользовательского интерфейса. Это упростило бы обновление своих систем и мониторинг ландшафта угроз, а также своевременное внедрение патчей безопасности.

И наконец, чтобы защитить устройства IoT, необходимо тщательное обнаружение и понимание того, что подключено к информационной среде системы здравоохранения. Только тогда может быть выполнена соответствующая сегментация этих устройств и правильная политика доступа. Это позволит предотвратить потенциальные атаки за счет глубокого контроля пакетов и фильтрации URL, например, для поддержания целостности данных, которые хранятся на этих устройствах, и операций, которые они выполняют.

ЭВОЛЮЦИЯ **ПРОИЗВОДСТВА**

ВВЕДЕНИЕ

Начиная с промышленной революции XVIII века в Манчестере, производство, как правило, претерпевает революцию каждые сто лет. Однако в эпоху постоянно растущего технологического прогресса времена меняются более быстрыми темпами, и, как мы видим, эпоха автоматизации на базе контроллеров постепенно заменяется «Умной фабрикой» (Smart Factory), иначе известной как «Промышленность 4.0» (Industry 4.0).

Несмотря на то, что она нацелена на упрощение производства и увеличение цифровых возможностей в рамках процессов цепочки поставок, Industry 4.0 также несет в себе новые киберриски и угрозы.

ПРОБЛЕМА

Полагая, что их заводы не являются мишенью для киберпреступников, многие промышленные предприятия в мае 2017 года были неприятно удивлены. В этом месяце атака вымогательского ПО WannaCry вызвала остановку автомобильных заводов Renault-Nissan в Европе и автомобильного завода Honda в Японии и создало массовые нарушения производственных циклов на предприятиях во всем мире. Летом того же года примерно половиной жертв вымогательского ПО Petya стали производственные предприятия.

Однако риску от кибератак подвержены не только производственные предприятия. Каждый производитель имеет жизненно важную информацию, которая может нанести ущерб, если она будет потеряна или украдена, начиная от данных исследований и разработок до проектных планов, не говоря уже о информации о клиентах. Риски для производственного сектора широкомасштабны, и они экспоненциально растут.

Поскольку мировая промышленность входит в следующую индустриальную революцию, разработка полностью интегрированного стратегического подхода к этим рискам будет иметь основополагающее значение для производственных цепочек, так как они объединяют операционные технологии (OT) и информационные технологии (IT).

82%

ПРОМЫШЛЕННЫХ КОМПАНИЙ ПОДВЕРГЛИСЬ ФИШИНГОВЫМ АТАКАМ В ПРОШЛОМ ГОДУ [18]

В связи с увеличением количества точек доступа, которые можно использовать для проникновения в обширную сеть, охватывающую не только цепочку поставок производства, но также подключенные устройства, используемые при администрировании бизнеса и предприятия, организациям необходимо иметь ввиду способы обеспечения безопасности этих точек для предотвращения несанкционированного доступа.

СОВЕТЫ И РЕКОМЕНДАЦИИ

Как и в любой другой отрасли, промышленные предприятия должны внедрять образовательные программы по кибербезопасности сотрудников, чтобы работники понимали основные методы обеспечения безопасности IT.

Кроме того, в производственной среде должны проводиться оценки рисков для определения наиболее ценных активов того, где они размещаются, у кого есть доступ к ним и методов их защиты. Это должно включать тщательный анализ предприятия, DSN, промышленных систем управления и всех подключенных устройств. Кроме того, нельзя упускать из виду такие методы «гигиены», как сегментация между OT и IT.

Также необходимо развернуть специализированные технологии ICS/SCADA. Для предотвращения манипулирования производственной средой необходима глубокая пакетная проверка протоколов SCADA, таких как связь MQTT/BACnet/Modbus между машинами и управляющими системами, которые их контролируют. Кроме того, решения должны обладать высокими параметрами видимости, включая гранулярный контроль трафика ICS/SCADA, виртуальное приложение патчей с использованием сигнатур ICS и устройств в защищенном исполнении для агрессивных сред.

Благодаря использованию как средств безопасности, так и облачных служб эмуляции угроз для защиты от атак «нулевого дня» и неизвестных вредоносных программ, промышленные организации также могут защищать свои сети от вымогательского ПО на более детальном уровне, включая проверку на уровне процессора.

Более того, промышленные организации могут предотвратить несанкционированный доступ к корпоративной информации с помощью контроля программ, антифишинга, защиты от шпионских программ, защиты данных и удаленного доступа, строя комплексную защиту с помощью единой архитектуры безопасности.

Защита «Промышленность 4.0» является сложной и широкомасштабной задачей, хотя есть много простых и стандартных способов, с помощью которых организации могут принять меры для собственной защиты.

