KASPERSKY lab

KASPERSKY SECURITY BULLETIN 2016

GREAT

ОГЛАВЛЕНИЕ

ПРОГНОЗЫ НА 2017 ГОД: КОНЕЦ «ИНДИКАТОРОВ ЗАРАЖЕНИЯ»

ПРОГНОЗЫ НА 2017 ГОД: КОНЕЦ «ИНДИКАТОРОВ ЗАРАЖЕНИЯ»

Пролетел еще один год, и, судя по событиям, произошедшим в сфере информационной безопасности, он войдет в историю. Это был год драм, интриг и эксплойтов. Сегодня, мысленно возвращаясь к наиболее нашумевшим историям года, мы пытаемся заглянуть в будущее и дать прогноз, каким будет ландшафт угроз в 2017 году. Мы не будем предлагать читателям завуалированную рекламу, а постараемся построить свои прогнозы на основе тех тенденций, которые мы наблюдали в ходе наших исследований, и дать пищу для размышлений как экспертам в области IT-безопасности, так и просто интересующимся ею.

ОГЛЯДЫВАЯСЬ НАЗАД

Прошлогодние прогнозы оправдались практически полностью, некоторые – даже с опережением графика. Напомним наиболее примечательные из них.

APT-атаки. Мы ожидали уменьшения акцента на устойчивость к обнаружению, а также более частых попыток «смешаться с толпой» за счет использования стандартного вредоносного ПО в целевых атаках. Мы много раз видели проявление этой тенденции в применении атакующими бесфайлового вредоносного ПО, а также во множестве обнаруженных целевых атак на активистов и компании, проводимых с помощью широко распространенных вредоносных программ, таких как NJRat and Alienspy/Adwind.

Программы-вымогатели. 2016 год смело можно назвать годом вредоносных программ-вымогателей. Из финансовых вредоносных программ, позволяющих киберпреступникам завладеть деньгами жертв, остались практически только такие. В их основе лежит наиболее эффективная схема вымогания денег, и это позволило киберпреступникам привлечь ресурсы от менее прибыльных схем.

Больше банковских краж. Прогнозируя переход финансовых преступлений на самый высокий уровень, мы допускали, что мишенями могут стать такие организации, как фондовые биржи. Наши прогнозы реализовались в виде атак на систему SWIFT: эффективные и грамотно размещенные вредоносные программы позволили киберпреступникам положить в свой карман миллионы.

Интернет-атаки. Зачастую игнорируемая масса плохо защищенных устройств с подключением к интернету совсем недавно вторглась в нашу жизнь в виде отвратительного IoT ботнета, который вызвал перебои в работе крупных интернет-сервисов, а также проблемы у тех, кто полагался на конкретного поставщика DNS-сервисов.

Предание позору. Публикация порочащей информации и вымогательство продолжили свое победное шествие: стратегически спланированные и беспорядочные сливы информации стали причиной огромного количества личных, репутационных и политических проблем. Мы должны признать, что мы были поражены и масштабами некоторых из этих утечек, и тем, кто оказался в числе жертв.

ЧТО ГОД 2017 НАМ ГОТОВИТ?

Эти страшные APT-атаки

Появление индивидуальных и пассивных имплантов

Несмотря на то что приходится прилагать немалые усилия, чтобы убедить компании и крупные предприятия реализовать защитные меры, когда эти меры становятся малоэффективными или вовсе перестают работать, необходимо признавать это. Индикаторы заражения (IoC) – отличный способ делиться данными о характеристиках (таких, как хэши и используемые домены) или об особенностях выполнения уже известных вредоносных программ, что позволяет жертвам обнаружить активное заражение. Тем не менее, киберпреступники, составляющие 1% наиболее серьезных участников кибершпионских игр, умеют защищаться от таких общепринятых мер. Недавно это было наглядно продемонстрировано APT-группировкой ProjectSauron, использующей полностью адаптируемую модульную вредоносную платформу, каждый элемент которой модифицируется в расчете на конкретную жертву, что не позволяет использовать индикаторы заражения для обнаружения вредоносного ПО в системах других жертв. Это не означает, что защититься от атак совершенно невозможно, однако мы убеждены, что пора активнее выступать за более широкое применение качественных правил Yara, которые позволяют полностью проверять всю инфраструктуру предприятия, внимательно изучать и определять признаки заражения в неактивных исполняемых файлах, а также проверять память на присутствие фрагментов известных атак.

ProjectSauron также продемонстрировала еще одну сложную тенденцию, развитие которой мы ожидаем увидеть в будущем, – применение пассивных имплантов. Сетевой бэкдор, размещенный в памяти или установленный в виде драйвера с бэкдор-функционалом на интернет-шлюзе или интернет-сервере, молча ожидает появления волшебных байтов для пробуждения своего вредоносного багажа. До отправки злоумышленниками сигнала на пробуждение пассивные импланты практически не подают признаков активного заражения. В результате они могут быть обнаружены только самыми дотошными специалистами по безопасности или в рамках более широкого сценария реагирования на инциденты. Нужно учитывать, что эти импланты не имеют заранее определенной инфраструктуры командных серверов, что усложняет их идентификацию и обеспечивает более высокую степень анонимности. Таким образом, это инструмент для самых осторожных киберпреступников, которым может потребоваться оперативно получить доступ в атакуемую сеть.

Короткие заражения

Помимо того, что PowerShell приобрел популярность среди администраторов Windows, для которых он стал «инструментом мечты», его взяли на вооружение и многие разработчики вредоносного ПО, которые ищут пути для скрытного развертывания своих программ, механизмы распространения их по сети, а также возможности получения разведывательных данных без лишних записей в журналах событий, используемых в стандартных конфигурациях. Можно предположить, что крошечные, размещаемые в оперативной памяти или в реестре вредоносные программы, использующие PowerShell, будут прекрасно себя чувствовать в современных системах Windows. В качестве развития этой тенденции в дальнейшем мы ожидаем увидеть короткие заражения: резидентное вредоносное ПО, предназначенное для проведения общей разведки и сбора учетных данных, для которого продолжительность нахождения в системе – не главное. В средах с высокими требованиями секретности злоумышленников, действующих скрытно, может устраивать возможность присутствия в системе до тех пор, пока при перезагрузке их вредоносная программа не будет удалена из памяти, если это будет означать отсутствие подозрений и риска провала при обнаружении их зловредов сотрудниками организации-жертвы или экспертами по безопасности. Риск подобных коротких заражений означает, что в состав передовых антивирусных решений должны входить системы проактивного обнаружения угроз и сложные эвристические механизмы (см.: Мониторинг активности).

Шпионаж становится мобильным

Мы уже сталкивались с использованием мобильных имплантов во вредоносных платформах, таких как Sofacy, RedOctober и CloudAtlas; они также применялись клиентами HackingTeam и, предположительно, использовались вредоносной программой для iOS под названием Pegasus, созданной компанией NSO. Однако все это было в рамках кампаний, ориентированных прежде всего на настольные компьютеры. Учитывая падение интереса пользователей к настольным операционным системам и фактическое перемещение цифровой жизни среднестатистического пользователя в его карманы, мы ожидаем рост количества мобильных кампаний, в первую очередь шпионских. Их реализацию, безусловно, облегчит менее пристальное внимание, а также наличие проблемы применения инструментов цифровой криминалистики к новейшими мобильными операционными системами. Широкое доверие к подписанному коду и проверкам целостности постепенно сходит на нет среди экспертов в мобильной безопасности, но это не заставит целеустремленных и имеющих в своем распоряжении значительные ресурсы злоумышленников отказаться от охоты на интересующие их объекты в этой области.

Будущее финансовых атак

«Мы слышали, вы хотите ограбить банк...»

Сообщения об осуществленных в этом году атаках на межбанковскую систему SWIFT вызвали волнение в финансовой отрасли – в том числе из-за дерзости атакующих, посягнувших на многомиллионные суммы. Эти атаки стали естественным этапом развития для таких игроков, как группировка Carbanak и, вероятно, другие известные группировки. Подобные ограбления – дело рук преступных групп, специализирующихся на APT-кампаниях, со сложившимся стилем работы и известной квалификацией. Вероятно, это не единственные игроки, кому интересна идея ограбить банк на крупную сумму?

Мы ожидаем, что, по мере роста интереса к данной теме со стороны киберпреступников, в многоуровневой структуре киберпреступных предприятий будут появляться посредники в организации SWIFT-краж. Чтобы осуществить подобное ограбление, требуется первоначальный доступ, специализированное ПО, терпение и, наконец, схема отмывания денежных средств. На каждом из этих этапов есть поле деятельности для уже состоявшихся киберпреступников, предлагающих свои услуги за деньги; недостающим звеном является специализированное ПО для проведения атак на SWIFT. Мы ожидаем, что произойдет товаризация таких услуг, а специализированные ресурсы станут предлагаться на продажу на подпольных форумах или в качестве криминальных сервисов.

Устойчивость платежных систем

Мы ожидали, что по мере внедрения и роста популярности платежных систем будет расти интерес к ним со стороны киберпреступников. Однако при реализации этих систем в них, по всей видимости, был заложен очень высокий уровень защищенности – на них по сей день не зафиксировано крупных атак. Для потребителя это к лучшему, однако для владельцев платежных систем все не так радужно, поскольку киберпреступники неизбежно будут пытаться осуществлять прямые атаки на инфраструктуру платежных систем. Вне зависимости от того, приведут ли такие атаки к прямым финансовым потерям или только к перебоям и отключениям сервисов, мы ожидаем, что рост популярности платежных систем приведет к повышению интереса к ним со стороны киберпреступников.

Грязное и лживое вымогательство

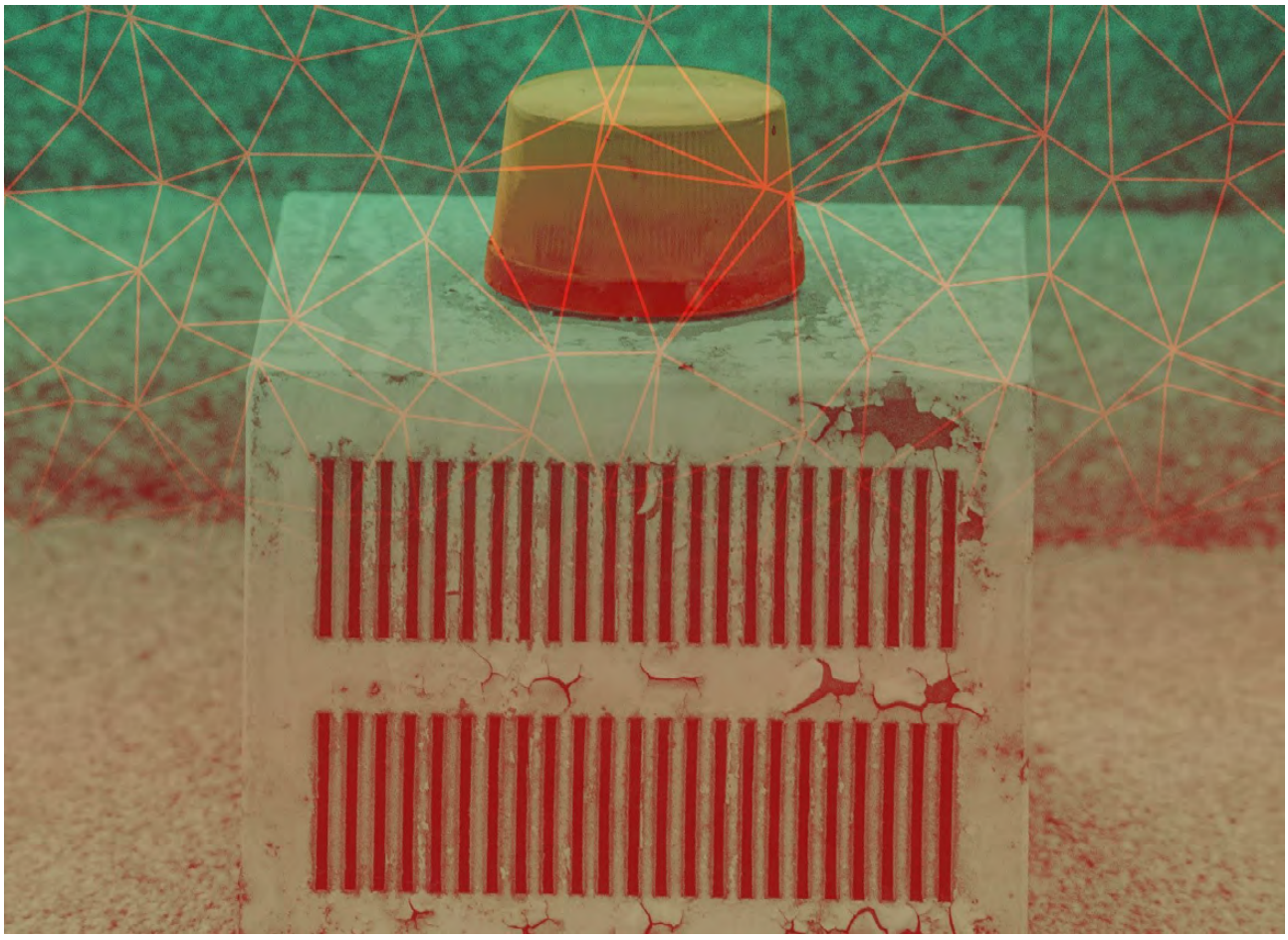
Хотя все мы ненавидим программы-вымогатели (и не без оснований), надо понимать, что в большинстве случаев успех вымогателей строится на своеобразных доверительных отношениях между жертвой и атакующей стороной. Киберпреступная экосистема основывается на посылке, что злоумышленник будет соблюдать молчаливое соглашение с жертвой о том, что, заплатив выкуп, жертва получит назад свои файлы. Киберпреступники, как это ни удивительно, демонстрируют некое подобие профессионализма в исполнении этого негласного обещания; и это стало основой процветания данной экосистемы. Однако программы-вымогатели становятся все более притягательными, привлекая менее квалифицированные слои киберпреступников. В результате в будущем мы будем все чаще сталкиваться с программами-вымогателями, за которыми стоят киберпреступники, не выполняющие вышеописанное молчаливое соглашение – из-за ошибок в коде или в силу того, что функционал восстановления файлов в программе просто не реализован.

