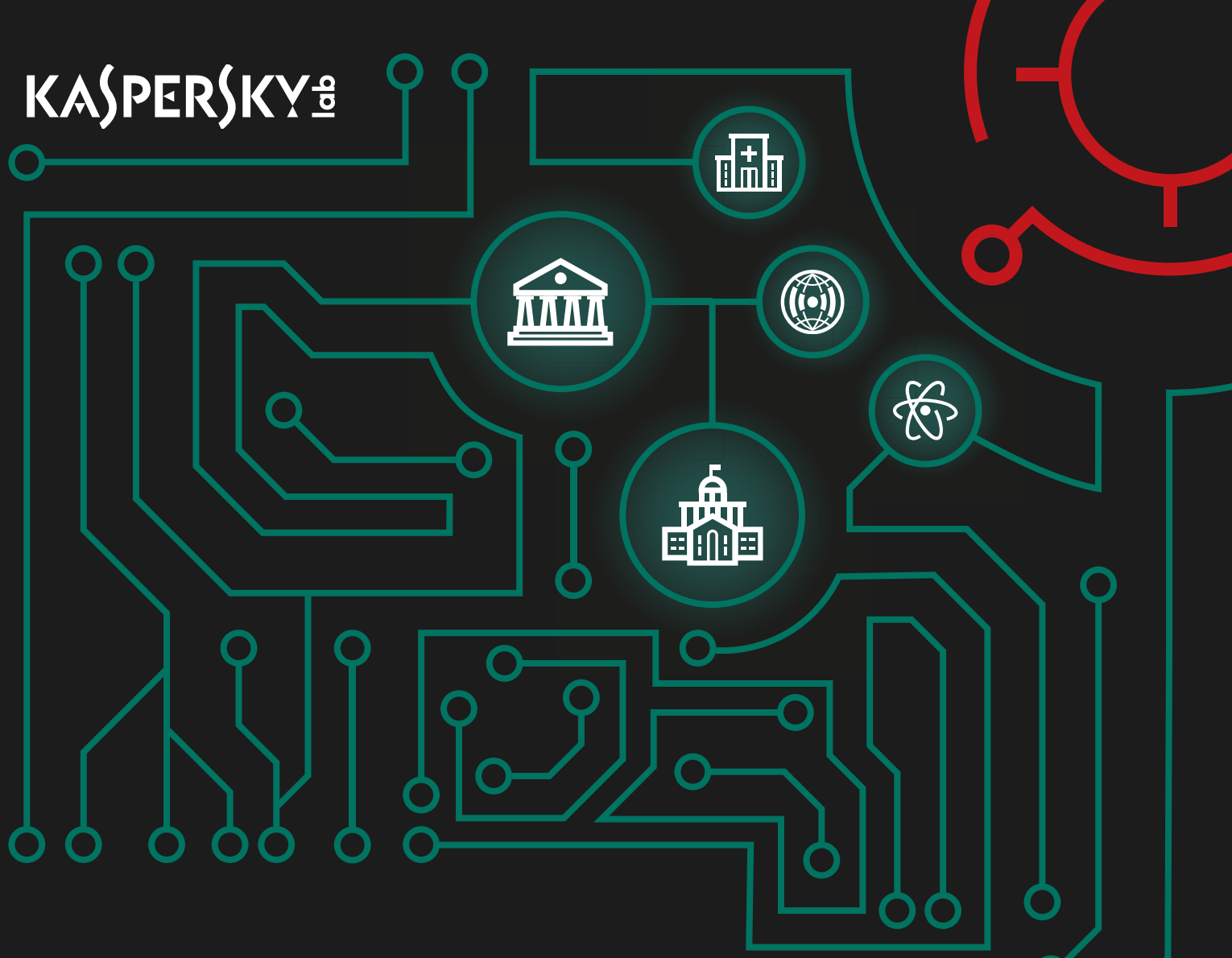
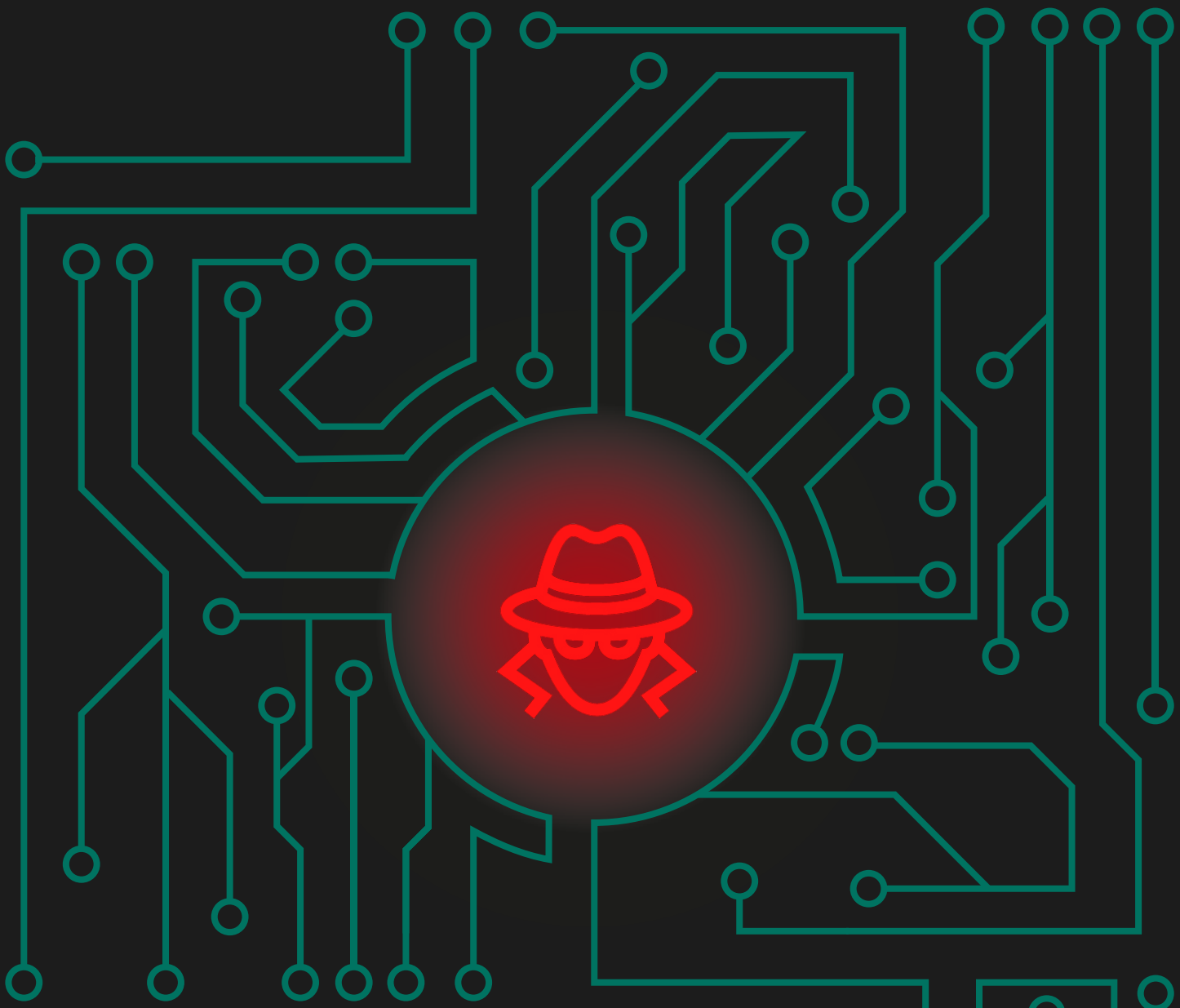
KASPERSKY lab