Комбинируя такой подход с надежными элементами управления доступом, критически важные технологии могут быть защищены в точках приложений и конечных точках для обеспечения безопасности как данных, так и процессов.

ВОПРОС **НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ**

ВВЕДЕНИЕ

По самой своей природе государственный сектор обладает ценной информацией как на национальном, так и на частном уровне. Благодаря конфиденциальным данным, касающимся каждого гражданина, а также информации, связанной с государственной политикой, от энергетики до дипломатии,— все это делает его популярной целью для хакеров.

Из-за внедрения новых технологий и предоставления большего количества услуг в режиме онлайн правительственные агентства также сталкиваются с постоянно растущим числом атак. Эти шаги, безусловно, необходимы, но влекут за собой определенные риски, которые необходимо оценивать и от которых надо защищаться.

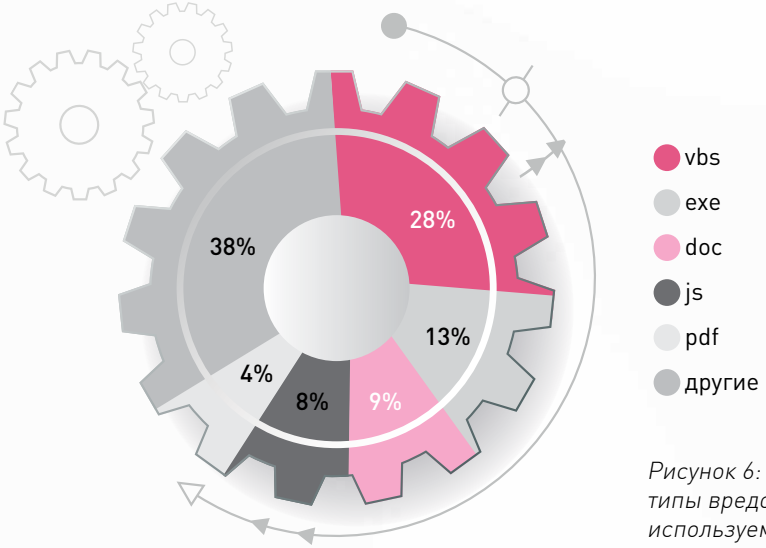


Рисунок 6: Самые распространенные типы вредоносных файлов, используемые для заражения компьютеров пользователей. [19]

ПРОБЛЕМА

Государственный сектор сам часто становится объектом атак с применением технологий, финансируемых государством, которые часто используются при нападениях на национальные агентства и учреждения и в которых участвуют самые передовые, искусные и упорные исполнители, обычно называемые группами Передовых постоянных угроз (Advanced Persistent Threats, APT).

Вместо того, чтобы искать самую легкую цель, группы APT обычно выбирают цели тщательно и концентрируются на них до тех пор, пока это требуется для получения доступа. При необходимости они будут разрабатывать индивидуальное оружие, чтобы проникнуть в определенную брешь в безопасности сети, против которого чрезвычайно сложно защищаться.

Одним из наиболее распространенных методов атаки, применяемых против государственных учреждений, является «фишинг». В июне 2017 года злоумышленники взломали систему начисления заработной платы системы государственной школы округа Денвер, чтобы украсть 40 000 долларов у сотрудников с помощью фишингового мошенничества. Такая атака воспользовалась, возможно, самой уязвимой частью безопасности любой сети — человеческим фактором. В подобных случаях фишинг-письма приходят как будто отправленными с адреса, с которым жертва привыкла работать и которому доверяет.

Также очень распространен захват учетных записей облачных приложений. Это наблюдалось в связи со взломом многих учетных записей электронной почты британских политиков в прошлом году, что путем атаки «грубой силы» позволило получить доступ даже к учетной записи премьер-министра.

Кроме того, как это показал вывод из строя национального банка, энергосистемы и аэропорта на Украине в июне 2017 года, правительственные инфраструктуры были среди тех глобальных целей, которые затронула атака вымогательского ПО Petya. Эта атака саботировала не только национальную инфраструктуру, но и нанесла экономический ущерб государству за счет вынужденного простоя промышленных предприятий.

Эти угрозы нельзя воспринимать легкомысленно. Последствия могут варьироваться от ослабленных позиций на переговорах и экономического ущерба до ущерба национальному суверенитету. Проще говоря, они превращают новую эру технологий в кошмар для правительств.

СОВЕТЫ И РЕКОМЕНДАЦИИ

Для защиты от несметного числа фишинговых атак следующего поколения требуется новый и многомерный подход. Такие средства безопасности должны защищать инфраструктуру электронной почты, обеспечивать высокоточную защиту от нежелательной почты и защищать правительства от широкого спектра угроз вирусов и вредоносного ПО, доставляемых по электронной почте.