Итак, мы ожидаем появления программ-вымогателей, созданных так называемыми «скрипт-кидди» (начинающими хакерами), которые будут блокировать файлы или доступ к системе или будут просто удалять файлы, обманным путем заставляя жертв платить, но при этом не возвращая им доступ к файлам. В этом случае вымогатели мало чем будут отличаться от вредоносных программ, уничтожающих данные, и следует ожидать, что в экосистеме программ-вымогателей возникнет «кризис доверия». Вероятно, это не помешает крупным профессиональным игрокам продолжать делать деньги на программах-вымогателях, но приведет к тому, что силы, пытающиеся противостоять разрастающейся эпидемии вымогательства, перестанут рассматривать идею оплаты выкупа как сколько-нибудь осмысленное решение проблемы.

Большая красная кнопка

Знаменитый Stuxnet, возможно, открыл ящик Пандоры, впервые реализовав возможности проведения атак на промышленные системы. Хотя разрабатывался он весьма тщательно с целью вывести из строя на длительное время совершенно определенные объекты. Даже когда вредоносная программа распространилась по всему миру, сопутствующий ущерб был невелик благодаря реализованным в ней ограничениям на запуск полезной нагрузки, и промышленного Армагеддона не произошло. Однако теперь при появлении любых слухов или сообщений об авариях на промышленных объектах или взрывах, произошедших по неизвестным причинам, будет выдвигаться версия кибердиверсии.

Тем не менее, аварии на промышленных объектах, вызванные подрывной деятельностью в киберпространстве, не являются чем-то невозможным. Поскольку критически важные объекты инфраструктуры и производственные мощности, будучи подключенными к интернету, часто по-прежнему не имеют надежной или хотя бы какой-нибудь защиты, они становятся привлекательными мишенями для хорошо обеспеченных ресурсами злоумышленников, стремящихся причинить как можно больший ущерб. Если не поддаваться панике, то можно заметить, что подобные атаки требуют определенных навыков и целеустремленности. Атаки с применением кибердиверсий наиболее вероятны там, где растет геополитическая напряженность и есть хорошо подготовленные киберпреступные группировки, стремящиеся к целенаправленному уничтожению или нарушению нормальной работы важнейших сервисов.



Перенаселенный интернет: ответный удар

Кирпич, как его ни назови

Мы уже давно предсказывали, что слабая защита «интернета вещей» (возможно, правильнее было бы назвать его «интернетом угроз») обернется для нас большими проблемами, и вот час настал. Как недавно наглядно продемонстрировал ботнет Mirai, слабая защита устройств, которые без необходимости подключены к интернету, дает злоумышленникам возможность сеять хаос, не неся за это практически никакой ответственности. Хотя для экспертов по информационной безопасности это не сюрприз, следующий шаг может оказаться особенно интересным: мы считаем, что хакеры-вигиланты могут взять дело в свои руки.

Идея установки патчей для известных и вновь обнаруженных уязвимостей близка сердцу исследователей в области информационной безопасности, поскольку это свидетельство того, что их тяжелый (и часто безвозмездный) труд был не напрасен. Поскольку производители устройств интернета вещей продолжают выпускать незащищенные устройства, которые вызывают массу проблем, хакеры-вигиланты, скорее всего, возьмут на себя решение проблемы. А какое решение может быть лучше, чем создать проблемы самим производителям, массово превращая эти уязвимые устройства в «кирпичи»? Поскольку ботнеты, состоящие из устройств «интернета вещей», продолжают вызывать головную боль, устраивая DDoS-атаки и распространяя спам, иммунным ответом экосистемы может стать отключение сразу всех этих устройств к огорчению и потребителей, и производителей. Не исключено, что в ближайшем будущем мы столкнемся с «интернетом кирпичей».

Молчание мерцающих коробочек

В августе 2016 года группировка ShadowBrokers шокировала многих, опубликовав дамп, который содержал огромное количество работающих эксплойтов для межсетевых экранов нескольких крупных производителей. Затем появились сообщения об обнаружении эксплойтов из дампа «в дикой среде», а производители кинулись разбираться с уязвимостями и выпускать патчи. Масштаб бедствия еще предстоит определить. Что получили злоумышленники, имея на руках эти эксплойты? Какие импланты могут находиться в уязвимых устройствах, не проявляя себя до поры до времени?

Если выйти за рамки вопроса о конкретных эксплойтах (не забывая при этом об обнаружении бэкдора в операционной системе ScreenOS компании Juniper в конце 2015 года), существует более крупная проблема с целостностью устройств, которая требует дальнейшего исследования, когда дело касается критически важного для безопасности периметра предприятия оборудования. Вопрос, «на кого работает ваш сетевой экран?», остается открытым.

А ты кто такой?

Тема киберпреступных операций, проводимых «под чужим флагом», и операций психологической войны представляет для нас особый интерес. Мы ожидаем активного развития угроз такого плана по нескольким направлениям.

Информационные войны

Такие киберпреступные группировки, как Lazarus и Sofacy, выступили пионерами создания фальшивых ресурсов для целевого слива информации и вымогательства. На протяжении нескольких месяцев мы наблюдали их деятельность, которая была в определенной степени успешной и привлекла к себе много внимания. Мы ожидаем, что в будущем информационные войны будут все чаще использоваться для манипулирования общественным мнением и создания хаоса вокруг общественных процессов. Киберпреступники мало что теряют, сливая информацию, полученную в результате своих действий, – для этого они создают легенду, используют известную или вновь созданную группу хакеров-активистов и перенаправляют внимание с самой атаки на содержание сливаемой информации.

Главную опасность в таких случаях представляет не сам факт взлома или нарушения конфиденциальности, а то, что журналисты и заинтересованные граждане привыкают принимать слитые данные как факты, заслуживающие доверия и освещения в прессе, и таким образом создают благоприятную среду для злоумышленников, стремящихся манипулировать общественным мнением за счет манипулирования данными или их выборочной публикации. Уязвимость к информационным войнам сейчас высока, как никогда, и мы надеемся, что по мере вовлечения в эту сферу новых (или старых, но сменивших маски) игроков потенциальные жертвы научатся вести себя осторожнее.

Как противостоять киберпреступникам

Кибератаки играют все более значимую роль в международных отношениях, и соответственно растет важность определения их источника (их атрибуции). Государственным органам предстоит решить непростую задачу – определить, какой уровень атрибуции будет достаточен для принятия решений о целесообразности дипломатических шагов или выдвижения публичных обвинений. Поскольку точная атрибуция практически невозможна ввиду фрагментированности информации, полученной от различных государственных и частных организаций, «приблизительная атрибуция» может быть принята как приемлемая в данном контексте. С одной стороны, в этом деле требуется крайняя осторожность, но с другой – необходимо, чтобы авторы кибератак почувствовали, что их действия чреваты последствиями для них же самих. При этом наше главное опасение состоит в том, что ответные меры способны вызвать еще более серьезные проблемы: хитрые киберпреступники могут обходить атрибуцию, ведя экспертов по ложному следу. Также нужно помнить, что по мере того как «ответные меры» будут набирать обороты, для проведения кибератак начнут широко использоваться вредоносные программы с открытым исходным кодом и продаваемые на коммерческой основе – такие как утилиты типа Cobalt Strike и Metasploit, использование которых позволяет киберпреступникам «скрыться в толпе» – возможность, отсутствующая при использовании проприетарных вредоносных программ.

«Чужие флаги»: повышение ставок

В отчете об операциях, проводимых «под чужим флагом», приводились случаи APT-атак «в дикой среде», использующих элементы мимикрии, но собственно операций «под чужим флагом» по сей день не наблюдалось. Под такой операцией мы понимаем действия, выполняемые злоумышленником А в полном соответствии со стилем злоумышленника Б и с использованием его ресурсов, с целью вызвать у жертвы ответные действия в отношении ни в чем не повинного злоумышленника Б. Действия такого рода будут иметь смысл только в том случае, если возмездие за кибератаку станет устоявшейся практикой. (При этом нельзя полностью исключать, что такие случаи уже имеют место, но пока неизвестны экспертам.) По мере того как ответные действия жертв кибератак (будь то зондирование, карательные меры или ответная эксплуатация компьютерных сетей) будут становиться более распространенными и импульсивными, можно ожидать появления собственно операций «под чужим флагом».

В этом случае можно прогнозировать, что киберпреступники будут готовы вкладывать еще больше ресурсов в операции «под чужим флагом» и, возможно, организовывать утечку данных об инфраструктуре и даже выкладывать во всеобщий доступ проприетарный набор инструментов, который сейчас ревниво охраняется. Таким образом ушлые киберпреступники могут спутать карты потенциальных жертв и экспертов по информационной безопасности, поскольку «скрипт-кидди», хакеры-активисты и киберпреступники получат доступ к проприетарным инструментам, принадлежащим продвинутой группе киберпреступников, что позволит сохранять анонимность при осуществлении значительной массы атак и отчасти подорвет возможности атрибуции для криминалистов и правоохранительных органов.

Какая еще конфиденциальность?

Ничего личного

Устранение последних остатков анонимности в киберпространстве чрезвычайно выгодно как рекламщикам, так и шпионам. Для первых ценным методом оказалось отслеживание активности пользователя с помощью постоянных cookie-файлов. Есть вероятность, что этот метод в будущем будет использоваться ещё шире, совмещаться с виджетами и прочими безобидными элементами на популярных веб-сайтах, что позволит компаниям отслеживать действия конкретных пользователей, в том числе за пределами доменов, принадлежащих этим компаниям, и таким образом получать связную картину поведения этих пользователей в интернете (к этой теме мы вернемся ниже).

В некоторых регионах будут развиваться удивительные по своей сложности методы отслеживания деятельности активистов и действий в соцсетях, которые «несут угрозу стабильности», а заинтересованные лица со средствами будут находить на редкость квалифицированные компании, о которых никто никогда не слышал, владеющие ноу-хау отслеживания деятельности диссидентов и активистов на просторах Сети. Такие лица зачастую проявляют большой интерес к отслеживанию тенденций в социальных сетях на уровне целых географических регионов и к тому, как голоса диссидентов влияют на настроения в целом. Нельзя исключить возникновение группировки киберпреступников, которая осмелится взломать какую-либо социальную сеть – неиссякаемый источник персональных данных пользователей и компромата на самых разных людей.

Шпионские рекламные сети

Среди повсеместно распространенных интернет-технологий рекламные сети больше всего подходят для использования при проведении целевых атак в полном смысле этого понятия. Рекламные сети – это по определению полностью коммерциализированные системы, и при этом их деятельность слабо регламентирована – иллюстрацией тому являются неоднократные случаи применения вредоносной рекламы на крупных веб-сайтах. В силу самой своей природы рекламные сети предоставляют отличные возможности профилирования потенциальных жертв путем отслеживания IP-адресов, сбора данных о браузере и системе пользователя, отслеживания предпочтений пользователя при интернет-навигации, а также путем идентификации пользователя по вводимым логинам. Использование таких данных позволяет атакующей стороне избирательно внедрять вредоносный контент в демонстрируемые пользователю страницы или перенаправлять отдельных пользователей на соответствующие их профилю вредоносные ресурсы, избегая таким образом использования «лишних» вредоносных программ и отказываясь от постоянной доступности в сети вредоносного контента, который так привлекает внимание экспертов по информационной безопасности. Мы ожидаем, что наиболее квалифицированные киберпреступники, специализирующиеся на кибершпионаже, придут к выводу, что создать рекламную сеть (или взять под контроль существующую) – это не слишком большое вложение, учитывая значительную потенциальную прибыль. Таким образом они смогут достичь своих целей, не подвергая риску свои новейшие наборы инструментов.

Выход на сцену хакеров-вигилантов

В 2015 году таинственный Финеас Фишер публикует дамп серверов HackingTeam, а затем он же выпускает пособие для начинающих хакеров по взлому нечистоплотных организаций и сомнительных компаний. Это вода на мельницу латентной веры в то, что асимметричная сила хакеров-вигилантов является силой добра – несмотря на тот факт, что в результате публикации дампа HackingTeam действующие APT-группировки бесплатно получили в свое распоряжение уязвимости нулевого дня. Не исключено также, что HackingTeam в результате слива получила новых клиентов, полных энтузиазма. По мере усиления вокруг избирательной кампании в США конспирологической риторики, основанной на убежденности в том, что утечка и слив данных – это способ склонить чашу информационных весов в определенную сторону, будет появляться все больше хакеров-вигилантов, взламывающих серверы ради получения дампов и организующих утечку данных в уязвимых организациях.

ПРОГРАММЫ-ВЫМОГАТЕЛИ: РЕВОЛЮЦИЯ

ВВЕДЕНИЕ

В 2016 году вредоносные программы-вымогатели продолжили завоевание мира, захватывая в плен данные и устройства как отдельных пользователей, так и целых компаний.

Цифры говорят сами за себя:

- Возникло 62 новых семейства программ-вымогателей.
- Количество новых модификаций вымогателей выросло в 11 раз — с 2900 в период с января по март до 32 091 в июле-сентябре.
- С января по конец сентября число атак на компании увеличилось в три раза: если в январе атаки проводились в среднем каждые две минуты, то в сентябре — уже каждые 40 секунд.
- Интенсивность атак на пользователей удвоилась: атаки проводились в среднем раз в 20 секунд в начале периода и раз в 10 секунд в его конце.
- Каждая пятая компания малого или среднего бизнеса, заплатившая выкуп, так и не получила доступ к своим данным.

В 2016 году наблюдался также рост сложности и разнообразия программ-вымогателей. Например, появились вымогатели, меняющие тактику при встрече с финансовым ПО; стало расти число вымогателей, написанных на скриптовых языках, вымогателей, использующих новые пути заражения, вымогателей, рассчитанных на отдельные группы пользователей, а также готовых решений типа «вымогатели как услуга» для тех, у кого недостаточно навыков, ресурсов или времени. Всё это происходит через расширяющуюся и всё более эффективную подпольную экосистему.

В то же время, в 2016 году в мире началось организованное противостояние вымогателям.