Kaspersky Security Bulletin:

2017. Развитие угроз

СОДЕРЖАНИЕ



ГОД РАЗМЫТЫХ ГРАНИЦ

Дэвид Эмм
Ведущий антивирусный эксперт
Центр глобальных исследований и анализа угроз
«Лаборатории Касперского» (GReAT)

ВВЕДЕНИЕ

Технологии подключенных устройств стали неотъемлемой частью нашей жизни, однако они дают киберпреступникам больше возможностей для проведения атак, чем когда-либо прежде. Во всем мире организации и отдельные пользователи все чаще становятся мишенями для атак злоумышленников, которые охотятся за деньгами и данными, стремятся вызвать сбои в работе, нанести физический и репутационный ущерб или просто развлекаются. Экосистема киберугроз строилась и развивалась годами, и наш ежегодный обзор основных тенденций в мире киберугроз и инцидентов безопасности является частью этого процесса.

В 2017 году наиболее заметной тенденцией стало постепенное стирание рамок и размывание традиционных границ между различными типами угроз и видами вредоносной деятельности. Интересно, как будут развиваться события в 2018 году.

В качестве примера можно привести прокатившуюся в июне волну атак троянца ExPetr. На первый взгляд эта вредоносная программа казалась очередным вымогателем, но на деле оказалась адресной деструктивной программой-вайпером. Другой пример – публикация дампа кода группировкой ShadowBrokers, в результате чего продвинутые эксплойты, возможно разработанные АНБ, попали в руки криминальных групп, которые иначе не получили бы доступа к коду такого высокого уровня. Еще один пример – появление APT-кампаний, проводимых не ради кибершпионажа, а для кражи денег с целью финансирования других видов деятельности, в которых участвует APT-группировка. Будет интересно узнать, какое развитие получит эта тенденция в 2018 году.

Эволюция программ-вымогателей в 2017 году и использование опубликованных Shadow Broker эксплойтов группировками более низкого уровня подробно описаны в отчете «Kaspersky Security Bulletin 2017. Сюжет года: Шифровальщики атакуют». Другие тенденции более подробно описаны ниже.

ЦЕЛЕВЫЕ АТАКИ

В 2017 году крупные международные киберпреступные группировки продолжили свою обычную деятельность, но с применением новых, более сложных в обнаружении инструментов и методов. Мы публиковали отчеты о целом ряде таких кампаний.

Русскоязычные кибергруппировки

В апреле 2017 года на конференции Security Analyst Summit «Лаборатория Касперского» и Королевский колледж Лондона представили результаты своих исследований возможной связи между Moonlight Maze — произошедшей 20 лет назад кампании кибершпионажа против Пентагона, NASA и других жертв, и современной APT-группировкой Turla. Данные, хранившиеся на сервере, который был взломан и использован злоумышленниками из Moonlight Maze в качестве прокси-сервера, позволили реконструировать операции, инструменты и методы, использованные преступниками. Параллельное было проведено расследование деятельности Turla. Было установлено, что при проведении обеих атак использовались бэкдоры на базе LOKI2 – программы, выпущенной в 1996 году и позволяющей извлекать данные через скрытые каналы.

В августе мы опубликовали новости о другой APT-кампании, имеющей отношение к группировке Turla и получившей название WhiteBear. В середине 2017 года WhiteBear расширил круг своих мишеней: теперь в зону его внимания, помимо посольств и консульств по всему миру, попали также оборонные учреждения. Мы предполагаем, что группировка использует целевые фишинговые письма для доставки жертвам зараженных PDF-файлов. Особенно интересен алгоритм шифрования, реализованный в основном модуле WhiteBear, который управляет работой всего зловреда. Злоумышленники шифруют/дешифруют и упаковывают/распаковывают раздел ресурсов при помощи уникального сочетания RSA+3DES+BZIP2. Большинство образцов WhiteBear подписаны действительным сертификатом, выданным британской компании, когда-то зарегистрированной под названием Solid Loop Ltd. Скорее всего, это подставная или уже несуществующая организация, чьим именем злоумышленники решили воспользоваться для создания поддельных цифровых сертификатов.

Англоязычные киберпреступные группировки

В апреле мы опубликовали отчет о новейших инструментах группы Lamberts, которую по уровню сложности можно сравнить с Duqu, Equation, Regin и ProjectSauron. Эта группировка, которая впервые попала в поле зрения специалистов по кибербезопасности в 2014 году, разработала и использовала в ходе своих атак набор сложных инструментов, в том числе сетевые бэкдоры, несколько поколений модульных бэкдоров, средства для сбора данных и программы-вайперы. Lamberts активна с 2008 года, а возможно, и раньше. Сейчас известны белая, синяя, зеленая, черная, розовая и серая версии зловреда для Windows и OS X, и весьма вероятно, что существуют версии Lamberts для других платформ, в том числе для Linux.