Для того чтобы правительственные учреждения могли предотвращать хищения учетных записей, например, такие, которым подвергся парламент Великобритании, им необходимо внедрить решения безопасности, которые объединяют как анализ сетей, так и устройств. Эта технология должна иметь возможность глубокой оценки состояния как сети, так и конечных устройств.

Современные технологии часто терпят неудачу, потому что они не только не всегда достаточно надежны, но также громоздки в реализации.

Необходимы новые технологии, которые являются прозрачными для пользователя и просты в использовании настолько, что конечный пользователь не должен замечать, что они работают. Кроме того, они должны принимать детерминированные решения, которые будут препятствовать доступу самозванцев, в реальном времени.

Раньше использование эксплоита «нулевого дня» означало, что игра закончилась. Сейчас положение изменилось. В последние годы мы разработали технологии, способные обнаруживать и блокировать эксплоиты «нулевого дня», о существовании которых мы даже не знали. Эти технологии используются для противодействия усилиям групп APT, способных создавать такие эксплоиты, нацеленные на заражение вымогательским ПО какого-либо одного правительственного агентства.

Возрастают атаки на критические инфраструктуры правительств, которые часто строятся без какой-либо заботы о кибербезопасности и, таким образом, пронизаны уязвимостями.

Однако сегодня специальные решения для таких систем, предназначенные для обеспечения бесперебойной работы инфраструктуры, поддерживая при этом защиту от таких угроз, существуют.

32%

ПРАВИТЕЛЬСТВЕННЫХ УЧРЕЖДЕНИЙ СТАЛО ЖЕРТВАМИ ВЗЛОМА В ПРОШЛОМ ГОДУ [20]

ДОРОГА **ВПЕРЕД**

ВВЕДЕНИЕ

Однажды Авраам Линкольн сказал: «Вы не можете избежать ответственности завтра, уклонившись от нее сегодня». Это высказывание в высшей степени верно и для мира кибербезопасности.

В этом разделе мы рассмотрим, какие угрозы для наших сетей и данных можно ожидать в будущем, а в следующем разделе мы увидим, как организации могут ответственно подготовиться, чтобы избежать их.

БУДУЩЕЕ — ЭТО ОБЛАКО И МОБИЛЬНОСТЬ

Мобильные устройства являются частью IT-экосистемы и бизнеса по всему миру. Однако в большинстве организаций эти устройства не защищены на том уровне, который соответствует стоимости хранящихся в них активов. Недостатки в мобильных операционных системах и технологиях будут по-прежнему обнаруживаться, указывая на необходимость того, чтобы организации развертывали расширенную защиту от мобильных вредоносных программ и перехвата сообщений.

Мобильное вредоносное ПО также будет продолжать распространяться, особенно вредоносное ПО для мобильных банковских услуг, каким является развивающаяся и растущая тенденция Malware-as-a-Service (MaaS), которая снижает порог требуемых технических навыков злоумышленника и, таким образом, упрощает проведение атак.

Кроме того, мы можем ожидать, что мобильные криптомайнеры в ближайшем будущем будут использоваться для сбора криптовалюты для преступников. До сих пор криптомайнеры поражали в основном веб-серверы и ПК, но учитывая недостаточно развитые средства мобильной безопасности, они, скорее всего, и будут следующим каналом атаки.

77%

ПРОФЕССИОНАЛОВ IT СЧИТАЮТ, ЧТО ИХ КОМАНДЫ НЕ ПОДГОТОВЛЕНЫ К СЕГОДНЯШНИМ ВЫЗОВАМ КИБЕРБЕЗОПАСНОСТИ [21]

ПЕРЕХОДЯ В ОБЛАКО

Предприятия будут продолжать перемещать свои данные в облако более высокими темпами, поскольку компании стремятся сделать свою деятельность еще более эффективной в сложной экономической обстановке.

Хотя в настоящее время использование облаков широко распространено среди предприятий из-за гибкости и сокращения затрат, которые оно предлагает, эти технологии по-прежнему являются относительно новыми и постоянно развивающимися. Такое положение дел предоставляет хакерам больше «черных ходов» для более глубокого доступа к корпоративным системам.

В результате часто возникают неправильные представления о требуемых уровнях безопасности, а также недостаточное понимание ответственности за эту безопасность. Это оставляет широко открытую дверь для взломов.

В течение 2017 года более 50% инцидентов безопасности, обработанных командой реагирования на инциденты Check Point, были связаны с облаками, и более 50% из них были захватами учетных записей приложений SaaS или хостящихся серверов. Утечки данных будут по-прежнему представлять серьезную проблему для организаций, перемещающихся в облако, особенно из-за более широкого использования облачных сервисов обмена файлами.