В июле был запущен проект No More Ransom, объединивший усилия Национальной полиции Нидерландов, Европола и компаний Intel Security и «Лаборатория Касперского»; в октябре к проекту присоединились ещё 13 организаций. Помимо прочих результатов, в рамках проекта в интернете было размещено несколько бесплатных утилит для расшифровки файлов; они уже помогли тысячам жертв восстановить данные, зашифрованные программами-вымогателями.

Наше сотрудничество в борьбе с программами-вымогателями только начинается, и многое ещё предстоит сделать. Вместе мы сможем добиться гораздо большего, чем каждый поодиночке.

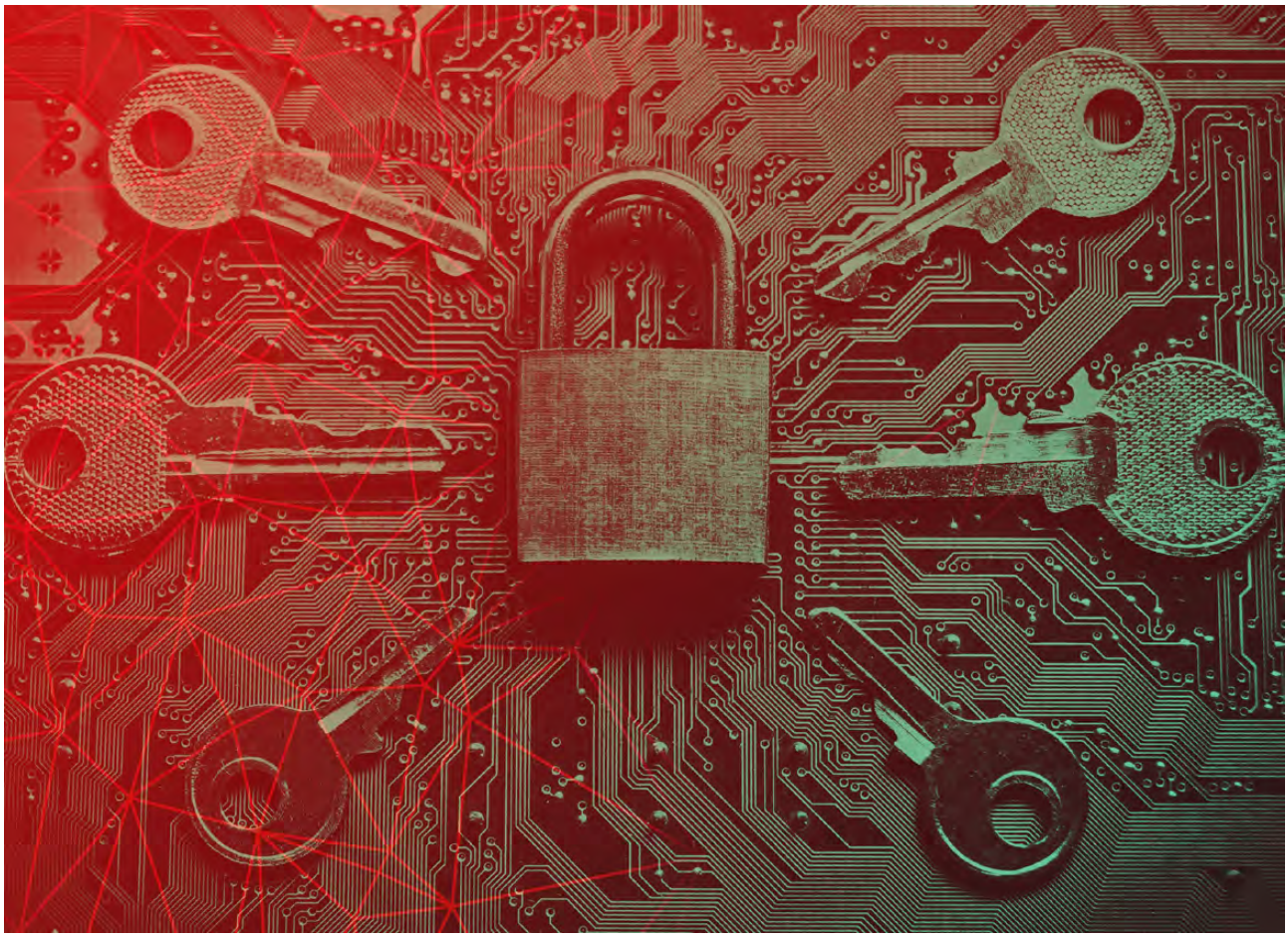
Что такое программы-вымогатели?

Программы-вымогатели бывают двух видов. Самый распространенный — это шифровальщики. Они зашифровывают данные на устройстве пользователя и требуют денег (выкуп), взамен обещая восстановить данные. В отличие от них блокировщики не изменяют данные, а блокируют доступ пользователя к устройству, на котором эти данные хранятся. Требование о выкупе демонстрируется на экране устройства и, как правило, маскируется под сообщение от правоохранительных органов о том, что пользователь получил доступ к незаконному веб-контенту и должен немедленно заплатить штраф. Обзор обоих типов программ-вымогателей доступен здесь.

ПРОГРАММЫ-ВЫМОГАТЕЛИ: ОСНОВНЫЕ ТЕНДЕНЦИИ И ОТКРЫТИЯ 2016 ГОДА

«В большинстве случаев успех вымогателей строится на специфических доверительных отношениях между жертвой и атакующей стороной, которые подразумевают, что после получения выкупа злоумышленник вернет жертве ее файлы. Как ни удивительно, киберпреступники до сих пор демонстрировали некое подобие профессионализма в исполнении этого негласного обещания».

GReAT, Прогноз развития угроз на 2017 г.



Новые и выбывшие игроки

Новые зловреды. В 2016 году увидели свет Cerber, Locky, CryptXXX и ещё 44 287 новых модификаций программ-вымогателей

На сегодняшний день вымогатель Locky распространился по

114

странам мира

Cerber и Locky появились в начале весны. Оба зловреда являются вымогателями, опасными и широко распространившимися – в основном через вложения к спам-сообщениям и наборы эксплойтов. Оба, «работая» как с частными пользователями, так и с корпоративным сектором, быстро утвердились в качестве крупных игроков. Несильно от них отстал и вымогатель CryptXXX. Все три семейства продолжают развиваться, требуя выкуп за зашифрованные данные у пользователей по всему миру, наравне с такими известными вымогателями, как CTB-Locker, CryptoWall и Shade.

Наиболее распространенные семейства программ-вымогателей, детектируемые продуктами «Лаборатории Касперского», по состоянию на октябрь 2016 года:

	Название	Вердикты*	Доля пользователей**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32%
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07%
3	TeslaCrypt (был активен до мая 2016 г.)	Trojan-Ransom.Win32.Bitman	6,54%
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85%
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79%
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36%
7	Shade	Trojan-Ransom.Win32.Shade	1,73%
8	(Generic-вердикт)	Trojan-Ransom.Win32.Snocry	1,26%
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15%
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90%

* Детектирующие вердикты продуктов «Лаборатории Касперского». Информация получена от пользователей продуктов «Лаборатории Касперского», давших свое согласие на передачу статистических данных.

** Процент пользователей, атакованных данным семейством шифровальщиков-вымогателей, от числа всех пользователей, атакованных шифровальщиками-вымогателями.

Выбывшие игроки – Teslascrypt, Chimera, Wildfire: не спеши говорить «до свиданья»...

Пожалуй, самой большой неожиданностью 2016 года стало отключение троянца-вымогателя TeslaCrypt и последующая публикация мастер-ключа к нему – видимо, самими владельцами зловреда.

TeslaCrypt «покончил с собой», а Encryptor RaaS и Wildfire были отключены полицией

Encryptor RaaS, один из первых троянцев, предлагавшихся вирусописателями другим киберпреступникам в рамках модели Ransomware-as-a-Service (вымогатель как услуга), прекратил свою активность после того, как полиция отключила часть его ботнета.

Затем, в июле некто, якобы имевший отношение к шифровальщику Petya/Mischa, опубликовал около 3500 ключей к вымогателю Chimera. Учитывая, что часть исходного кода Chimera была использована в Petya, вполне может быть, что за этими двумя вымогателями стоит одна и та же группировка, которая просто решила обновить свою продуктовую линейку и заодно покуражиться.

Похожая история произошла с вымогателем Wildfire — его командные серверы были отключены, а совместными усилиями «Лаборатории Касперского», Intel Security и Европола был создан ключ расшифровки. Однако теперь вымогатель, судя по всему, возродился под именем Hades.

«Учебные» вымогатели на службе у киберпреступников

Исследователи, действовавшие из лучших побуждений, создали «учебные» программы-вымогатели, чтобы дать системным администраторам инструмент моделирования атак с применением такого вредоносного ПО для целей тестирования защитных систем. Киберпреступники быстро приспособили эти инструменты для своих криминальных целей.

Из программ-вымогателей, созданных в «образовательных» целях, возникли, в частности, такие зловреды как Ded Cryptor и Fantom

Разработчик «учебного» вымогателя Hidden Tear & EDA2 из лучших побуждений опубликовал его исходный код на веб-сервисе GitHub. Не удивительно, что в 2016 году появилось множество троянцев, созданных на основе этого кода, в том числе вымогатель Ded Cryptor, который менял фон рабочего стола на зараженном компьютере на картинку со злобным Санта-Клаусом и требовал выкуп размером в два биткойна (около 1300$). Другой такой программой был Fantom, который маскировался под обновление Windows и показывал экран обновления, очень похожий на настоящий.

Нестандартные подходы

Злоумышленники теперь нацелились на резервные копии и жесткие диски, а также на подбор паролей

- **Зачем возиться с файлом, если можно зашифровать сразу весь диск?**

  В 2016 году возник такой новый подход в работе программ-вымогателей, как шифрование диска: эти зловреды блокируют доступ к диску или шифруют сразу все файлы на нем. В качестве примера можно привести троянскую программу Petya, которая шифрует главную файловую таблицу (master file table, MFT) жесткого диска и делает невозможной нормальную перезагрузку компьютера. Другой троянец, Dcryptor, также известный как Mamba, пошел еще на шаг дальше – он блокирует сразу весь жесткий диск. Это особенно неприятный вымогатель — он шифрует каждый сектор диска, включая операционную систему, приложения, файлы совместного использования и все личные данные, с помощью программы с открытым исходным кодом DiskCryptor.

- **Метод «ручного» заражения**

  Заражение троянцем Dcryptor происходит вручную — злоумышленники подбирают пароли, чтобы получить удаленный доступ к компьютеру-жертве. Подход не нов, но стал значительно более популярен в 2016 году; он часто используется для проведения атак на серверы и последующего проникновения в корпоративную сеть.

  В случае успешной атаки троянец устанавливается на сервере и шифрует файлы, которые хранятся на нем и, в некоторых случаях, на всех доступных с этого сервера сетевых ресурсах. Мы обнаружили, что данный подход применяется в троянце TeamXRat — с его помощью бразильские киберпреступники заражают программой-вымогателем бразильские сервера.

Обнаружив на компьютере финансовое ПО, Shade скачивал на него шпионскую программу

- **Заражение «два-в-одном»**

  В августе мы обнаружили образец Shade, у которого был неожиданный функционал: в случае, если зараженный компьютер имел отношение к департаменту финансов, троянец вместо стандартного шифрования файлов скачивал и устанавливал шпионскую программу, вероятно с более долгосрочной целью кражи денежных средств.

Вымогатели на скриптовых языках

Ещё один тренд 2016 года, на который мы обратили внимание, — это рост числа шифровальщиков, написанных на скриптовых языках. Только в третьем квартале мы обнаружили несколько новых семейств троянцев-вымогателей, написанных на Python, в их числе HolyCrypt и CryPy, а также Stampado, который написан на AutoIt — языке для автоматизации выполнения задач.

Армия киберпреступников-любителей и плагиаторов

Если программа-вымогатель плохого качества, то это увеличивает вероятность безвозвратной утери данных

Многие троянцы-вымогатели, впервые обнаруженные в 2016 году, оказались низкого качества — незамысловатые, с ошибками в коде и банальными описками в текстах требования выкупа.

Кроме того, мы заметили, что создатели программ-вымогателей копируют друг друга. В частности, мы обнаружили следующее:

- Троянец Bart копирует текст требования выкупа и стиль страницы уплаты выкупа у Locky.
- Написанный на AutoIt троянец-вымогатель, копирующий Locky (он получил название AutoLocky) использует то же расширение для зашифрованных файлов – ".locky".
- Crusis (он же Crysis) использует расширение ".xtbl", позаимствованное у Shade.
- Xorist полностью копирует схему именования зашифрованных файлов, используемую Crusis.

Из всех творений плагиаторов, обнаруженных в этом году, пальму первенства мы присуждаем Polyglot (он же MarsJoke). Этот троянец полностью копирует внешний вид CTB-Locker и его подход к обработке файлов.

Мы ожидаем, что все эти тенденции получат свое развитие в 2017 году.

«Программы-вымогатели становятся все более притягательными, привлекая менее квалифицированные слои киберпреступников. В результате в будущем мы будем все чаще сталкиваться с программами-вымогателями, за которыми стоят киберпреступники, не выполняющие вышеописанное молчаливое соглашение — из-за ошибок в коде или в силу того, что функционал восстановления файлов в программе просто не реализован. Мы ожидаем появления программ-вымогателей, созданных так называемыми «скрипт-кидди» (начинающими хакерами), которые будут блокировать файлы или доступ к системе или будут просто удалять файлы, обманным путем заставляя жертв платить, но при этом не возвращая им доступ к файлам».

GReAT, Прогноз развития угроз на 2017 г.