Китайскоязычные киберпреступные группировки

Мы также раскрыли новые технические сведения о группировке Spring Dragon, которая начала свою деятельность в 2012 году и специализировалась на целевом фишинге и атаках типа watering hole. Среди ее мишеней — крупные госструктуры, политические партии, образовательные заведения и телекоммуникационные компании в странах Юго-Восточной Азии, включая Тайвань, Индонезию, Вьетнам, Филиппины, Гонконг, Малайзию и Таиланд. Мы подробно исследовали бэкдоры, использованные группой для кражи данных, запуска дополнительных вредоносных компонентов и исполнения системных команд на зараженных компьютерах. Эти бэкдоры позволяют злоумышленникам выполнять на зараженных компьютерах широкий спектр вредоносных действий. Spring Dragon поддерживает большую сеть командных серверов, куда входят более 200 уникальных IP-адресов и доменов.

Кибрепреступные группировки, использующие другие языки

В октябре наши системы автоматической защиты от эксплойтов обнаружили новый эксплойт нулевого дня для Adobe Flash. Он доставлялся с документами Microsoft Office и использовался «в дикой среде» для заражения компьютеров наших клиентов последней версией вредоносной программы FinSpy. В нашей клиентской базе мы нашли только одну такую атаку, поэтому считаем, что их количество минимально и применяются они крайне избирательно. Анализ вредоносной программы позволил нам с уверенностью связать эту атаку с группировкой BlackOasis. Мы уверены, что эта же группировка несет ответственность за еще один эксплойт нулевого дня (CVE-2017-8759), обнаруженный FireEye в сентябре. Мы впервые столкнулись с BlackOasis в мае 2016 года, когда исследовали другой эксплойт нулевого дня для Adobe Flash (CVE-2016-4117), который активно применялся «в дикой среде». Данные, полученные из Kaspersky Security Network, помогли нам идентифицировать две аналогичные цепочки эксплойтов, использованные BlackOasis в июне 2015 года и на тот момент также бывшие эксплойтами нулевого дня (CVE-2015-5119 и CVE-2016-0984). Эти цепочки эксплойтов также доставляли установочные пакеты FinSpy. Мишенями BlackOasis являются политики и другие значимые фигуры в странах Ближнего Востока: видные деятели в Организации Объединенных Наций, оппозиционные блоггеры и активисты, а также корреспонденты региональных новостных служб.

Еще одна группа киберпреступников, занимающаяся целевыми атаками, – это Black Energy, которая, возможно, стояла за атаками криптовымогателей ExPetr и BadRabbit. Исследователи полагают, что между ExPetr и вымогателем KillDisk группы BlackEnergy, который действовал в 2015-2016 гг., может существовать связь.

ДЕСТРУКТИВНЫЕ АТАКИ

В 2017 году мы наблюдали возобновление целевых атак, направленных на уничтожение данных наряду с их кражей либо вместо нее.

В последние годы было выявлено несколько атак с использованием вайперов, и в 2017 году мы сообщили о еще двух таких атаках – Shamoon 2.0 и StoneDrill. Shamoon, с помощью которой, как считается, в 2012 году была стерта информация на более чем 30 000 компьютеров компании Saudi Aramco, вновь заявила о себе в ноябре 2016 и начале 2017 гг. в ходе атак на организации, играющие важную роль в экономике Саудовской Аравии. В версии 2.0 применяются новые инструменты и методы, в том числе специально созданная программа-вайпер, которая использует украденные учетные данные для распространения по корпоративной сети организации. Проникнув в сеть, этот вайпер активируется в заранее заданный день и выводит из строя зараженные машины. В состав Shamoon 2.0 также входит ransomware-компонент, который пока не применялся «в дикой среде».

Исследуя атаки Shamoon, эксперты «Лаборатории Касперского» обнаружили ранее неизвестную вредоносную программу-вайпер, которая, предположительно, предназначалась для проведения атак на организации в Саудовской Аравии. Мы назвали ее StoneDrill. StoneDrill имеет определенные стилистические сходства с Shamoon, но также несет дополнительные функции, затрудняющие ее обнаружение. Одна из жертв StoneDrill, по данным Kaspersky Security Network (KSN), находилась в Европе (компания работает в сфере нефтехимии). Это позволяет предположить, что стоящие за StoneDrill киберпреступники расширяют сферу своих интересов за пределы Ближнего Востока. Наиболее существенным различием между этими двумя зловредами является сам процесс удаления данных. Shamoon получает прямой доступ к диску при помощи драйвера диска, тогда как StoneDrill делает инъекцию кода вайпера непосредственно в память браузера, которым чаще всего пользуется жертва. Кроме того, в состав StoneDrill входит бэкдор, который использовался для проведения шпионских операций против ряда организаций-мишеней.

Неизвестно, стоят ли за Shamoon и StoneDrill одни и те же киберпреступники или это две разные группы, чьи интересы и география жертв совпадают. Наиболее вероятной мы считаем вторую версию.

Кстати, троянец ExPetr, который часто упоминается в этом обзоре, также относится к данной категории, поскольку он предназначался исключительно для уничтожения данных, хоть и был замаскирован под программу-вымогателя. Интересно, не предполагается ли при необходимости использовать не применявшийся пока ransomware-компонент Shamoon 2.0 для подобного отвлекающего маневра?

УСПЕХ БЕЗ СЛОЖНЫХ ИНСТРУМЕНТОВ

В 2017 году мы раскрыли случаи, когда злоумышленники добивались успеха, проводя технически несложные, слабо организованные кампании, иногда длившиеся годами.

Целевые атаки не обязательно должны быть технически сложными, чтобы успешно поражать свои мишени. В январе 2016 года в результате ареста итальянской полицией двух подозреваемых был выявлен ряд кибератак на известных политиков, банкиров, членов масонской ложи и сотрудников правоохранительных органов. Использованная в ходе атаки EyePyramid вредоносная программа была простой, а методы маскировки преступников – слабыми. Тем не менее, атака была достаточно успешной: злоумышленникиам удалось заразить около 1600 компьютеров, главным образом в Италии, прежде чем их задержала полиция. В полицейском отчете не указывались технические подробности распространения вредоносного ПО, однако были названы несколько командных серверов, IP-адресов и адресов электронной почты, использованных злоумышленниками для вывода украденных данных.