Растущее внедрение электронной почты SaaS, такой как Office 365 и Google's G Suite, а также IaaS, делает ее привлекательной мишенью для киберпреступников, и мы ожидаем, что в 2018 году они будут все чаще становиться целями атак.

Кроме того, эти потенциальные угрозы будут усугубляться серьезными штрафами, которые могут быть наложены в связи с региональными регулирующими требованиями, такими как GDPR, в отношении компаний, которые не соответствуют этим новым нормативным обязательствам.

50%

ИНЦИДЕНТОВ БЕЗОПАСНОСТИ, ОБРАБОТАННЫХ КОМАНДОЙ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ CHECK POINT, БЫЛИ СВЯЗАНЫ С ОБЛАКАМИ [22]

ЗАЩИЩАЯ ВАШУ СЕТЬ

Вымогательское ПО зарекомендовало себя как высокоэффективный источник денег для преступников, а также маскировка для достижения более разрушительных целей. Из-за своей эффективности против всех типов пользователей, от потребителей до корпораций, вымогательское ПО будет продолжать расти, и мы можем ожидать увидеть более крупные, хорошо организованные всемирные кампании его использования, аналогичные WannaCry, Petya и Bad Rabbit.

Кроме того, мы можем ожидать от преступников дополнительных, более творческих методов вымогательства, таких как концепция «рекомендуй другу», чтобы побудить жертв распространять вредоносное ПО в обмен на более низкие платежи выкупа разблокировки их компьютеров.

По мере того, как операционные системы становятся более безопасными, мы можем ожидать снижение использования эксплоитов, нацеленных на эксплуатацию их уязвимостей. В свою очередь это приведет к увеличению использования базовых методов взлома, которые полагаются на человеческую ошибку и социальную инженерию в деле распространения вымогательского ПО.

75%

ОРГАНИЗАЦИЙ ИМЕЮТ ПРОБЛЕМЫ С ПЕРСОНАЛОМ И РЕСУРСАМИ БЕЗОПАСНОСТИ [23]

Кроме того, возможность использования вымогательского ПО для сбора средств для киберпреступников уже инициировала создание «вымогательского ПО-как-сервис» (Ransomware-as-a-Service) и других аналогичных услуг в «темной сети». Мы можем ожидать их рост и расширение спектра услуг, ориентированных не только на обычные компьютерные сети, но и на мобильные устройства и устройства «Интернета вещей».

ВВЕДЕНИЕ GDPR

Новые Общие положения о защите данных Европейского союза (GDPR) будут иметь далеко идущие последствия для многих организаций во всем мире. Основные элементы GDPR подробно описывают ряд «прав граждан ЕС» в отношении использования их персональных данных. Список обширен и потребует значительных изменений в приложениях, политиках и процедурах для достижения соответствия регулирующим правилам. В результате GDPR с учетом временных рамок и подразумеваемых наказаний окажет значительное влияние на любую организацию, которая обрабатывает данные граждан ЕС.

Однако, поскольку это регулирование является новым, опыт предыдущих аудитов, на которые может опираться организация, отсутствует. Кроме того, многие аспекты GDPR по-прежнему находятся в процессе разработки. Например, GDPR создает Европейский совет по защите данных (EDPB), чтобы «играть активную роль в обеспечении соблюдения закона о защите данных ЕС». Однако на момент публикации формализация EDPB все еще продолжается и спецификации еще не определены.

Тем не менее, ограниченное время, оставшееся до вступления регулирования в силу, означает, что организации уже должны фокусироваться и выделять ресурсы для реализации своей стратегии GDPR. Это включает в себя планы по набору персонала, аудиту и классификации данных, анализу рисков, журналированию активности и выявлению взломов, а также основным контролям.

«ИНТЕРНЕТ ВЕЩЕЙ» СТАНОВИТСЯ УМНЕЕ

Распространение устройств «Интернета вещей» будет продолжаться, что будет расширять потенциальную поверхность атаки. Следовательно, мы увидим больше вариантов атак Mirai и BlueBorne на «Интернет вещей» и подключенные устройства, которые появятся на нашем горизонте в 2018 году и в последующие годы.

Поскольку все больше интеллектуальных устройств встроены в структуру корпоративных сетей, а также сетей более широкого охвата, организациям необходимо будет начать использовать более эффективные методы обеспечения безопасности как для устройств, так и для сетей, к которым они подключаются. Это будет иметь решающее значение для предотвращения потенциальных широкомасштабных атак, и их применение может стать обязательным и контролироваться международными нормами.