ПРОЦВЕТАЮЩАЯ ЭКОНОМИКА, ОСНОВАННАЯ НА ТРОЯНЦАХ-ШИФРОВАЛЬЩИКАХ

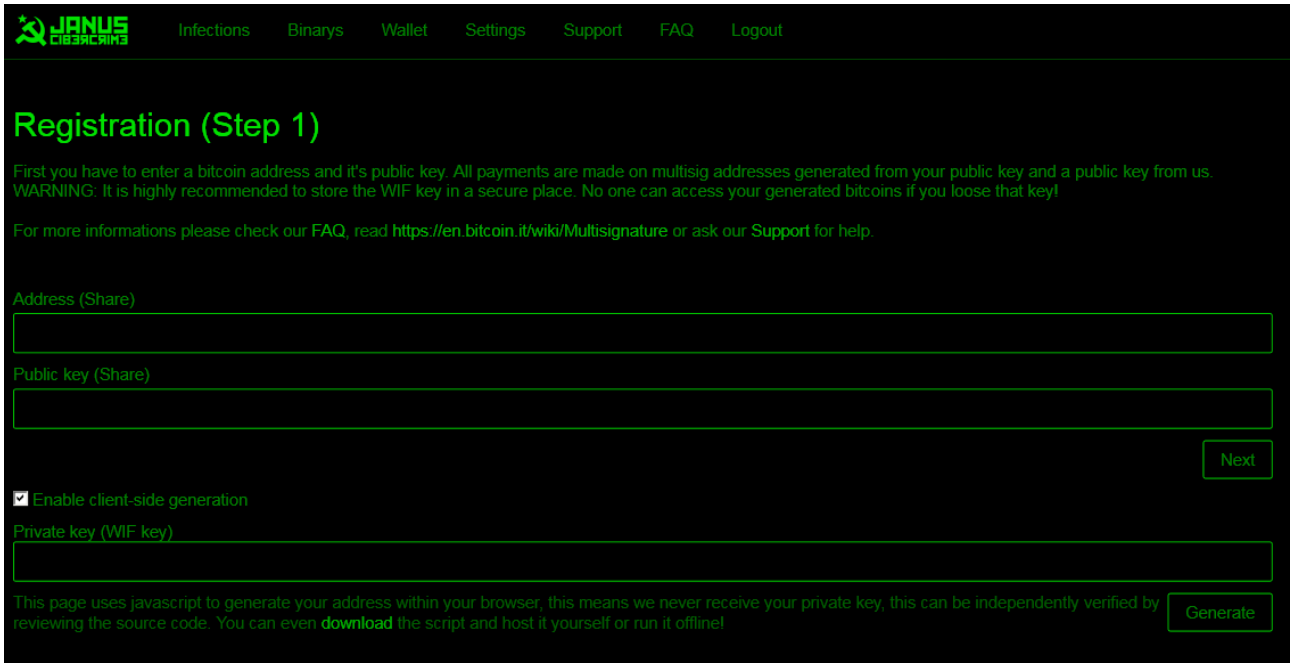
Программы-вымогатели все чаще сдаются в аренду на криминальном рынке

Рост популярности RaaS

Модель «Вымогатель как услуга» (Ransomware-as-a-Service, RaaS) — это не новое явление, но в 2016 году эта схема распространения программ-вымогателей продолжала совершенствоваться, и все больше вирусописателей предлагали свой вредоносный продукт «по требованию». Такой подход оказался чрезвычайно популярным среди злоумышленников, которым не хватает специальных навыков, ресурсов или желания создавать собственное вредоносное ПО.

Характерными примерами программ-вымогателей, появившихся в 2016 году и использующих эту модель, являются троянцы Petya/Mischa и Shark, который после «ребрендинга» получил имя Atom.

Эта бизнес-модель постоянно развивается и усложняется:



Партнерский сайт программы-вымогателя Petya

Для партнеров часто действует стандартная схема, основанная на комиссионном вознаграждении. Например, из «таблицы выплат» за распространение троянца Petya видно, что если продажи партнера составляют 125 биткойнов в неделю, то его недельный заработок составит 106,25 биткойнов.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Таблица выплат за распространение троянца Petya

Существует также первоначальный взнос за использование программ-вымогателей. Например, тому, кто хочет воспользоваться шифровальщиком Stompado, нужно заплатить всего $39.

Учитывая, что другие киберпреступники предлагают услуги в области распространения спама, создания требований о выкупе и т.д., начинающему злоумышленнику достаточно легко вступить в игру.

От партнерских сетей с комиссионным вознаграждением до клиентской поддержки и брендинга

Преступники предлагают клиентскую поддержку, чтобы обеспечить максимальный процент оплаты выкупа жертвами

Наиболее «профессиональные» киберпреступники предлагали своим жертвам консультационную и техническую поддержку, помогая им приобрести биткойны для уплаты выкупа, а иногда даже вступали в переговоры с ними. При этом каждый их шаг подталкивал жертву к тому, чтобы заплатить выкуп.

Кроме того, специалисты «Лаборатории Касперского», изучая программы-вымогатели в Бразилии, заметили, что во многих атаках достаточно большое значение придавалось брендингу. Те, кто стремился привлечь внимание средств массовой информации и напугать клиентов, активно использовали резонансные события, имена известных людей или рекламные приёмы. Те же, кто предпочитал оставаться незамеченными, отказывались от искушения прославиться и оставляли своих жертв один на один с адресами электронной почты для связи со злоумышленниками и реквизитами для внесения биткойнов.

Биткойны по-прежнему в чести

В течение всего 2016 года наиболее популярные семейства программ-шифровальщиков по-прежнему требовали оплату в биткойнах. В основном суммы выкупа были умеренными, в среднем около $300, но некоторые киберпреступники требовали (и получали!) гораздо больше.

Другие группировки, в основном те, чьи кампании имели региональную направленность или управлялись в ручном режиме, зачастую предпочитали локальные варианты оплаты, хотя это лишало их возможности растворяться в толпе себе подобных, смешавшись с остальными группировками, использующими программы-вымогатели.

БИЗНЕС НА ПРИЦЕЛЕ У ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Программы-вымогатели атакуют компании каждые 40 секунд

В первом квартале 2016 года 17% атак с применением программ-вымогателей были направлены против корпоративного сектора — другими словами, в среднем во всем мире проводилось по одной атаке на ту или иную компанию каждые две минуты*. К концу третьего квартала эта доля выросла до 23,9% — в среднем одной атаки каждые 40 секунд.

По данным исследования «Лаборатории Касперского», в 2016 году каждая пятая компания по всему миру столкнулась как минимум с одним инцидентом IT-безопасности в результате атак с применением программы-вымогателя.

- 42% предприятий малого и среднего бизнеса испытали на себе атаки с применением программ-вымогателей за последние 12 месяцев.
- 32% атакованных компаний заплатили выкуп.
- Каждая пятая компания не сумела восстановить свои файлы даже после оплаты.
- 67% жертв программ-вымогателей полностью или частично потеряли свои корпоративные данные, причем у каждой четвертой жертвы на попытки восстановления доступа к данным ушло несколько недель.

* Оценка основана на следующем расчете: 17% от 372 602 уникальных пользователей, атаки программ-вымогателей на которых были заблокированы продуктами «Лаборатории Касперского» в течение первого квартала 2016 года, и 23,9% от 821 865 уникальных пользователей, атаки программ-вымогателей на которых были заблокированы продуктами «Лаборатории Касперского» в течение третьего квартала 2016 года

Каждой пятой компании малого и среднего бизнеса не удается вернуть свои данные даже после оплаты выкупа

Отраслей, мало подверженных риску, больше не осталось

Ключевыми факторами уязвимости компаний остаются социальная инженерия и человеческий фактор. Каждый пятый случай потери важных данных при атаках программ-вымогателей стал результатом неосторожности или неосведомленности сотрудников.

Некоторые отрасли страдают сильнее, чем другие, однако наши исследования показывают, что в зоне риска находятся все.

	Отрасль	% организаций, атакованных программами-вымогателями
1	Образование	23
2	Информационные технологии/ телекоммуникации	22
3	Развлечения/СМИ	21
4	Финансы	21
5	Строительство	19
6	Правительство/государственный сектор/ оборона	18
7	Производство	18
8	Транспорт	17
9	Здравоохранение	16
10	Розничная/оптовая торговля/досуг	16

«Мы обнаруживаем все больше целевых атак с применением программ-вымогателей: киберпреступные группировки тщательно отбирают жертв и атакуют их целевыми фишинговыми рассылками, ориентируясь на то, какие данные у них есть и/или насколько сильно они зависят от доступности этих ценных данных».

Джон Фоккер, Координатор группы по борьбе с киберпреступлениями, Национальное управление Нидерландов по противодействию преступлениям в области высоких технологий

Наиболее значительные атаки программ-вымогателей в 2016 году

- **Больницы стали популярными мишенями.** В результате операции отменялись, пациентов переводили в другие больницы и т.д., но последствия могли быть гораздо более серьезными.
  - Наиболее резонансная атака с использованием программ-вымогателей произошла в марте. Преступники заблокировали компьютеры медицинского центра Hollywood Presbyterian в Лос-Анжелесе и разблокировали их только после того, как получили выкуп в сумме $17 000.
  - Через несколько недель после этого инцидента атакам подверглись несколько больниц в Германии.
  - 28 учреждений национальной службы здравоохранения Великобритании сообщили о том, что стали жертвами атак в 2016 году.
- В сентябре **хостинг-провайдер виртуальных рабочих столов и облачных сервисов VESK** выплатил почти $23 000 в качестве выкупа, чтобы вернуть доступ к одной из своих систем
- В марте 2016 года **ведущие СМИ**, в том числе New York Times, BBC и AOL, подверглись атакам с использованием программ-вымогателей.
- Крупнейший исследовательский центр — **Университет города Калгари в Канаде** — признал, что заплатил около $16 000 за восстановление электронных писем, которые были зашифрованы и оставались недоступными в течение недели.
- **Небольшой полицейский участок в штате Массачусетс** вынужден был выплатить $500 выкупа (в биткойнах) за то, чтобы вернуть важные данные по расследуемым делам. Данные были зашифрованы программой-вымогателем после того, как один из сотрудников открыл вредоносное вложение в почте.
- **Под ударом оказался даже автоспорт**: в апреле одна из ведущих гоночных команд NASCAR рассталась с данными, стоимость которых оценивается в несколько миллионов долларов, после атаки программы-вымогателя TeslaCrypt.

ОТПОР ВЫМОГАТЕЛЯМ

Через применение технологий

Новейшие версии продуктов «Лаборатории Касперского» для небольших компаний были усилены функционалом для противодействия вредоносным программам-шифровальщикам. Кроме того, была выпущена новая бесплатная утилита для борьбы с программами-вымогателями, которую может загрузить и применить любая компания, независимо от того, какое защитное решение она использует.

Доступна новая бесплатная утилита для защиты от программ-вымогателей, совместимая с любыми антивирусными решениями

Утилита Kaspersky Anti-Ransomware Tool for Business — это «легкое» решение, которое может функционировать параллельно с другим антивирусным ПО. Утилита использует два компонента, необходимых для раннего обнаружения троянских программ, а именно распределенную облачную сеть Kaspersky Security Network и модуль Мониторинг активности, который отслеживает активность приложений.

Kaspersky Security Network быстро проверяет репутацию файлов и URL-адресов по облачной базе, а Мониторинг активности отслеживает поведение программ и обеспечивает проактивную защиту от не известных на данный момент версий троянцев. Особенно важно, что утилита может создавать резервные копии файлов, открываемых подозрительными приложениями, и осуществлять откат изменений, если действия программ будут признаны вредоносными.

Через сотрудничество: инициатива «No More Ransom»

На сегодняшний день в рамках проекта «No More Ransom» свыше 4400 пользователей смогли восстановить свои данные, а киберпреступники недополучили выкуп на сумму 1,5 миллиона долларов

25 июля 2016 года Национальная полиция Нидерландов, Европол и компании Intel Security и «Лаборатория Касперского» объявили о запуске инициативы «No More Ransom». Это некоммерческий проект, объединяющий государственные и частные организации с целью информировать людей об опасности программ-вымогателей и помогать им в восстановлении заблокированных данных.

В настоящее время на интернет-портале доступны восемь утилит для дешифровки файлов, пять из которых созданы «Лабораторией Касперского». Они позволяют восстанавливать файлы, зашифрованные более чем двадцатью типами вредоносных программ-шифровальщиков. На сегодняшний день свыше 4400 пользователей сумели восстановить свои данные, сэкономив более 1,5 миллиона долларов в результате отказа от выплаты выкупа.

В октябре к проекту присоединились правоохранительные органы еще 13 стран, включая Боснию и Герцеговину, Болгарию, Колумбию, Францию, Венгрию, Ирландию, Италию, Латвию, Литву, Португалию, Испанию, Швейцарию и Великобританию.

Евроюст и Европейская комиссия также поддерживают цели и задачи проекта. Ожидается, что в ближайшее время будет объявлено о присоединении к проекту новых партнеров — частных организаций и правоохранительных органов разных стран.

«Государственно-частное партнерство — это суть и сила инициативы «No More Ransom». Оно имеет принципиальное значение для эффективного и действенного решения проблемы, обеспечивая значительно более широкие возможности и охват, чем если бы правоохранительные органы действовали в одиночку».

Стивен Уилсон,
глава Европейского центра по борьбе
с киберпреступностью Европола

Как дать отпор вымогателям и обеспечить свою безопасность

1. Регулярно создавайте резервные копии данных.
2. Используйте надежное защитное решение. Следите за тем, чтобы основные его функции, такие как Мониторинг активности, были всегда включены.
3. Вовремя обновляйте ПО на всех своих устройствах.
4. Будьте осторожны с почтовыми вложениями и письмами от незнакомых людей. Если сомневаетесь, не открывайте их.
5. Если вы представляете компанию, вам необходимо также обучать ваших сотрудников и IT-специалистов. Храните конфиденциальную информацию отдельно от остальных данных, ограничивайте доступ к ней. Кроме того, у вас всегда должны быть резервные копии всех ваших данных.
6. Если вам не повезло и вы стали жертвой программы-шифровальщика, не паникуйте. Зайдите на наш сайт No More Ransom с незараженного компьютера — не исключено, что там найдется утилита, которая позволит вам расшифровать ваши данные.
7. И наконец, не забывайте, что применение вредоносных программ-вымогателей — это уголовное преступление. Обязательно заявляйте о таких случаях в правоохранительные органы.