Используя эту информацию, мы создали правило YARA, с помощью которого проверили наши системы на наличие известных образцов этого зловреда. Это исходное правило помогло обнаружить два образца, проанализировав которые, мы создали более точное правило YARA, которое выявило в нашей коллекции еще 42 образца. Дальнейший поиск позволил получить больше данных об EyePyramid. В атаках активно применялись методы социальной инженерии с целью обманом заставить жертв открывать и запускать зараженные файлы, содержавшиеся во вложениях к адресным фишинговым письмам. Временные метки образцов говорят о том, что они были скомпилированы в 2014-2015 гг. Таким образом, несмотря на низкий уровень сложности этих атак, злоумышленники оставались незамеченными в течение нескольких лет и успели украсть у своих жертв гигабайты данных.

Вредоносная кампания Microcin – еще один пример того, как киберпреступники могут достигать своих целей, используя дешевые инструменты и тщательно выбирая своих жертв. Злоумышленники применили атаку типа watering hole с эксплойтом для Microsoft Office. Они заразили форум, на котором обсуждалось получение льготных квартир российскими военнослужащими и их семьями. Преступники создавали на компьютере жертвы исполняемый файл, который загружал дополнительные модули, расширявшие функционал вредоносного ПО. Нападавшие использовали PowerShell-скрипт и другие утилиты для кражи файлов и паролей, найденных на зараженной машине. Методы, применявшиеся преступниками, не являются ни сложными, ни дорогостоящими, но при этом они эффективны. Два аспекта этой атаки представляют особый интерес. Во-первых, злоумышленники решили использовать человеческий фактор, вместо того чтобы тратить время и деньги на разработку кода эксплойта для запуска прямой атаки на корпоративные ресурсы. Во-вторых, они воспользовались стандартными корпоративными инструментами для распространения зловреда в сети организации-жертвы.

КРАСТЬ, ЧТОБЫ ШПИОНИТЬ?

В 2017 году стало очевидно, что злоумышленники, реализующие сложные угрозы, широко применяют обычную кражу средств для финансирования своей высокозатратной деятельности.

В 2017 году стало очевидно, что злоумышленники, реализующие сложные угрозы, широко применяют обычную кражу средств для финансирования своей высокозатратной деятельности.

В феврале 2016 года группа неизвестных в то время хакеров пыталась украсть 851 млн. долларов, и успешно перевела со счетов Центрального Банка Бангладеша 81 миллион долларов. Это крупнейшее и наиболее успешное киберограбление на сегодняшний день. Расследование «Лаборатории Касперского» и других исследователей показало, что эти атаки почти наверняка были проведены известной кибершпионской и диверсионной группировкой Lazarus, в активе которой атака на Sony Pictures в 2014 году, а также атаки на промышленные компании, СМИ и финансовые учреждения в 18 странах, проводимые с 2009 года. Интерес к финансовым махинациям появился у Lazarus относительно недавно. Похоже, этим в составе группировки занимается отдельная команда, которую мы назвали Bluenoroff. На данный момент мы выявили четыре основных типа ее мишеней: это финансовые учреждения, казино, разработчики ПО для финансовых трейдеров и те, чей бизнес связан с криптовалютами.

Одной из самых заметных кампаний Bluenoroff стала атака на финансовые учреждения в Польше. Злоумышленникам удалось заразить государственный веб-сайт, к которому часто обращаются многие финансовые учреждения, что превратило его в особенно мощный вектор атаки.

Lazarus — это больше, чем просто очередная APT-группировка. Масштаб ее активности поражает: создается впечатление, что Lazarus представляет собой целую фабрику вредоносного ПО, создающую новые инструменты по мере того, как «расходуются» старые. Группировка использует различные методы обфускации кода, переписывает собственные алгоритмы, применяет коммерческие системы защиты ПО, а также использует свои собственные и сторонние подпольные упаковщики. Такой подход требует больших затрат, и это может объяснять, почему Lazarus обратилась к нелегальным заработкам.

Есть предположение, что WannaCry, начавший распространяться в мае 2017 года, также является детищем группы Lazarus. Подробнее об этой атаке можно прочитать в отчете «Kaspersky Security Bulletin 2017. Сюжет года: Шифровальщики атакуют». Однако по-прежнему остается загадкой, почему такая продвинутая группировка стояла за выпуском пусть и весьма разрушительного, но весьма несовершенного и плохо контролируемого вредоносного кода.

ДРУГИЕ ФИНАНСОВЫЕ АТАКИ

В 2017 году продолжился рост числа атак на банкоматы. В ходе атак на банковскую инфраструктуру и платежные системы наряду с заклеиванием объективов камер и сверлением отверстий применялись сложные бесфайловые зловреды.

В этом году на конференции Security Analyst Summit два исследователя «Лаборатории Касперского» — Сергей Голованов и Игорь Суменков — рассказали о трех атаках, направленных на кражу денег из банкоматов.

В первом случае зловред ATMitch заражал банковскую инфраструктуру и позволял злоумышленникам удаленно управлять работой банкоматов. Эксплуатируя незакрытую уязвимость, они проникали на серверы банка и заражали компьютеры в банковской сети, используя ПО с открытым кодом и публично доступные инструменты. При этом вредоносное ПО существовало только в оперативной памяти компьютера и не сохранялось на жестком диске, поэтому при перезагрузке компьютера практически все его следы терялись. После заражения зловред устанавливал соединение с командным сервером, позволяя злоумышленникам удаленно устанавливать на банкоматы вредоносное ПО. Защитные механизмы банка при этом не срабатывали, поскольку действия маскировались под легальное обновление ПО банкоматов. После установки зловред определял, сколько денег находится в банкомате, а затем выдавал ему команду на выдачу денег, которые забирал ожидающий у банкомата человек, так называемый «денежный мул». После этого зловред удалял следы своего присутствия.

Исследование другой банковской атаки также началось с запроса от банка. Из банкомата пропали деньги, при этом журналы банкомата были чисты, а камеры видеонаблюдения оказались заклеены. Банк привез банкомат в наш офис; вскрыв его, мы обнаружили подключенный Bluetooth-адаптер. После его установки злоумышленники выждали три месяца, чтобы журнал банкомата перезаписался, затем вернулись, заклеили видеокамеры, при помощи Bluetooth-клавиатуры перезапустили банкомат в сервисном режиме и забрали из него все деньги.