Помимо масштабных атак DDoS, которые мы видели в 2017 году, домашние устройства «Интернета вещей» будут использоваться киберпреступниками, чтобы получить доступ не только к домашней сети жертвы, но также и для того, чтобы физически следить за ее домом. Это было подчеркнуто в нашем отчете об «умных домах» LG в прошлом году. Поскольку домашние пользователи, как правило, не знают об элементах безопасности своих домашних устройств IoT, они часто оставляют в них настройки по умолчанию. Это оставляет дверь открытой для злоумышленников, так что они постоянно имеют доступ к домашней сети пользователя.

Инициативы «Умный город» (Smart City) IoT продолжат свой импульс, помогая городам обеспечить лучший уровень обслуживания клиентов и существенно сократить расходы. В то же время решения кибербезопасности пятого поколения должны быть серьезно рассмотрены на каждом шагу, чтобы предотвратить потенциальные атаки.

В силу того, что организации здравоохранения сильно пострадали от атаки WannaCry, вертикаль здравоохранения также начнет акцентировать внимание на защите подключенных к Интернету медицинских устройств в больницах, чтобы предотвратить потенциальные атаки, несущие угрозу жизни.

ЦИФРОВЫЕ ВАЛЮТЫ

Случится ли так, что к криптовалютам, которые все чаще становятся предпочтительным способом оплаты преступникам в актах вымогательства и средством финансирования других незаконных действий, будут применяться более строгие правила?

Значительные ресурсы, необходимые для создания криптовалют, привели также и к появлению криптомайнеров. Это новые инструменты квазивредоносного ПО, которые используются для извлечения дохода путем захвата мощности процессора ни о чем не подозревающих пользователей компьютеров для создания валюты часто без ведома пользователя или их согласия. Мы уже могли наблюдать несколько таких примеров, и, поскольку стоимость криптовалют достаточно высока, мы можем ожидать, что киберпреступники найдут новые способы использования вычислительной мощности жертв, чтобы добывать эти валюты для собственной финансовой выгоды.

Кроме того, из-за высокой стоимости биткоина и других криптовалют, окружающие их системы, такие как криптовалютные биржи, также могут стать целью злоумышленников, которые желают использовать их уязвимости.

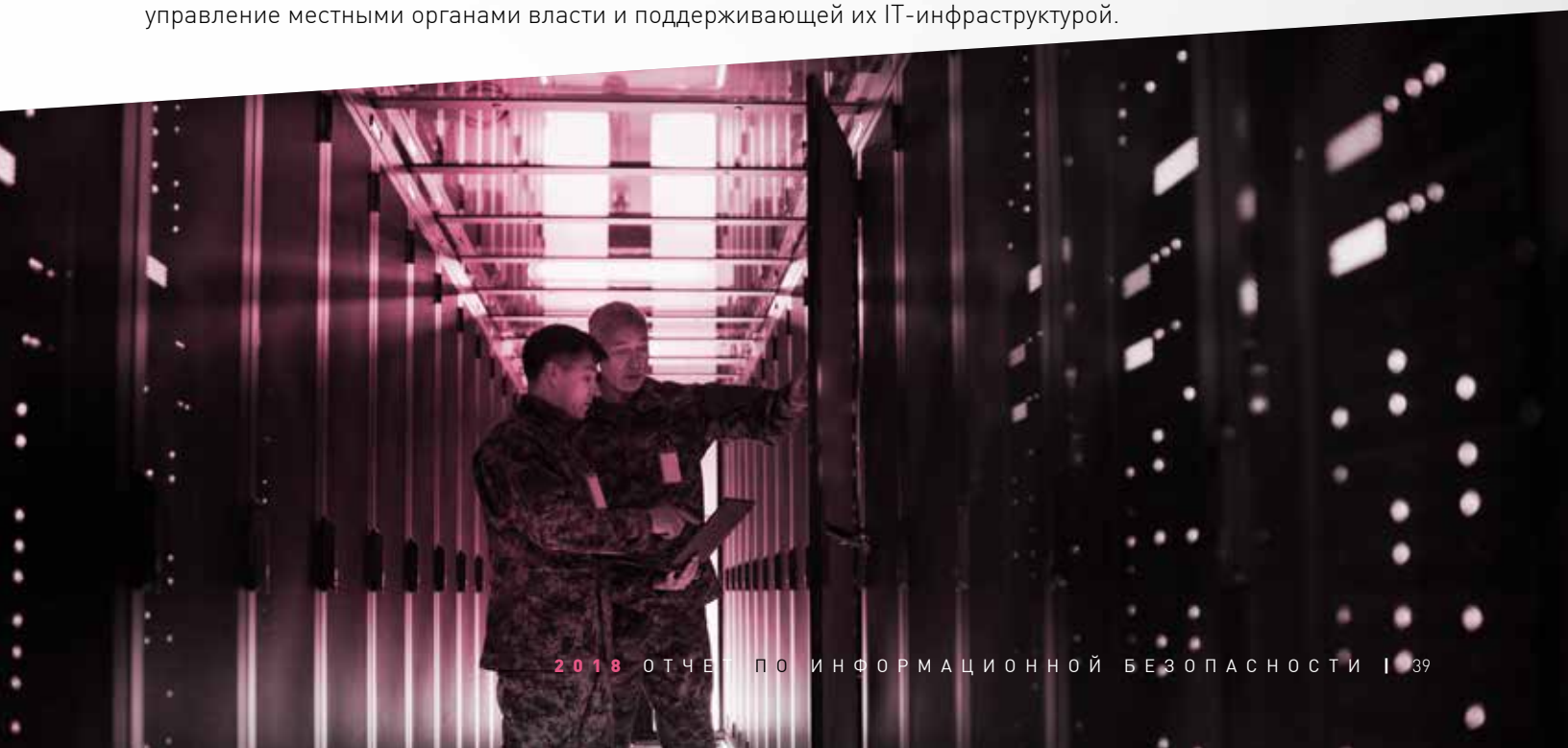
Сочетание этих факторов может привести к тому, что международные правительственные и правоохранительные органы предпримут меры против злоупотребления криптовалютами, что в свою очередь негативно повлияет на стоимость самой валюты.