**«Мы убедительно просим пользователей сообщать об атаках: каждый из потерпевших обладает важными уликами, которые могут серьезно помочь нам анализе проблемы. Мы, со своей стороны, готовы информировать этих пользователей о положении дел и защищать их от сомнительных сторонних «предложений» о расшифровке данных.
В то же время нужно повышать осведомленность правоохранительных органов и их готовность бороться с киберпреступлениями».**

Тон Маас, Координатор группы по борьбе с киберпреступлениями, Национальное управление Нидерландов по противодействию преступлениям в области высоких технологий

Почему не следует платить выкуп — рекомендации Национального управления Нидерландов по противодействию преступлениям в области высоких технологий

1. Заплатив, вы станете более привлекательной жертвой для киберпреступников.
2. Нельзя доверять киберпреступникам — нет никаких гарантий, что вы сможете восстановить свои данные, даже если заплатите выкуп.
3. В следующий раз размер выкупа для вас будет выше.
4. Платить — значит поощрять киберпреступников.

ВОЗМОЖНО ЛИ ПОБЕДИТЬ В БОРЬБЕ С ПРОГРАММАМИ-ВЫМОГАТЕЛЯМИ?

Да, мы считаем, что это возможно, но только объединив усилия. Программы-вымогатели — это прибыльный криминальный бизнес. Чтобы остановить его, нам всем необходимо объединиться, разрушить сложившиеся криминальные схемы и сделать так, чтобы киберпреступникам было все труднее проводить свои атаки и получать от них прибыль.

РАЗВИТИЕ УГРОЗ

ЦЕЛЕВЫЕ АТАКИ

В наши дни целевые атаки стали неотъемлемой частью ландшафта угроз, и неудивительно, что им посвящен специальный раздел в нашем годовом отчете.

Представляем обзор крупных APT-кампаний, которые произошли в этом году.

BlackEnergy

За одну массированную атаку BlackEnergy было выведено из строя энергоснабжение, удалено ПО и запущена DDoS-атака

Год начался с кибератаки BlackEnergy на предприятия энергетического сектора Украины. Атака стала уникальной по масштабам причиненного вреда: хакерам удалось отключить системы распределения электроэнергии на Западной Украине, запустить в атакованные системы программу Wiper для удаления содержимого зараженных компьютеров и провести телефонную DDoS-атаку на службы техподдержки атакованных компаний. «Лаборатория Касперского» раскрыла ряд аспектов деятельности ответственной за атаку группировки, опубликовав, в частности, анализ механизма, использованного для проникновения в системы. Общий обзор атаки доступен в отчете американского SANS Institute, подготовленного вместе с ICS-CERT.

Операция «Blockbuster»

«Лаборатория Касперского» стала одним из участников операции «Blockbuster» — совместного исследования деятельности Lazarus Group, проведенного несколькими крупными компаниями — лидерами в области кибербезопасности (отчет «Лаборатории Касперского» можно прочитать здесь). Lazarus — это киберпреступная группировка предположительно северокорейского происхождения, ответственная за атаку на Sony Pictures в 2014 году. Lazarus Group известна с 2009 года, а с 2011 года она заметно активизировалась. Группа ответственна за такие известные атаки, как Troy, Dark Seoul (Wiper), WildPositron. Мишенями группировки были предприятия, финансовые организации, радио и телевидение.

Adwind

У «зловреда напрокат» Adwind было 1 800 клиентов

В феврале, на форуме Security Analyst Summit мы представили результаты расследования деятельности Adwind — кроссплатформенного многофункционального троянца, используемого как инструмент удаленного доступа (Remote Access Tool) и распространяемого через единый сервис «зловред как услуга». Со времени своего первого выпуска в 2012 г., троянец носил разные имена: AlienSpy, Frutas, Unrecom, Sockrat, JSocket, jRat. Мы полагаем, что в период с 2013 по 2016 год этот троянец использовался при проведении атак более чем на 443 000 частных пользователей, коммерческих и некоммерческих организаций по всему миру. Одно из главных отличий Adwind от прочих коммерческих вредоносных программ — то, что он распространяется открыто как платный сервис — клиент платит определенную сумму в обмен за использование вредоносной программы. По нашим оценкам, к концу 2015 года в системе было около 1 800 клиентов. Таким образом, Adwind на сегодняшний момент является одной из самых больших вредоносных платформ.

Атаки с участием эксплойтов к уязвимости CVE-2015-2545

В мае мы сообщили о наблюдаемой волне кибершпионских атак, проводимых различными APT-группировками в Азиатско-Тихоокеанском и Дальневосточном регионах. У всех этих атак была одна общая черта: они эксплуатировали уязвимость CVE-2015-2545. Эта уязвимость позволяет атакующей стороне исполнять произвольный код при помощи специально созданного графического файла с расширением EPS, при этом используется язык PostScript и обходятся встроенные в ОС Windows методы защиты Address Space Layout Randomization и Data Execution Prevention. Уже было известно, что эту уязвимость эксплуатируют группировки Platinum, APT16, EvilPost и SPIVY, а недавно добавились еще и группы Danti и SVCMONDR. Обзор APT-группировок, эксплуатирующих эту уязвимость, доступен здесь.

Уязвимость, закрытую ещё в 2015 году, эксплуатировало более шести APT-группировок

Самой поразительной чертой этих атак является то, что они с успехом эксплуатируют уязвимость, патч к которой компания Microsoft выпустила в сентябре 2015 г. В прогнозах на 2016 год мы прогнозировали, что APT-кампании станут прилагать меньше усилий для разработки сложных инструментов и будут чаще использовать для своих целей готовое вредоносное ПО. Вышеописанный случай является хорошим примером: используется известная уязвимость, а не разрабатывается эксплойт к уязвимости нулевого дня.

Это говорит о том, что компаниям следует уделять больше внимания своевременной установке исправлений безопасности, чтобы обеспечить защиту корпоративной IT-инфраструктуры.

Операция Daybreak

В кампании кибершпионажа «Операция Daybreak», организованной группировкой ScarCruft, была использована неизвестная на тот момент уязвимость — CVE-2016-1010

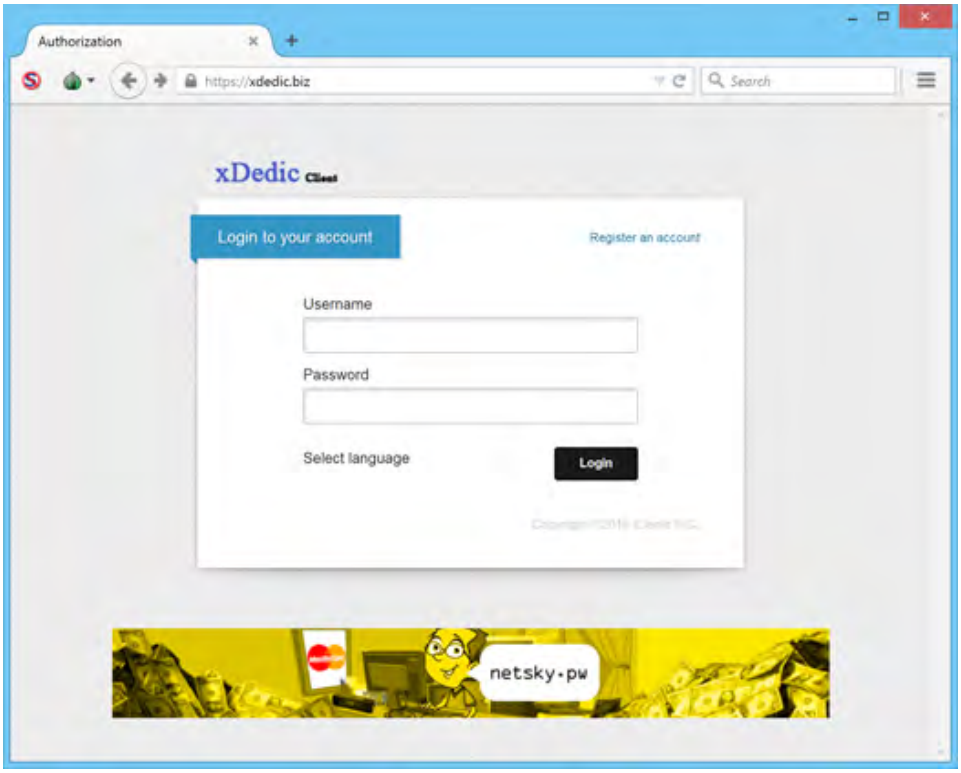
Естественно, всегда найдется и APT-группировка, стремящаяся воспользоваться эксплойтами нулевого дня. В июне мы сообщали о кампании кибершпионажа, получившей кодовое название «Операция Daybreak» («Рассвет»), запущенной группировкой под названием ScarCruft и использующей ранее неизвестный эксплойт к Adobe Flash Player (уязвимость CVE-2016-1010). Это относительно новая группировка, до сих пор она не привлекала особого внимания. Мы полагаем, что ранее эта группировка могла запустить еще один эксплойт нулевого дня (CVE-2016-0147) — эта уязвимость была закрыта в апреле. Среди ее жертв — правоохранительные органы одной из азиатских стран, одна из крупнейших мировых торговых компаний, американская компания по мобильной рекламе и монетизации приложений, частные лица, связанные с Международной ассоциацией легкоатлетических федераций и ресторан, расположенный в одном из крупнейших торговых центров Дубая.

Стопроцентной безопасности не бывает, но можно усилить линию безопасности настолько, что для атакующих злоумышленников станет слишком дорого пробивать в ней брешь, так что они откажутся от своих намерений или выберут другую цель. Лучший метод защиты от целевых атак — это следовать комплексному подходу, который сочетает традиционные антивирусные технологии с хостовыми системами предотвращения вторжений, запретом по умолчанию на основе белых списков и управлением исправлениями. По данным исследования австралийского Управления радиотехнической обороны, 85% проанализированных целевых атак могут быть остановлены с применением четырех стратегий: белые списки приложений, обновлений приложений, обновление операционных систем и ограничение административных прав.

xDedic

xDedic был торговой площадкой, на которой были выставлены данные минимум 70 000 взломанных серверов. Большая часть жертв ничего об этом не знали

В этом году «Лаборатория Касперского» исследовала кибер-преступную торговую площадку под названием xDedic — черный онлайн-рынок учетных данных взломанных серверов, расположенных по всему миру, каждый из которых доступен по протоколу Remote Desktop Protocol (RDP). Поначалу мы полагали, что на рынке представлено около 70 000 серверов, но новые данные заставляют предположить, что xDedic гораздо больше и содержит учетные данные 176 000 серверов. На площадке есть своя поисковая система, так что потенциальные покупатели могут выбрать практически любой сервер на свой вкус, включая серверы в государственных и корпоративных сетях, и все это всего за 8 долларов за сервер! За эту цену покупатели получают доступ к данным о взломанных серверах и могут использовать сами серверы как плацдарм для осуществления целевых атак.



Черные рынки — явление не новое; однако в данном случае мы видим более высокий уровень специализации. Хотя модель, взятую на вооружение владельцами XDedic, не так просто будет воспроизвести, мы полагаем, что в будущем есть вероятность возникновения других специализированных рыночных площадок.

Dropping Elephant

Группировка Dropping Elephant показала, насколько опасной может быть тщательно продуманная социальная инженерия

Целевые атаки не обязательно должны быть технически сложными, чтобы увенчаться успехом. В июле мы сообщили о группировке Dropping Elephant (известной также под названиями Chinastrats и Patchwork). Используя социальную инженерию в сочетании со старым кодом эксплойтов и несколькими вредоносными программами на базе PowerShell, группировка успешно крала конфиденциальные данные у влиятельных организаций, работающих в дипломатической и экономической сфере и связанные с внешнеполитическими отношениями Китая. При проведении атак использовалось сочетание целевого фишинга и атак типа watering hole. В успехе группировки Dropping Elephant примечательно то, что ей удавалось взламывать системы влиятельных жертв без использования эксплойтов нулевого дня или сложных технических приемов. Dropping Elephant — это еще один пример того, что применение готового набора инструментов при низком уровне инвестиций может быть чрезвычайно эффективным в сочетании с тщательно продуманной социальной инженерией.

Подобным атакам можно противостоять, своевременно устанавливая обновления безопасности и повышая уровень информированности сотрудников в области информационной безопасности.

Operation Ghoul

Атаки Operation Ghoul подтвердили эффективность точечного фишинга в сочетании с использованием коммерческих вредоносных программ

Серия атак, за которыми стояла группировка Operation Ghoul — мы сообщали о них в июне 2016 г., — явилась еще одним примером того, насколько успешными могут оказаться методы социальной инженерии в руках киберпреступников, стремящихся проникнуть в сеть атакуемой организации и закрепиться в ней. В ходе этой операции киберпреступники рассылали фишинговые сообщения с вредоносными вложениями преимущественно руководителям и менеджерам среднего звена из множества компаний; сообщения выглядели так, как будто они были отправлены банком из ОАЭ. В сообщение, которое якобы содержало платежное извещение банка, был вложен документ SWIFT. Однако в действительности архив содержал вредоносное ПО. По информации, полученной с sinkhole-серверов, на которые были переключены некоторые из командных серверов группировки, большинство этих организаций задействованы в сфере промышленного производства и машиностроения. Кроме того, среди мишеней были логистические, фармацевтические, производственные, торговые и образовательные организации.

Вредоносное ПО, применяемое группировкой Operation Ghoul, основано на коммерческом пакете шпионского ПО Hawkeye, которое открыто продается на подпольных сайтах (Dark Web). После установки вредоносное ПО собирает с компьютеров жертв интересующие злоумышленников данные, включая нажатия клавиш, содержимое буфера обмена, учетные данные аккаунтов на FTP-серверах, данные учетных записей из браузеров, систем обмена сообщениями и почтовых клиентов, а также информацию об установленных приложениях.

Тот факт, что социальная инженерия по-прежнему успешно применяется злоумышленниками для проникновения в сети атакуемых организаций, означает, что обучение сотрудников и повышение их информированности об угрозах должно стать центральным элементом стратегии обеспечения безопасности компании.

ProjectSauron

В сентябре решение «Лаборатории Касперского» Anti-Targeted Attack Platform обнаружило аномальные явления в сети одного из корпоративных клиентов компании. В результате анализа данного инцидента была обнаружена кибергруппировка ProjectSauron, которая занималась кражей конфиденциальных данных у организаций в России, Иране, Руанде и, возможно, в других странах с июня 2011 года.