О третьей атаке мы также узнали от представителей банка, которые обратились к нам с просьбой расследовать кражу денег из банкомата. В этот раз подход киберпреступников оказался намного грубее: мы обнаружили в банкомате отверстие около 4 см в диаметре, проделанное около клавиатуры. Вскоре мы узнали о других подобных атаках на банкоматы

в России и Европе. Ситуация прояснилась, когда полиция задержала подозреваемого с ноутбуком и какими-то проводами. Мы вскрыли банкомат, чтобы выяснить, к чему злоумышленник пытался получить доступ через проделанное отверстие, и обнаружили 10-штыревой разъем, подсоединенный к шине, связывающей все компоненты банкомата. Кроме того, оказалось, что система шифрования в банкомате слабая и легко может быть взломана. Получив доступ к любому компоненту банкомата, можно было легко контролировать все остальные; а поскольку никакой авторизации между компонентами не было, любой из них можно было незаметно подменить. Потратив около 15 долларов и некоторое количество времени, мы смастерили простую схему, которая после подсоединения к шине позволила нам контролировать банкомат, в том числе отдавать команды на выдачу денег. Решение этой проблемы требует замены аппаратного обеспечения, что невозможно проделать удаленно. Для проведения замены к каждому такому банкомату должен выехать технический специалист.

Недавно экспертами «Лаборатории Касперского» была обнаружена новая целевая атака, направленная на финансовые учреждения – в основном банки в России, но также в Армении и Малайзии. Злоумышленники, стоящие за троянцем, получившим название Silence, применяют методику, подобную той, которую использовал Carbanak: они получают постоянный доступ к внутренней банковской сети, перехватывают данные с экранов компьютеров сотрудников банка, изучают рабочие процессы и установленное ПО, а затем используют эту информацию для кражи денег. В качестве метода проникновения используются адресные фишинговые письма с вредоносными вложениями. Интересная особенность Silence заключается в том, что атакующие используют зараженную банковскую инфраструктуру для рассылки новым жертвам вредоносных фишинговых сообщений с реально существующих электронных адресов сотрудников, что существенно повышает вероятность успешного заражения.

ЗАРАЖЕНИЕ ЦЕПОЧКИ ПОСТАВЩИКОВ ПО КАК СПОСОБ ПРОВЕДЕНИЯ АТАКИ

Это нацеленная на бизнес угроза, которая активно развивалась в 2017 году, и в 2018 году, скорее всего, будет расти.

В этом году мы наблюдали ряд «ступенчатых» атак, когда киберпреступники сперва атаковали поставщика своей мишени, пользуясь тем, что его ресурсы проще взломать. Именно так действовал июньский ExPetr – под удар попала компания, поставляющая бухгалтерское ПО для украинских предприятий. Большинство жертв находились на Украине, но в результате атаки также пострадали организации международного уровня, в том числе Maersk — мировой лидер в области морских контейнерных перевозок. В финансовом отчете компании указано, что Maersk ожидает убытков в размере 200–300 миллионов долларов США из-за «значительных перебоев в работе» в результате атаки ExPetr. Еще одна жертва – FedEx – сообщила, что ее европейское подразделение TNT Express было вынуждено приостановить работу, в связи с чем упущенный доход составил около 300 миллионов долл. США.

Киберпреступники, стоящие за появившейся в августе ShadowPad, использовали тот же подход – получили доступ к сети NetSarang, компании-производителя популярного программного обеспечения для управления серверами, с целью заражения некоторых ее клиентов, работающих в области финансовых сервисов, энергетики, розничной торговли, технологий и СМИ. Атакующие видоизменили одно из обновлений ПО, включив в него бэкдор, позволяющий злоумышленникам загружать и исполнять произвольный код, создавать процессы и поддерживать виртуальную файловую систему в реестре, шифруя все это и сохраняя в местах, уникальных для каждой жертвы.

В сентябре была зафиксирована еще одна атака, задействующая цепочку поставки ПО: злоумышленники взломали обновление CCleaner — утилиты для очистки Windows, распространяемой компанией Avast. Преступники внесли изменения в инсталлятор CCleaner 5.3, чтобы при установке утилиты он загружал вредоносную программу. Зловред, подписанный действительным сертификатом, был активен в течение месяца и заразил около 700 000 компьютеров. Злоумышленники действовали в два этапа: сначала на командные серверы преступников доставлялась информация о потенциальных жертвах, а затем в отношении выбранных мишеней проводилась атака.

ИНТЕРНЕТ ВЗЛОМАННЫХ ВЕЩЕЙ

Спустя год после активности ботнета Mirai в 2016 году, 300 000 подключенных устройств стали частью ботнета Hajime – и это лишь одна из многих кампаний, нацеленных на подключенные устройства и системы.

В наши дни умные устройства стали частью повседневной жизни. Сюда относятся популярные бытовые приборы и устройства – телефоны, телевизоры, термостаты, холодильники, радионяни, фитнес-браслеты и детские игрушки, но также автомобили, медицинские устройства, камеры видеонаблюдения и парковочные счетчики. Сейчас некоторые дома и квартиры сразу создаются «умными». Все эти устройства подключены к Сети через вездесущий Wi-Fi и объединены в Интернет вещей (IoT), который призван сделать нашу жизнь проще, но одновременно дает киберпреступникам больше возможностей для атак. Если IoT-устройства не защищены должным образом, личные данные, которыми они обмениваются, могут быть перехвачены, а сами устройства могут стать мишенью или средством для проведения атаки.

В октябре 2016 года ботнет Mirai блокировал работу части интернета в результате массированной DDoS-атаки, для проведения которой использовались зараженные подключенные домашние устройства, такие как видеорегистраторы, камеры видеонаблюдения и принтеры. А в апреле 2017 года злоумышленники, стоявшие за ботнетом Hajime, заразили более 300 000 устройств, хотя этот ботнет до сих пор не был использован для вредоносных целей: возможно, нападавшие просто хотели привлечь внимание общественности к недостаточной безопасности некоторых подключенных устройств. Исследователи обнаружили множество примеров незащищенных IoT-устройств. Опасения в отношении использования куклы My Friend Cayla злоумышленниками привели к тому, что Федеральное агентство сетей Германии, призванное защищать телекоммуникационную отрасль страны, посоветовало родителям, купившим куклу, избавиться от нее во избежание проблем. На Security Analyst Summit эксперт по кибербезопасности Джонатан Андерссон продемонстрировал, как умелый злоумышленник может создать устройство для угона дрона в течение нескольких секунд. Угроза взлома дронов может показаться экзотикой, однако дроны уже покидают свою узкую нишу: в декабре прошлого года платформа онлайн-торговли Amazon тестировала возможность использования дронов для доставки посылок покупателям.