ЗАЩИЩАЯ ГОСУДАРСТВО

В 2018 году и в следующие годы киберзащита обретет влияние и известность среди правительственных учреждений, поскольку они станут более чувствительными и настроенными на взаимосвязанный мир, в котором живут их граждане.

Кроме того, агентства, финансируемые государством, будут продолжать разрабатывать технологии кибератак для защиты и нападения, а преступные группы, движимые получением выгоды, будут продолжать искать способы монетизации кибератак. Кроме того, хактивисты будут продолжать использовать кибератаки для публикации своих сообщений, а негосударственные террористические группы также могут перейти в киберпространство, поскольку оружие, которое раньше использовалось для правительственных оборонных ведомств, стало публичным.

В результате мы вполне можем увидеть, что правительства развертывают больше средств защиты над своей собственной критической инфраструктурой, такой как энергетика и водоснабжение, медицинские услуги, управление местными органами власти и поддерживающей их IT-инфраструктурой.



РЕКОМЕНДАЦИИ **ПО ПЛАТФОРМЕ**

ДВИГАЯСЬ К АРХИТЕКТУРЕ 5-ГО ПОКОЛЕНИЯ IT-БЕЗОПАСНОСТИ

От конвергенции приложений и данных в IP-сети до развертывания «родных» облачных приложений, политик BYOD и использования устройств «Интернета вещей» — быстрая цифровая трансформация бизнес-приложений постоянно повышает требования к безопасности.

Существующие архитектуры безопасности для управления всем этим устарели и являются наиболее распространенной причиной проблем, связанных с потерей доступности и безопасности, приводящих к катастрофическим сбоям.

Однако, внедряя архитектуру «Поколения V», предприятия могут устранить единые точки отказа, получив необходимую силу и отказоустойчивость для поддержания операций и безопасности при любых обстоятельствах.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ПРЕДОТВРАЩЕНИЯ НА **30%** УСКОРЯЕТ ИДЕНТИФИКАЦИЮ И УСТРАНЕНИЕ УГРОЗ [24]

Архитектура безопасности «Поколения V» создает консолидированную унифицированную архитектуру безопасности, которая управляет и интегрируется с мобильными, облачными и сетевыми средами для защиты и предотвращения кибератак пятого поколения. Также должна работать интегрированная защита от угроз с динамической политикой безопасности на всех платформах, которая отвечает потребностям бизнеса, поддерживает параметры облачных сред с автоматическим масштабированием и может быть полностью интегрирована со сторонними API.

Кроме того, унифицированная и расширенная многоуровневая среда предотвращения угроз должна включать в себя предотвращение угроз с использованием «песочницы» на уровне процессора, извлечение угроз, антифишинговые и антивымогательские решения для защиты от известных и неизвестных атак «нулевого дня».

Таким образом, наличие правильной архитектуры, на которой работает вся инфраструктура безопасности, является единственным способом обеспечить единую сплошную защитную стену для предотвращения кибератак пятого поколения.