Группировка ProjectSauron навсегда изменила ландшафт угроз, создав продвинутую модульную платформу для ведения кибершпионажа с уникальным набором инструментов для каждой отдельной жертвы

Нам удалось идентифицировать более 30 жертв. Все эти организации выполняют ключевые государственные функции и относятся к правительственным и финансовым структурам, вооруженным силам, научно-исследовательской сфере и телекоммуникациям. Затратность проекта, его сложность, упорство злоумышленников и конечная цель (кража секретных данных у близких к государству организаций) указывают на то, что ProjectSauron — кампания, поддерживаемая на государственном уровне. Судя по техническим характеристикам проводимых атак, эта группа злоумышленников целенаправленно перенимает опыт других сложных атак, включая Duqu, Flame, Equation и Regin, берет на вооружение их наиболее инновационные методы и совершенствует их тактику, чтобы избежать обнаружения. Все вредоносные артефакты создаются индивидуально для каждой жертвы, что снижает их значимость как индикаторов заражения любой другой жертвы.

Вот основные факты о ProjectSauron:

1. ProjectSauron — модульная платформа, разработанная для осуществления длительных кампаний кибершпионажа.
2. Во всех модулях и сетевых протоколах используются сильные алгоритмы шифрования, такие как RC6, RC5, RC4, AES, Salsa20 и др.
3. Для управления свои модулями и плагинами платформа использует модифицированный интерпретатор Lua.
4. В качестве расширения базового функционала в платформе предусмотрено более 50 различных типов плагинов.
5. Те, кто стоит за ProjectSauron, проявляют большой интерес к программам шифрования для коммуникационных каналов, которыми пользуются государственные организации — они похищают ключи шифрования, конфигурационные файлы и IP-адреса ключевых серверов, имеющих отношение к ПО для шифрования.
6. Атакующие могут извлекать данные из не подключенных к интернету сетей при помощи специально подготовленных USB-носителей, размещая украденную информацию в их скрытой области, недоступной стандартным средствам операционной системы.

7. Платформа активно использует протокол DNS для извлечения данных и передачи информации о статусе атаки в режиме реального времени.
8. APT-кампания активна по меньшей мере с июня 2011 года и оставалась актуальной угрозой до апреля 2016 г.
9. Изначальный вектор заражения остается неизвестным.
10. Атакующие используют каналы распространения легитимного ПО для распространения внутри зараженной сети.

Новым является однократное использование уникальных ресурсов, таких как командный сервер, ключи шифрования и т.д., в сочетании с самыми современными методами, перенятыми у других крупнейших киберпреступных группировок.

Единственный эффективный способ противостоять подобным угрозам — создать многоуровневую систему безопасности с сенсорами, способными обнаружить малейшие аномалии в цифровом документообороте организации, в сочетании с оперативным получением сведений об актуальных угрозах и проведением криминалистического анализа. Дополнительную информацию о методах, с помощью которых можно противостоять подобным угрозам, можно найти здесь.

ФИНАНСОВЫЕ УГРОЗЫ

Для киберпреступников один из самых коротких путей к деньгам — это атаки на клиентов банков. Как правило, злоумышленники с помощью социальной инженерии обманным путем добиваются, чтобы жертвы сообщали свои личные данные или устанавливали вредоносное ПО, собирающее персональную информацию (такую как пароли), которую они используют для доступа к своему банковскому счету. В 2016 году решения «Лаборатории Касперского» заблокировали попытки запустить вредоносное ПО, предназначенное для кражи денег через системы онлайн-банкинга, на **2 871 965** устройствах.

Тем не менее, киберпреступники охотятся не только на клиентов банков. Последние годы мы наблюдаем рост числа атак непосредственно на банки и другие финансовые организации. Вероятно, наиболее известная из подобных угроз — Carbanak. Она использует для кражи денег методы проникновения в систему жертвы, характерные для целевых атак. В этом году мы снова наблюдали подобные атаки на финансовые организации.

Группировка Metel проводила целевые атаки на банки — а затем по ночам отправляла людей снимать наличные средства в банкоматах

В феврале 2016 года «Лаборатория Касперского» сообщила о деятельности других APT-группировок, специализирующихся на атаках на финансовые организации. Группировка, стоящая за атакой Metel, с помощью целевых фишинговых атак и браузерных эксплойтов проникала в корпоративные сети банков и брала под контроль ключевые компьютеры в их IT-инфраструктуре. Такой уровень доступа позволял атакующим осуществлять автоматический откат операций, совершаемых через банкоматы: члены преступной группировки использовали дебетовые карты для кражи средств из банкоматов, причем баланс карт оставался неизменным, что позволяло преступникам неоднократно осуществлять транзакции с одними и теми же картами в банкоматах, принадлежащих разным банкам. Злоумышленники орудовали исключительно ночью, успевая за одну ночь украсть средства из нескольких банкоматов. Мы обнаружили вредоносное ПО Metel в системах более 30 финансовых организаций, однако нашей группе реагирования на инциденты удалось очистить зараженные сети, не позволив злоумышленникам нанести организациям-жертвам серьезный ущерб. Тем не менее, киберпреступники, стоящие за Metel, все еще активно действуют, и мы полагаем, что их вредоносное ПО распространено достаточно широко.

МЕТЕЛЬ: СОХРАНЯЙ СПОКОЙСТВИЕ И ОТМЕНЯЙ ОПЕРАЦИИ

*ВСЕ НАЗВАНИЯ ВЫМЫШЛЕНЫ. ВСЕ СОВПАДЕНИЯ СЛУЧАЙНЫ.

Еще один пример — группировка GCMAN (названная так, потому что в основе ее вредоносного ПО лежит код, скомпилированный при помощи компилятора GCC). Она проникает в IT-инфраструктуру финансовых организаций с помощью целевого фишинга с использованием электронных писем, содержащих вредоносный RAR-архив. При открытии архива запускается исполняемый файл, что и вызывает заражение. Попав в сеть, группировка использует легальные технологии и инструменты для тестирования системы на проникновение, такие как Putty, VNC и Meterpreter, чтобы, распространяя заражение по сети, найти ключевые компьютеры, через которые можно напрямую переводить средства в сервисы обмена криптовалют. Затем в один из банковских серверов внедряется cron-скрипт (Cron — это планировщик задач в Unix-подобных операционных системах, используемый для периодического выполнения заданий в определенное время), позволяющий осуществлять финансовые транзакции в размере $200 в минуту. Планировщик каждую минуту вызывает скрипт, помещающий новые транзакции прямо в систему обработки платежей. К счастью, финансовые организации вовремя обнаружили подозрительную активность в сети и отменили транзакции. Если бы это не было сделано, злоумышленникам удалось бы перевести средства в различные сервисы обмена криптовалют без оповещения каких-либо систем банка. Эксперты «Лаборатории Касперского» сотрудничали с тремя финансовыми организациями в России, которые были заражены вредоносным ПО GCMAN, но мы считаем, что эта угроза, вероятно, распространена значительно шире.

Группировка GCMAN в течение 18 месяцев собирала сведения о жертвах заражения, прежде чем начать атаку. При этом распространение по сети осуществлялось с помощью легальных инструментов

Интересно, что, как нам удалось выяснить, собственно атака была осуществлена за 18 месяцев до обнаружения вредоносного ПО. Группировка провела атаку, основанную на внедрении SQL-кода в коммерческое ПО, выполняемое на публичных веб-серверах банка, а потом вернулась через полтора года и использовала собранную за это время информацию для взлома сети банка. За два месяца до этого инцидента кто-то пытался подобрать пароль к учетной записи администратора на сервере банка. Злоумышленники действовали очень упорно, но исключительно по субботам, позволяя себе лишь три попытки в неделю, — все это для того, чтобы избежать обнаружения их активности подразделениями безопасности атакуемых организаций. Деятельность группировки GCMAN иллюстрирует набирающую силу тенденцию в мире киберугроз — предпочтение легальных инструментов специально созданным вредоносным модулям.

Легальные инструменты могут быть не менее эффективны, реже вызывают срабатывание систем защиты и позволяют киберпреступникам быстрее окупить вложения. Подразделениям IT-безопасности следует принимать это во внимание при доработке корпоративной стратегии обеспечения безопасности.

Более подробную информацию о кампаниях Metel и GCMAN можно найти здесь.

Банки, конечно, работают не сами по себе. Для осуществления международных денежных переводов существует межбанковская сеть, которая называется SWIFT (Society for Worldwide Interbank Financial Telecommunication — Общество всемирных межбанковских финансовых каналов связи).

После кражи 100 миллионов долларов многим банкам пришлось усовершенствовать свою систему аутентификации и процедуру обновления ПО SWIFT

В феврале 2016 года хакеры использовали учетные данные сотрудников Центрального банка Бангладеш в SWIFT для отправки фальшивых запросов на проведение транзакций в Федеральный резервный банк Нью-Йорка с целью перевести миллионы долларов на различные банковские счета в Азии. Хакерам удалось перевести 81 миллион долларов в филиппинский банк Rizal Commercial Banking Corporation и еще 20 миллионов долларов в Pan Asia Banking. Ущерб был бы значительно больше, если бы не опечатка в одном из запросов на перевод средств — хакеры напечатали слово foundation (фонд) как «fandation». Федеральный резервный банк обнаружил опечатку, и Банку Бангладеш удалось отменить транзакции на сумму 850 миллионов долларов. Подробно об этом ограблении можно прочитать здесь. Уже после кражи средств из Банка Бангладеш стало известно и о других атаках на банки с использованием учетных данных в SWIFT.

Помимо группировки, стоящей за кампанией Metel, на краже денег из банкоматов специализировались и другие киберпреступные группы. Вредоносные программы для банкоматов существовали и раньше, однако в последние годы число таких программ растет. До 2016 года наиболее примечательной кампанией такого рода была Tyupkin. Чтобы взять банкомат под свой контроль, злоумышленники физически получали доступ к нему и вставляли в него загрузочный компакт-диск.

В мае 2016 года мы сообщили о новой версии вредоносного ПО для банкоматов Skimer. Тот отчет был подготовлен по результатам расследования инцидента, которое мы проводили годом раньше. Вредоносная программа была впервые обнаружена в 2009 году, однако позднее она была переработана. При этом тактика использовавших ее киберпреступников также поменялась. Новая версия имеет глобальный охват — мы обнаружили атаки на банкоматы, расположенные в ОАЭ, Франции, США, России, Макао, Китае, на Филиппинах, в Испании, Германии, Грузии, Польше, Бразилии и Чешской Республике.

Незащищенные банкоматы стали одной из основных мишеней кибер-преступников

Вместо применения широко распространенного метода, основанного на установке в банкомат фальшивого считывателя карт, злоумышленники берут под контроль весь банкомат целиком. Вначале они устанавливают на него вредоносную программу Skimer, используя физический доступ к банкомату или взламывая внутреннюю сеть банка. Вредоносная программа заражает ядро банкомата — ту его часть, которая отвечает за взаимодействие с банковской инфраструктурой, обработку карт и выдачу наличных. В отличие от атак с применением обычных скиммеров для платежных карт, здесь нет никаких физических признаков заражения банкомата, что позволяет атакующим спокойно собирать данные карт, вставляемых в зараженный банкомат (включая платежные данные карты клиента и PIN-код карты), или красть денежные средства напрямую.

Киберпреступник «пробуждает» зараженный банкомат, вставляя карту, содержащую определенную запись на магнитной полосе. После считывания карты Skimer выполняет команду, жестко закодированную на магнитной полосе, или принимает команды через специальное меню, активируемое картой. Пользовательский интерфейс Skimer выводится на экран только после возврата карты и только в том случае, если киберпреступник в течение 60 секунд введет правильный сессионный ключ. Меню предлагает 21 команду, включая выдачу наличных средств, сбор сведений о картах, вставляемых в банкомат, самоудаление и обновление вредоносной программы. Киберпреступник может сохранить реквизиты карт на чипе своей карты или распечатать собранные сведения.

Злоумышленники стараются не привлекать внимание к атаке. Вместо непосредственного снятия наличных в банкомате, которое было бы немедленно обнаружено, они выжидают (иногда в течение нескольких месяцев), прежде чем начать действовать. В большинстве случаев они собирают данные о картах, вставляемых в банкомат, чтобы впоследствии клонировать эти карты. Клонированные карты они вставляют в другие, незараженные банкоматы, спокойно снимая средства со счетов жертв. В результате проследить связь между банкоматами, использованными для снятия средств, и зараженным банкоматом практически невозможно.

Рост числа атак на банкоматы в последние годы — закономерное развитие широко распространенного метода, основанного на применении физических скиммеров для захвата данных с карт, вставляемых во взломанные банкоматы. К сожалению, во многих банкоматах используются операционные системы, в которых, с точки зрения безопасности, есть известные слабые места. Это делает обеспечение физической безопасности банкоматов еще более важной задачей.

«Лаборатория Касперского» предлагает несколько рекомендаций банкам, желающим защититься от подобных атак. Им необходимо регулярно проводить антивирусную проверку своих систем, использовать технологии вайтлистинга (белых списков), применять эффективную политику контроля устройств, внедрить полнодисковое шифрование, защищать BIOS банкоматов паролями, запретить загрузку системы не с жесткого диска и изолировать сети банкоматов от остальной своей IT-инфраструктуры. Один из наших экспертов опубликовал подробный анализ способов обогащения с помощью банкоматов с рекомендациями по мерам, необходимым для эффективной защиты этих устройств.

Новые биометрические скиммеры рассчитаны на системы аутентификации нового поколения, основанные на распознавании отпечатков пальцев, рисунка вен на запястье и радужной оболочки глаза

Вполне естественно, что мы не ограничиваемся расследованием атак, которые уже произошли, но и изучаем вновь появляющиеся технологии, анализируя, каким образом киберпреступники могут пытаться использовать их для своих целей. Недавно мы опубликовали результаты исследования способов аутентификации, которые могут быть использованы, — в том числе бесконтактной аутентификации с помощью технологии NFC, одноразовых паролей и биометрических методов. Возможно, вы удивитесь, узнав, что мы обнаружили 12 производителей, которые уже сейчас предлагают фальшивые сканеры отпечатков пальцев (т.е. биометрические скиммеры) и как минимум трех производителей, разрабатывающих устройства, которые позволят киберпреступникам получать данные с систем распознавания рисунка вен на запястье и радужной оболочки глаза. Данный отчет можно найти здесь.