Проблема не ограничивается бытовыми устройствами. Организации, которым ранее не нужно было думать о кибербезопасности, теперь все чаще сталкиваются с кибератаками. Одним из ярких примеров может служить здравоохранение. Медицинская информация, которая традиционно существовала в бумажной форме, теперь хранится в базах данных, на порталах и в медицинском оборудовании. Опасность заключается в том, что атака на подключенную к Интернету вещей больницу может привести не только к краже личной информации пациентов, но и к изменению диагностических данных, в результате чего больным может быть назначено неправильное лечение. Ранее в этом году мы сообщали о потенциальных угрозах такого рода и давали рекомендации по обеспечению безопасности медицинских учреждений.

УТЕЧКА ДАННЫХ

В 2017 году были взломаны базы Equifax и многих других организаций, с утечкой колоссальных объемов данных, последствия чего могут ощущаться годами.

Личная информация – ценный товар, поэтому неудивительно, что киберпреступники атакуют онлайн-провайдеров в надежде получить данные, которые они смогут затем продать или использовать для будущих атак на пользователей и бизнес. В 2017 году от утечки данных пострадали многие крупные компании, в том числе Yahoo (сообщение о взломе, произошедшем в 2013 году), Avanti Markets, Election Systems & Software, Dow Jones, America Link Link Alliance и Equifax. Также в ноябре 2017 года была обнародована информация о взломе Uber, который имел место в октябре 2016 года и привел к утечке данных 57 миллионов клиентов и водителей.

Некоторые из этих атак привели к утечке огромных объемов данных, причем в большинстве случаев это можно было предотвратить. Инциденты в Election Systems & Software и Dow Jones (а также другие, о которых мы не упоминаем в этом отчете) стал следствием неправильной конфигурации Amazon Web Services. В случае с американским Job Link Alliance хакеры использовали известную уязвимость в веб-приложении. Взлом Equifax стал возможен из-за уязвимости, которую Oracle исправила за несколько месяцев до атаки, но обновления безопасности не были вовремя установлены.

ЗАКЛЮЧЕНИЕ

В 2017 году многие угрозы на деле оказались не тем, чем представлялись поначалу: вымогатель оказался программой-вайпером, легитимное бизнес-ПО – вредоносным оружием, продвинутые кибергруппировки стали использовать простые методы, а в руки мелких злоумышленников попали высокотехнологичные инструменты. Одним словом, с точки зрения ландшафта киберугроз этот год принес перемены, которые поставили перед специалистами по кибербезопасности новые непростые задачи.

Проблема коснулась не только крупных предприятий. В 2017 году выросло число атак с использованием цепочки поставок, а это значит, что жертвой злоумышленников может быть любая компания, особенно если она станет мишенью для кибергруппировки, решившей взломать ее клиентскую базу. Как известно, стопроцентную безопасность обеспечить невозможно, однако организации и частные лица могут многое сделать, чтобы защитить себя от кибератак.

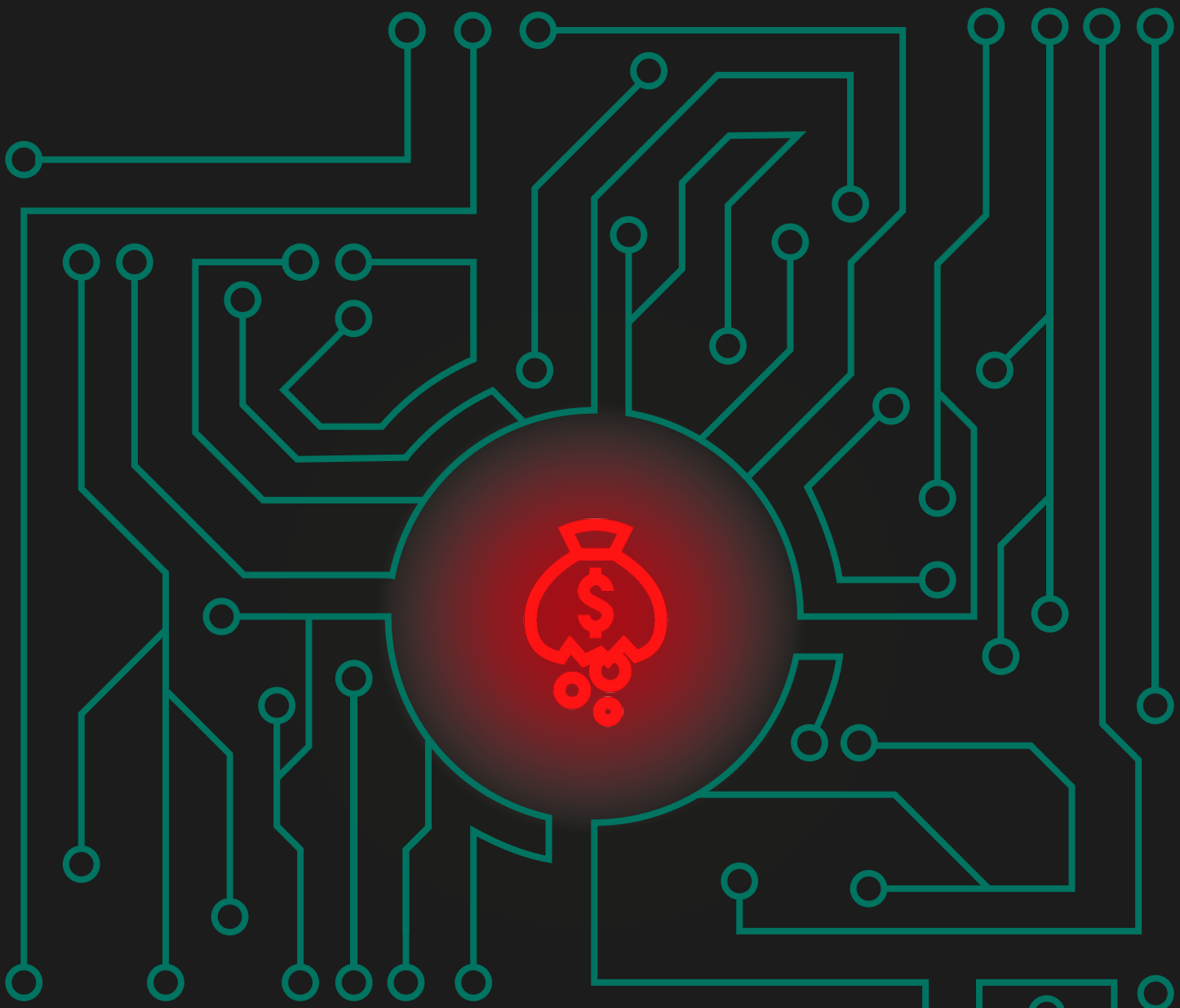
Лучшую защиту от целевых атак для бизнеса предоставляет многоуровневый подход, сочетающий применение традиционных технологий защиты от вредоносных программ с управлением установкой исправлений и использованием системы обнаружения вторжений, стратегии белых списков, сценария «Отказ по умолчанию» и актуальной информации об угрозах. Обеспечение безопасности должно рассматриваться как непрерывный процесс, требующий применения надежных инструментов и обширного экспертного опыта. Подписавшись на наши аналитические отчеты об APT-угрозах, вы получите доступ к новейшим исследованиям и обнаруженным угрозам в режиме реального времени, включая подробные технические сведения. Не стоит забывать и о человеческом факторе. Социальная инженерия остается ключевым методом киберпреступников, поэтому важно повышать осведомленность сотрудников о киберугрозах и способах борьбы с ними.