КОНСОЛИДИРОВАННОЕ УПРАВЛЕНИЕ
С ИСПОЛЬЗОВАНИЕМ ЛУЧШИХ ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

СТРОЯ СВОЮ ОБЛАЧНУЮ ИНФРАСТРУКТУРУ

По мере развития организаций к их бизнес-данным все чаще обращаются в любое время и в любом месте, используя облачные платформы. Это означает, что сетевой трафик выходит за рамки традиционных средств защиты IT-безопасности, а риски, связанные с этим, представляют собой огромную проблему. Более того, вредоносное ПО, внедряемое в облако, может легко распространяться среди облачных приложений, атаковать виртуальные сегменты или даже беспрепятственно переходить в корпоративные сети.

Чтобы преодолеть эти проблемы, предприятиям необходимо добиться синергии между лучшими практиками безопасности и облачными технологиями безопасности. Они должны в первую очередь подразумевать передовые методы блокировки и предотвращения угроз. Кроме того, они должны включать в себя мощные и хорошо знакомые инструменты и методы управления, обеспечивающие всесторонний обзор, мониторинг и отчетность. Это позволит им быстро идентифицировать вредоносную сетевую активность или известные показатели компрометации (IOC) и соответствующим образом реагировать на них.

Чтобы обезопасить облачные центры обработки данных, жизненно необходимо поддерживать гибкость и скорость в облаке на оптимальном уровне, чтобы решение обладало бесшовной автоматизацией и совместимостью с широким спектром облачных инфраструктур, таких как AWS, Cisco ACI, Microsoft Azure, OpenStack , VMWare и другие. Кроме того, решение должно включать расширенные средства управления безопасностью, разработанные для облачной инфраструктуры, которая основывается на сетевой безопасности с поддержкой микросегментации. Это может помочь уменьшить поверхность атаки и стать важным первым шагом в предотвращении кибератак в виртуальной сети.

Защита приложений SaaS путем блокирования захвата учетных записей, попыток фишинга и предотвращения распространения вредоносных программ «нулевого дня» в корпоративных сетях требует использования передовых решений. Эти решения должны быть направлены на определение законности доступа пользователей путем анализа данных в реальном времени как на ПК, так и на мобильных устройствах.

Наконец, чтобы полностью адаптировать облачные технологии, организации должны иметь как правильные политики, так и технологии обеспечения защиты. Это означает использование сбалансированной модели «совместной ответственности» между компанией-клиентом и облачным провайдером для защиты облачной инфраструктуры и данных, которые там находятся.

ВНЕ КОРПОРАЦИИ

По мере приближения организаций на платформах мобильности и SaaS к модели «Вне корпорации» («BeyondCorp») элементы управления доступом смещаются от периметра к отдельным устройствам и пользователям. Это обеспечивает беспрецедентный уровень доступа к важной бизнес-информации. Предоставление сотрудникам доступа к этой информации на мобильных устройствах по их выбору имеет много преимуществ, но также подвергает ваш бизнес рискам.

Вредоносные программы «нулевого дня», атаки «человек посередине» через Wi-Fi, попытки фишинга через SMS и уязвимости операционной системы могут использоваться для кражи конфиденциальной информации, такой как электронные письма, тексты, фотографии, календари и приложения.

В результате организации должны обеспечить конфигурацию всех своих мобильных устройств с использованием следующего поколения усовершенствованных технологий обнаружения и предотвращения угроз. В рамках защиты от эксплоитов уязвимостей ОС это означает

94%

КОМПАНИЙ ОЖИДАЮТ УВЕЛИЧЕНИЯ АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА[25]

использование как статических, так и динамических методов для мониторинга всех изменений конфигурации на корневом уровне устройства и использование механизма поведенческого анализа для обнаружения неожиданного поведения системы.

Предотвращение вредоносного ПО, доставляемого через поддельные приложения, должно включать решение, которое захватывает приложения по мере их загрузки и запускает каждое приложение в виртуальной среде «песочницы» для анализа его поведения. Помимо прочего оно должно объединять и сопоставлять сведения об источнике и репутации приложения на серверах приложения, а также использовать реверс-инжиниринг приложения для анализа кода.

Только решения, включающие поведенческий анализ для обнаружения мошеннических точек доступа и вредоносной сетевой активности, смогут автоматически отключать подозрительные сети. Технологии восстановления на устройствах также смогут динамически запускать защищенную VPN, которая обеспечивает конфиденциальность и целостность ваших сообщений.

Всесторонняя мобильная и SaaS-безопасность должна быть системой компонентов, которые работают сообща. Только решения, которые могут анализировать поведение по всем векторам для выявления показателей атаки, могут эффективно защитить мобильные устройства и обеспечить их безопасность.