ИНТЕРНЕТ ВЕЩЕЙ

В 2016 году опасность подключения всего что можно к интернету должна быть очевидна всем

Сегодня мы окружены «умными» устройствами. Все больше предметов для домашнего пользования: телефоны, телевизоры, термостаты, холодильники, видеоняни, фитнес-браслеты и даже детские игрушки — используют смарт-технологии. Иногда даже целые дома проектируются со встроенными «интеллектуальными» возможностями. Но дело не ограничивается бытовыми приборами: в список умных устройств входят автомобили, медицинские приборы, камеры видеонаблюдения и счётчики на парковках. Вездесущий Wi-Fi (иногда, правда, не такой вездесущий, как нам хотелось бы) подключает все эти устройства к Сети, и они становятся частью Интернета вещей (IoT).

Эти вещи создаются, чтобы сделать нашу жизнь легче. Поскольку подключенные к интернету бытовые предметы способны собирать и передавать данные автоматически, без участия человека, они могут работать более эффективно и рационально. Однако Интернет вещей — это площадка, предоставляющая киберпреступникам еще большие возможности для атак. Если устройства, подключённые к интернет-сетям, не защищены, личные данные, которыми они обмениваются, могут быть похищены, при этом устройство может само стать объектом атаки или использоваться для проведения атак на другие устройства.

К сожалению, защитные решения продавать трудно. Подключенные устройства создаются различными производителями — на свободном рынке, и для них критически важным является возврат инвестиций. На конкурентном рынке предметы, которые делают жизнь людей проще, как правило, имеют приоритет. Кроме того, возможности подключения к интернету нередко реализуются на базе уже существующей телекоммуникационной сети, которая создавалась без учета требований безопасности. Таким образом, о защитных функциях на стадии разработки обычно никто не задумывается, если о них вообще когда-либо встает вопрос. Исторически сложилось так, что проблемами безопасности начинают заниматься лишь после того, как случилось что-то, что продемонстрировало, к чему может привести слабая защита.

Последние несколько лет исследователи постоянно поднимают вопрос о защите подключенных устройств. Возможно, вы помните, что один из наших экспертов в области безопасности исследовал свой собственный дом, чтобы выяснить, кибербезопаснен ли он. В прошлом году Чарли Миллер и Крис Валашек продемонстрировали, как можно получить беспроводной доступ к критически важным системам Jeep Cherokee, успешно взяв под свой контроль и заставив ее съехать с дороги! Василиос Хиуреас из «Лаборатории Касперского» и Томас Кинзи из Exigent Systems провели исследование потенциально слабых мест в защите систем видеонаблюдения. Позднее один из производителей медицинского оборудования сообщил об уязвимости в выпускаемой им инсулиновой помпе, позволяющей злоумышленникам отключить устройство или изменить дозировку лекарства. Были опасения и по поводу предметов, которые мы ежедневно используем, таких как детские игрушки, видеоняни и дверные звонки.

В феврале мы показали, как легко выбрать больницу для проведения атаки, получить доступ к ее внутренней сети, а затем взять под контроль МРТ-сканер — найти личные данные пациентов, информацию о них, об их лечении, получить доступ к файловой системе МРТ-аппарата. В этом году наш исследователь Сергей Ложкин представил свои выводы на саммите аналитиков безопасности, выделив ключевые факторы, влияющие на безопасность систем больниц. Во-первых, на медицинских устройствах, подключенных к интернету, использовались без изменения установленные по умолчанию пароли. Многие из этих устройств работали под управлением операционной системы Windows XP и имели десятки неисправленных старых уязвимостей, позволяющих удаленно взломать систему. Во-вторых, эти медицинские устройства не были изолированы от локальной больничной сети. Иными словами, получив доступ к одной из Wi-Fi-сетей больницы (защищенной с помощью слабого пароля), можно было получить полный доступ к этим устройствам. В-третьих, уязвимости на уровне архитектуры программного обеспечения означают, что подключившись к устройству и пройдя установленный по умолчанию экран входа в систему, можно получить доступ к интерфейсу управления, а также личным данным и диагнозам пациентов больницы. Кроме того, в интерфейсе устройства была реализована командная оболочка, которая обеспечивала доступ к файловой системе аппарата. Отчет вы можете прочитать здесь.

Больницы должны срочно принять меры по защите своих систем:

- использовать сильные пароли для защиты внешних точек доступа;
- обновить политики IT-безопасности, разработать систему оценки уязвимостей и своевременной установки исправлений;
- защитить паролями доступ к медицинским системам внутри локальной сети на случай попыток получения несанкционированного доступа к зонам, которые считаются доверенными;
- защитить инфраструктуру от вредоносного ПО и хакерских атак с помощью комплексного защитного решения;
- регулярно создавать резервные копии важной информации и хранить их вне сети.

Исследование датчиков дорожного движения показало, что принцип «security-through-obscurity» не работает в мире вещей, подключенных к интернету

В апреле мы опубликовали результаты исследований датчиков дорожного движения, которые появились в российских городах и в других местах за последние несколько лет. Эти датчики способствуют тому, чтобы водители соблюдали скоростной режим: детекторы обнаружения камер скорости, установленные в салоне автомобиля, реагируют на сигналы, поступающие от новых датчиков, так же как на радары, используемые сотрудниками ГИБДД. Но датчики были установлены не для этого. Они собирают первичные данные о пробках на дорогах (количество машин в каждой полосе, средняя скорость и т.д.) и передают их для анализа в соответствующие структуры городского управления.

«Умные города» – это сложные открытые экосистемы, безопасность которых необходимо продумывать на этапе их проектирования

Наш исследователь Денис Легезо обнаружил, что обмен этими данными не шифруется и на него можно воздействовать извне. Нет никакой авторизации, помимо предусмотренной в Bluetooth, но и та была настроена не лучшим образом. Производитель датчиков дорожного движения щедро делится информацией с сервисными инженерами — большое количество данных о его устройствах доступно публично, в том числе на официальном сайте.

Это положительный момент: подход «security through obscurity» всё равно не работает. Любой мотивированный злоумышленник так или иначе выяснит систему команд и получит доступ к инженерному ПО, так что лучше сочетать открытость, программы bug bounty и быстроту реакции на найденные уязвимости. Хотя бы потому, что число сторонних исследователей популярного оборудования и ПО в любом случае будет больше, чем количество сотрудников в любом ИБ-подразделении. Отчет нашего аналитика доступен здесь.

В большинстве устройств-компонентов «умных городов», ОС спрятана за графическим интерфейсом — но его уязвимости позволяют злоумышленникам получить доступ к устройству

Современные города представляют собой сложные экосистемы, состоящие из сотен различных компонентов, включая и цифровые устройства. Задача умного города — сделать жизнь его обитателей удобной и безопасной. Однако если есть работающее устройство, значит, и взломать его можно. В сентябре мы представили результаты проведенного нами исследования различных аспектов «умного города». Наши эксперты Денис Макрушин и Владимир Дащенко по результатам исследования подготовили отчет, который стал частью нашего вклада в «Securing Smart Cities» — международную некоммерческую инициативу, задуманную как возможность собрать вместе экспертов в технологиях IT-безопасности «умных городов». Терминалы покупки билетов в кинотеатрах, пункты велопроката, устройства электронных очередей в госучреждениях, билетные и информационные стойки в аэропортах, информационно-развлекательные терминалы в такси — все эти устройства могут выглядеть по-разному, но внутри практически все они одинаковы. Любой такой терминал — это устройство, работающее на базе Windows или Android. Основное их отличие заключается в том, что на них работает интерактивная графическая оболочка, обеспечивающая режим «киоска». Это ПО предоставляет пользователю легкий доступ к специфичным функциям терминала и при этом перекрывает доступ к прочим функциям ОС — в частности перекрыта возможность запустить веб-браузер и виртуальную клавиатуру. Если злоумышленник сообразит, как обойти эту блокировку (выйти из режима «киоска»), то получит большие возможности для взлома системы — так, как если бы он сидел перед обычным компьютером. Исследование показало, что практически любое из вышеупомянутых устройств, работающих в режиме «киоска», содержит одну, а то и несколько уязвимостей, воспользовавшись которыми злоумышленник может получить доступ к скрытым функциям ОС. Отчет доступен здесь.

В наши дни разные стороны нашей повседневной жизни всё чаще имеют цифровую форму. Если меры безопасности не планируются на этапе разработки, то это может привести к серьезным последствиям, а исправлять задним числом проблемы безопасности может оказаться не таким простым делом. Чтобы комфортно существовать в данной среде, современный человек должен понимать, что «умный город» — это информационная система, требующая отдельного подхода и специальных знаний для своей защиты

Интернет в заложниках у микроволновки

В октябре киберпреступники использовали ботнет, состоящий из подключенных к интернету домашних устройств (IP-камер, цифровых видеорегистраторов, камер видеонаблюдения и принтеров), чтобы провести DDoS-атаку против компании Dyn — DNS-провайдера, обслуживающего такие компании, как Twitter, Amazon, PayPal, Netflix. В результате веб-сайты этих компаний работали с перебоями или вообще были недоступны. Злоумышленники заражали уязвимые устройства зловредом Mirai. Ранее этот зловред использовался при проведении DDoS-атаки на сайт блога Брайана Кребса — по некоторым данным, это была мощнейшая DDoS-атака за всю историю (нельзя сказать, что за этими двумя атаками стоят одни и те же киберпреступники, поскольку исходный код зловреда недавно был опубликован в интернете). Ботнет Mirai состоит, по оценкам, из 550 000 ботов. Злоумышленники получали доступ к онлайн-устройствам, используя стандартные пароли. Сразу после того как на устройство был записан вредоносный код, он становился частью ботнета Mirai. Как при любой DDoS-атаке, злоумышленники посылали с зараженных устройств множество запросов на сайт своей жертвы, чтобы направить на него большой объем трафика и сорвать таким образом его нормальную работу.

Злоумышленники при проведении этой атаки (как и при других атаках, использующих взломанные IoT-устройства) воспользовались тем фактом, что большинство пользователей не меняют заводские пароли на «умных» устройствах. И это упрощает задачу киберпреступников — стандартный типовой пароль подобрать гораздо легче. К тому же, прошивка многих таких устройств вовремя не обновляется. Наконец, IoT-устройства являются удобной мишенью для киберпреступников по той причине, что они чаще всего круглосуточно включены и подключены к интернету.

Главная рекомендация для всех пользователей, у кого есть дома «умные» устройства, подключенные к интернету — поменять на всех таких устройствах пароли, установленные по умолчанию (новые пароли должны быть сложными), чтобы исключить возможность удаленного доступа. Это относится и к домашним маршрутизаторам — по сути они представляют собой вход в вашу домашнюю сеть.

Кому-то может прийти в голову мысль, что в свете таких новостей лучше отключить все «умные» устройства от сети, однако в современном мире это нереально. При этом всегда бывает полезно обратить внимание на функциональные возможности каждого устройства и отключить те функции, которые вам не нужны. Большая роль в обеспечении безопасности IoT-устройств принадлежит разумным практикам назначения паролей. И наконец, вывод для производителей: безопасность IoT-устройств в идеале должна продумываться на этапе проектирования; исправлять проблемы безопасности задним числом, как правило, гораздо сложнее.

МОБИЛЬНЫЕ УГРОЗЫ

Основными мобильными угрозами в 2016 году были рекламные троянцы, способные получить права суперпользователя на зараженном устройстве. Получение прав суперпользователя не является чем-то новым для этого типа вредоносного ПО, однако в 2016 году все больше троянцев для Android стали использовать их, поскольку эти права позволяют делать на устройстве все. Для того чтобы получить права суперпользователя, троянцы эксплуатируют уязвимости в системе. Поскольку многие устройства не обновляются регулярно, они не получают патчи для этих уязвимостей. На наш взгляд, это станет причиной роста количества и увеличения сложности троянцев, имеющих права суперпользователя.

Недавние обновления операционной системы Android содержали не только патчи для уязвимостей, но и новые защитные функции, однако троянцы быстро нашли способ их обходить. Мы полагаем, что в дальнейшем еще больше мобильных зловредов научатся успешно обходить новые защитные функции. Некоторые их этих функций, возможно, смогут противостоять атакам мобильных троянцев-вымогателей, но их поведение, скорее всего, изменится соответственно.

Вредоносное ПО с правами суперпользователя

Самыми популярными и опасными троянцами в 2016 году были рекламные троянцы, которые способны получить на устройстве права суперпользователя. Основные угрозы исходили от троянцев семейств Trojan.AndroidOS.Ztorg и Trojan.AndroidOS.Iop.

В течение всего года их количество продолжало расти — в ТОП 30 популярных троянских программ по сравнению с прошлым годом оно удвоилось (22 места в 2016 году против 11 в 2015).