Любая организация, которая хранит личные данные пользователей, обязана заботиться об их эффективной защите. Если в результате взлома произошла утечка личной информации, компания должна предупредить об этом своих клиентов, чтобы они могли предпринять шаги для минимизации потенциального ущерба.

Одной из основных угроз для домашних пользователей по-прежнему остается мобильное вредоносное ПО. Развитие этой угрозы в 2017 году рассматривается в следующем разделе.

И наконец, никогда не теряют своей актуальности такие базовые для обеспечения кибербезопасности меры, как использование надежных паролей, регулярные обновления программного обеспечения и отключение не используемых функций. Это в равной степени касается любого подключенного устройства, будь то домашний принтер или критически важное медицинское оборудование.

2017 год преподнес нам много уроков, особенно в сфере защиты бизнеса. 2018 год покажет, какие из этих уроков были нами усвоены.



Мобильные угрозы 2017

Роман Унучек
Старший антивирусный эксперт

ВВЕДЕНИЕ

Для домашних пользователей, особенно для пользователей устройств Android, мобильные вредоносные программы являются, вероятно, одной из главных угроз. В 2017 году из-за зараженных троянцами мобильных приложений пользователи столкнулись с агрессивной рекламой, атаками вымогателей и кражей денег через системы SMS- и WAP-биллинга. В мобильных зловредах использовались новые приемы для обхода детектирования, обмана защитных технологий и эксплуатации новых сервисов. Как и в 2016 году, многие зараженные приложения были доступны во внушающих доверие магазинах, таких как Google Play Store.

Ниже приведен обзор основных мобильных угроз в 2017 году.

ТРОЯНЦЫ-РУТОВАЛЬЩИКИ

В течение последних нескольких лет троянцы-рутовальщики остаются самой серьезной угрозой для пользователей Android. Эти троянцы не только очень сложны, но также обладают большими возможностями и при этом широко распространены. Их главные цели – показ пользователю максимального количества рекламы, а также скрытая установка и запуск проплаченных приложений. В некоторых случаях из-за всплывающих окон и агрессивной рекламы нормальное использование устройства становится невозможным.

Этот тип вредоносного ПО обычно пытается получить права суперпользователя на зараженном устройстве, используя его уязвимости или же права, полученные при предыдущем заражении. Права суперпользователя предоставляют троянцу почти неограниченные возможности. Как правило, он устанавливает модули для самозащиты от удаления из системы, даже после сброса устройства до заводских настроек.

Распространение рутовальщиков через Google Play – явление не новое. Например, троянец Dvmap (Trojan.AndroidOS.Dvmap.a), внедрявший вредоносный код в системные библиотеки, скачивался из магазина Google Play более 50 000 раз. Мы также обнаружили на Google Play почти 100 зараженных троянцем Ztorg приложений, одно из которых было установлено более миллиона раз. Эти приложения получали рут-права, используя старые и давно известные уязвимости на устройствах, где не были установлены обновления безопасности, после чего внедряли свои модули в системы, чтобы стать неуязвимыми для попыток своего удаления и скрыто устанавливать новые программы.

Хотя в 2017 году количество пользователей, атакованных рутовальщиками, снизилось по сравнению с 2016 годом, почти половина (12) из 30 самых распространенных троянских программ для Android в этом году относились именно к этой категории (в 2016 году таких было 22). В основном мы связываем снижение популярности рутовальщиков с уменьшением количества старых устройств Android. На современных смартфонах и планшетах такие троянцы не могут эксплуатировать уязвимости для получения прав суперпользователя.

Однако это не означает, что киберпреступники, стоящие за троянцами-рутовальщиками, прекратили свои атаки. Некоторые из них просто отказались от использования рут-прав, но по-прежнему показывают агрессивную рекламу и загружают другие приложения. Кроме того, удалить такие приложения с устройства по-прежнему сложно, поскольку они могут эксплуатировать системные функции.

Мы также обнаружили, что троянец Ztorg начал осваивать новые способы получения денег, атакуя, например, мобильные платежные системы. Мы выявили два приложения с такими вредоносными функциями – в общей сложности они были загружены с Google Play десятки тысяч раз. Эти приложения отправляли SMS-сообщения на платные номера и удаляли все входящие SMS, таким образом незаметно похищая деньги со счета мобильного телефона жертвы. Исследования также показали, что некоторые из дополнительных модулей Ztorg содержали файл, написанный на JavaScript и позволяющий красть деньги с помощью кликджекинга (перехвата кликов) на сайтах, использующих WAP-биллинг.