«НЕТ» СЛАБЫМ ЗВЕНЬЯМ

Быстрый рост вредоносного ПО, растущая изощренность атак злоумышленников и появление новых неизвестных угроз «нулевого дня» требуют иного подхода для обеспечения безопасности корпоративных сетей и данных, нежели традиционные межсетевые экраны.

В пятом поколении сетевой безопасности для борьбы с известными и неизвестными кибератаками и угрозами необходимо применять унифицированный подход с такими функциями безопасности, как межсетевой экран, система предотвращения вторжений, антибот, антивирус, контроль приложений и фильтрация URL.

Вместе с передовыми методами эмуляции и извлечения угроз на более высоких уровнях OSI технологии «Поколения V» идут дальше и глубже в инспекции вредоносных программ на уровне центрального процессора и уровне ОС для выявления эксплоитов. Инновационные технологии «песочницы» должны включать в себя быстрые и точные техники обнаружения и блокировки, устойчивость к уклонению и глубокие проверки самого широкого массива файлов, включая неисполняемые.

Объединяя несколько технологий извлечения угроз в рамках единого устройства, решение сетевой «песочницы» также должно быть способно запускать механизмы предотвращения в разные моменты времени на основе сигнатур и динамического анализа, обеспечивая контроль доступа к сети на высоких скоростях и не создавая неудобств ведению бизнес-операций.

ЗАКЛЮЧЕНИЕ

За последние 25 лет атаки, равно как и меры безопасности, быстро развивались. Кибератаки постепенно совершенствовались для совершения киберпреступлений с использованием последних инноваций. Однако большинство организаций не эволюционировали и по-прежнему используют кибербезопасность второго или третьего поколения. Это создает огромный риск, так как мы уже сталкиваемся с пятым поколением кибератак.

Кибератаки пятого поколения, такие как мега-атаки 2017 года, определяются как крупномасштабные и быстротекущие атаки. Эти сложные атаки легко обходят традиционные, основанные на антивирусной защите, средства безопасности, используемые сегодня большинством организаций.

97% 

ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ УСТАРЕВШИЕ ТЕХНОЛОГИИ КИБЕРБЕЗОПАСНОСТИ [26]

Для борьбы с этими новыми атаками компании должны внедрить кибербезопасность пятого поколения, которая использует расширенную защиту от угроз в реальном времени и защищает все сетевые, виртуальные, облачные, удаленные и мобильные операции бизнеса.

К сожалению, сегодняшние атаки являются более передовыми и эффективными, чем мы когда-либо видели, а безопасность, развернутая большинством предприятий, отстает и неспособна защитить от таких атак. Наши исследования показывают, что огромное количество компаний сегодня используют только защиту второго или третьего поколения и только 3% фактически используют инструменты и методы пятого поколения.

Чтобы обеспечить лучшую защиту от расширенных угроз, описанных в этом отчете, организации должны подходить к решениям безопасности «Поколения V» для защиты от кибератак пятого поколения.

ССЫЛКИ

1. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
2. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
3. Source: Bloomberg, June '17, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections
4. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
5. Source: UK National Audit Of ce, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
6. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
7. Source: Check Point Mobile Threat Research Publications, https://research.checkpoint.com/check-point-mobile-research-team-looks-back-2017/
8. Source: Check Point Mobile Threat Research Report, November '17, sample size: 850 organizations.
9. Source: The State of Security Ef ciency Survey, February '18, sample size: 452 participants.
10. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
11. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
12. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
13. Source: Check Point Research Survey of IT Security Professionals, March '18, sample size: 443 participants.
14. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
15. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
16. Source: KPMG Consumer Loss Barometer Survey, August '17, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
17. Source: KPMG Consumer Loss Barometer Survey, August 17, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
18. Source: Check Point Meta-Analysis by Industry Survey, February '18, sample size: 450 participants.
19. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
20. Source: Check Point Meta-Analysis by Industry Survey, February '18, sample size: 450 participants.
21. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
22. Source: Check Point Incident Response Team.
23. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
24. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
25. Source: Check Point Dimensional Research Survey into Mobile Device Security, sample size: 410 participants.
26. Source: Check Point Research Survey of IT Security Professionals, March '18, sample size: 443 participants.

НАШИ КОНТАКТЫ

МЕЖДУНАРОДНАЯ ШТАБ-КВАРТИРА

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Телефон: 972-3-753-4555 | Факс: 972-3-624-1100
Эл. почта: info@checkpoint.com

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
Эл. почта: Russia@checkpoint.com

ПОДВЕРГЛИСЬ АТАКЕ?

Свяжитесь с нашей Командой Реагирования на инциденты:
emergency-response@checkpoint.com

WWW.CHECKPOINT.COM