КРАЖА СРЕДСТВ С ПОМОЩЬЮ КЛИКДЖЕКИНГА ПРИ ИСПОЛЬЗОВАНИИ СЕРВИСОВ WAP-БИЛЛИНГА

Сервисы, использующие WAP-биллинг, подвергаются атакам не только со стороны рутовальщиков. В 2017 году отмечался общий рост количества таких вредоносных программ. Их функционал не отличается новизной: Trojan-SMS.AndroidOS.Podec атаковал сервисы, использующие WAP-биллинг, еще в 2015 году. Однако в 2017 году в этом секторе появилось много новых и популярных троянцев, а количество атакованных пользователей по сравнению с 2016 годом возросло в 2,4 раза.

Большинство этих троянцев получают от своих командных центров URL-ссылки, которые они могут открывать и даже посещать соответствующие веб-страницы без ведома жертвы, иногда используя специальные JavaScript-файлы, чтобы нажимать кнопки на посещаемых сайтах. Если это просто рекламные страницы, особой опасности для жертвы нет (кроме случаев вредоносной рекламы, подобной той, что распространяет Ztorg), но это могут быть и сайты, поддерживающие WAP-биллинг, и мы обнаружили специальные JavaScript-файлы, созданные для эмуляции кликов на таких веб-страницах.

Обычно для подтверждения оплаты через WAP-сервис клиент перенаправляется на собственный сайт мобильного оператора, где ему предлагается подтвердить свое действие. Это ограничение троянцы научились обходить – они могут незаметно для пользователя нажимать на таких страницах кнопки, подтверждающие его согласие. Существует еще один уровень защиты – направление клиентам SMS-уведомлений о платежах, совершенных через WAP-сервис, но большинство троянцев способны незаметно удалять входящие сообщения.

БАНКОВСКИЕ ТРОЯНЦЫ

Банковское вредоносное ПО также расширило свой функционал, и в 2017 году мы выявили несколько новых методов, используемых для кражи денег. Одна из модификаций FakeToken атаковала более 2000 финансовых приложений. Этот троянец перекрывает приложения фишинговыми окнами, предназначенными для кражи данных банковской карты пользователя. Мы обнаружили модификации FakeToken, атакующие приложения для вызова такси, заказа билетов, бронирования гостиниц и даже для оплаты штрафов за нарушение ПДД.

Как правило, обновления ОС Android содержат новые функции безопасности, основная цель которых – защитить пользователей и сократить ущерб от вредоносных программ. Но вредоносные программы всегда находят способы обойти эти защитные средства. В июле 2017 года мы обнаружили, что Svpeng (Trojan-Banker.AndroidOS.Svpeng.ae) может выдавать себе все необходимые права, эксплуатируя специальные возможности устройства.

Специальные возможности – это системная функция, позволяющая разработчикам создавать приложения для пользователей с ограниченными возможностями использования устройства (такие ограничения могут быть постоянными или временными – например, во время вождения автомобиля). Троянец запрашивал у пользователя право использовать специальные возможности, а затем выдавал себе все необходимые разрешения для отправки SMS, просмотра контактов, совершения звонков и т.д. Кроме того, троянец незаметно перекрывал другие приложения и добавлял себя в список администраторов устройства. Он успешно препятствовал своему удалению, нажимая кнопки в системных диалогах. Использование специальных возможностей также позволяло ему похищать данные, вводимые через пользовательские интерфейсы приложений, и даже действовать в качестве клавиатурного шпиона.

В августе 2017 года мы обнаружили еще одну модификацию троянца Svpeng, которая также эксплуатировала специальные возможности мобильных устройств, но основной целью этого троянца было блокирование устройства, шифрование всех файлов жертвы и требование выкупа за разблокирование и расшифровку. Это не первый раз, когда мобильные банковские троянцы действуют как шифровальщики – у FakeToken также есть модификация, способная шифровать файлы.

В целом, Svpeng (Trojan-Banker.AndroidOS.Svpeng.q) оказался самым популярным мобильным банковским троянцем в 2017 году, хотя количество атакованных им пользователей по сравнению с 2016 годом сократилось в 1,5 раза. Еще одним активно действующим троянцем был Asacub (Trojan-Banker .AndroidOS.Asacub), распространяемый через спамовые SMS-сообщения. В 2017 году в Топ-30 популярных мобильных банковских троянцев было в три раза больше модификаций Asacub, чем в 2016 году (12 против 4).

ВЗЛЕТ И ПАДЕНИЕ КРИПТОВЫМОГАТЕЛЕЙ

В первом полугодии 2017 года значительно выросло количество мобильных троянцев-вымогателей – число установочных пакетов увеличилось в 1,6 раза по сравнению со всем 2016 годом. Но после июня 2017 г. оно сократилось до прежних значений. Подавляющее большинство (83%) мобильных вымогателей, ставших причиной этой вспышки активности, принадлежало семейству Congur (Trojan-Ransom.AndroidOS.Congur). По большей части это были довольно простые троянцы — они запрашивали права администратора устройства, меняли на нем PIN-код, а затем показывали сообщение на китайском языке, в котором жертву просили связаться со злоумышленниками через QQ – популярный китайский сервис обмена сообщениями.

Мобильные троянцы-вымогатели не сильно изменились в 2017 году: большинство из них продолжают использовать для блокировки устройств прежние методы. Мы не зарегистрировали большого количества пользователей, атакованных мобильными шифровальщиками.

ЗАКЛЮЧЕНИЕ

С увеличением количества мобильных устройств, расширением области их применения и ростом числа мобильных пользователей повышается вероятность появления и активного развития мобильных вредоносных программ. Так формируется постоянная «гонка вооружений» между киберпреступниками, разработчиками ПО и специалистами по кибербезопасности. Но это не означает, что пользователи обречены становиться жертвами киберпреступников – существует много возможностей защитить себя от угроз и обеспечить безопасность своих устройств и хранящихся на них данных. Прежде всего, следует пользоваться интернет-магазинами с хорошей репутацией и перед скачиванием приложения проверять его разработчика. Также мы рекомендуем установить на свои устройства надежное защитное решение, такое как Kaspersky Internet Security для Android.

KASPERSKY lab