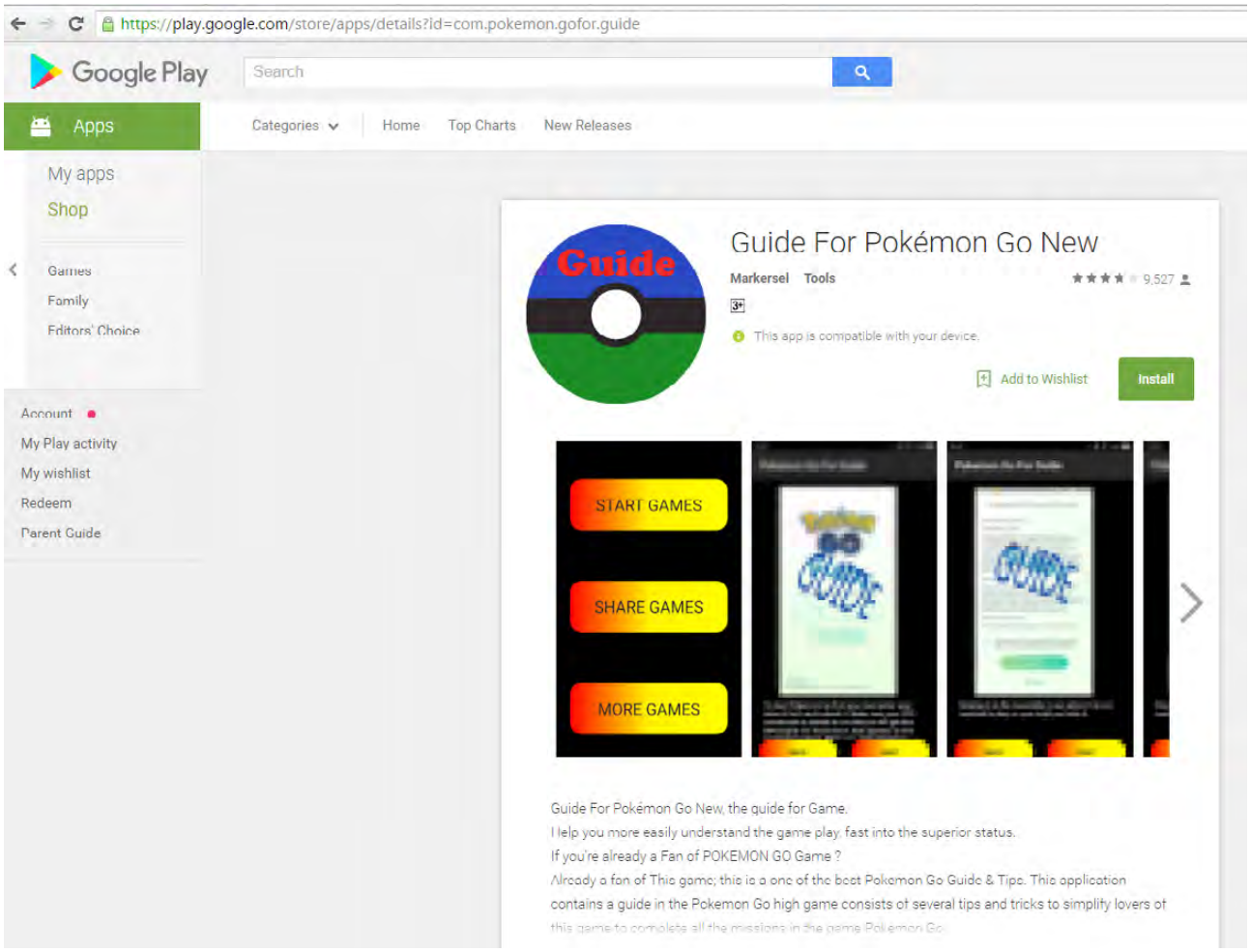
Для получения прав суперпользователя они могли использовать различные эксплойты или уже существующие права суперпользователя, если root-доступ на устройстве был получен ранее.

Все больше троянцев стремились получить права уровня root, чтобы предотвратить свое обнаружение и устанавливать рекламное и вредоносное ПО

Мобильные троянцы использовали права суперпользователя в основном для осуществления двух целей. Во-первых, они могли спрятаться в системной папке, что делало их обнаружение практически невозможным. Некоторые из них могли даже заражать инструмент для восстановления заводских настроек устройства, и тогда невозможным становилось их удаление даже путем возврата к заводским настройкам. Во-вторых, они применяли права суперпользователя для установки в тайне от пользователя и запуска различных приложений, демонстрирующих назойливую рекламу. Большинство новых установленных приложений содержали рекламу и не были вредоносными, однако все же было зарегистрировано несколько случаев, когда они устанавливали новое вредоносное ПО, в том числе модульное приложение-загрузчик Backdoor.AndroidOS.Triada, которое модифицировало процесс Zygote. Это позволяло ему обосноваться в системе и изменять SMS-сообщения, отправленные другими приложениями, и использовать их для кражи денег пользователя. Права суперпользователя давали возможность этому троянцу делать буквально все, включая замену URL в браузерах.

Устройством, зараженным рекламным приложением, становится практически невозможно пользоваться — из-за обилия назойливой рекламы и установленных приложений. Эти троянцы очень трудно удалить, тогда как они могут незаметно устанавливать и даже покупать новые приложения на Google Play.

Как правило, они распространяются через сторонние магазины приложений, но бывает, что они предустановлены на дешевых устройствах. В этом году мы наблюдали их распространение через Google Play. Согласно статистике магазина, некоторые зараженные приложения были установлены более 100 000 раз. А в одном случае киберпреступники осуществили с Google Play более 500 000 установок, используя для этого зараженное руководство к игре Pokemon GO (детектируется как Trojan.AndroidOS.Ztorg.am).

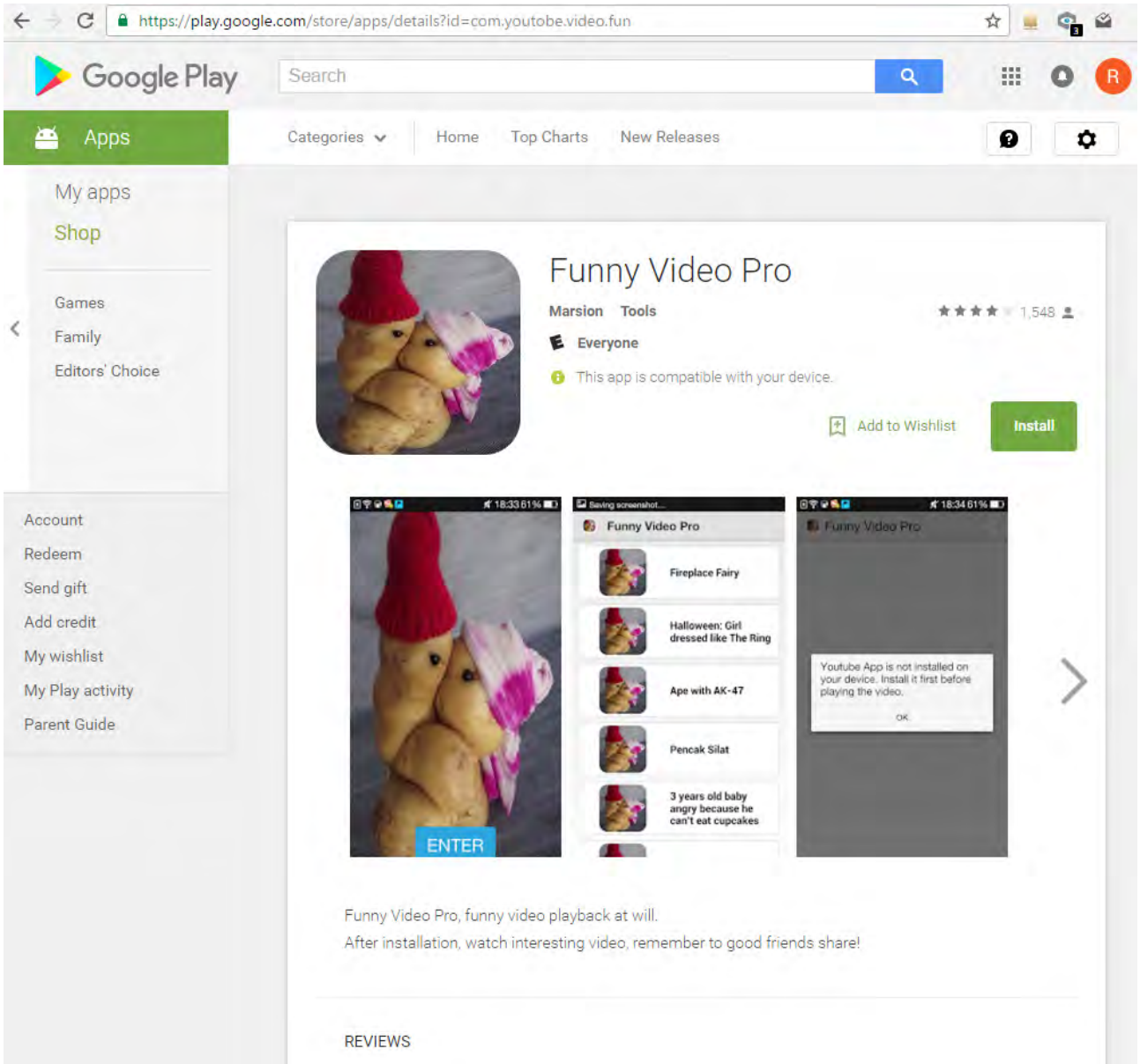


Trojan.AndroidOS.Ztorg.ad в магазине приложений Google Play Store

Киберпреступники продолжают использовать магазин приложений Google Play Store

Вредоносные программы, распространявшиеся через магазин Google Play, были загружены сотни тысяч раз

Киберпреступники продолжают использовать Google Play Store для распространения вредоносных программ. За одну только неделю октября мы выявили более десяти новых приложений в Google Play Store, зараженных Trojan.AndroidOS.Ztorg.am, — новой модификацией троянца Trojan.AndroidOS.Ztorg.ad. Многие из этих приложений были установлены более 100 000 раз.



Trojan.AndroidOS.Ztorg.ad в магазине Google Play Store

Один троянец для Android был установлен и обновлен как «чистое» приложение перед тем, как его зараженная версия попала на компьютеры пользователей

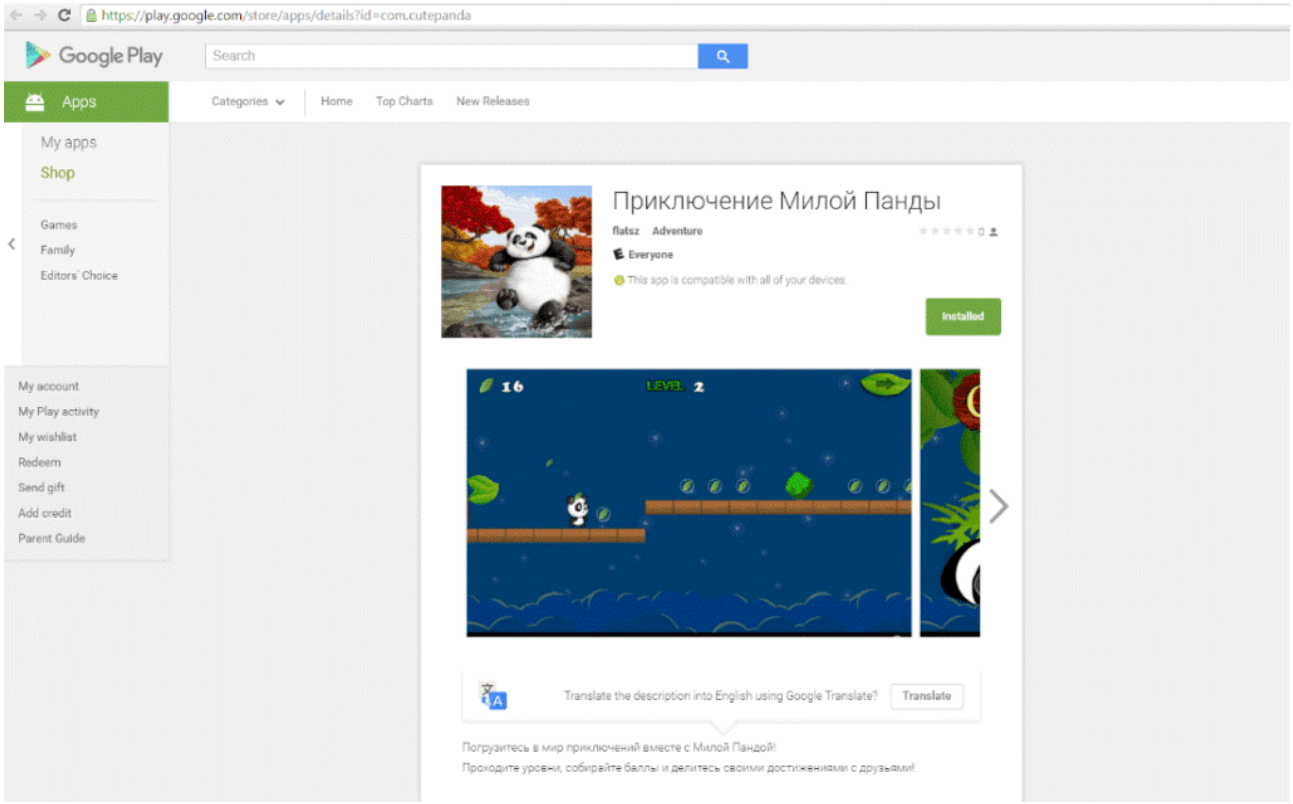
Однако через магазин Google Play распространялись не только рутовальщики, но и PSW-троянцы. В октябре 2015 года мы обнаружили в Google Play Store троянца Trojan-PSW.AndroidOS.MyVk.a. Это зараженное приложение скачали более 100 000 пользователей, поскольку оно выглядело как легитимное приложение для проигрывания аудиозаписей, выложенных в социальной сети «ВКонтакте». Но помимо этого оно крадет аккаунты в социальной сети «ВКонтакте». В течение всего 2016 года киберпреступники несколько раз публиковали в Google Play новые модификации этого троянца. Чтобы избежать детектирования защитными решениями, они сначала опубликовали несколько «чистых» обновлений и в какой-то момент выложили зараженную версию. Этот алгоритм злоумышленники использовали по крайней мере дважды.

Еще одним примером вредоносного ПО, предназначенного для кражи идентификационных данных и доступного в Google Play Store, является HEUR:Trojan-Spy.AndroidOS.Instealy.a. Эти вредоносные приложения выкладывались под видом программ, которые информируют пользователя о том, кто просматривал его профиль — в действительности же они вторгались в процесс аутентификации при подключении к Instagram.

Через магазин Google Play Store распространялись не только рутовальщики и PSW-троянцы. Киберпреступники использовали этот канал для распространения Trojan-Ransom.AndroidOS.Pletor.d.

Trojan-Ransom.AndroidOS.Pletor.d в магазине приложений Google Play Store

Изначально семейство Trojan-Ransom.AndroidOS.Pletor зашифровывало файлы на зараженном устройстве пользователя, но эта модификация лишь блокировала зараженное устройство и требовало у пользователя деньги за его разблокирование. Интересно, что Pletor был создан той же криминальной группировкой, которая придумала банковский троянец Acecard. В декабре 2015 года эта группировка использовала Google Play Store для распространения Trojan-Downloader.AndroidOS.Acecard.b, троянской программы, которая скачивала и устанавливала Trojan-Banker.AndroidOS.Acecard.a.



Страница Trojan-Downloader.AndroidOS.Acecard.b в магазине приложений Google Play Store

Не только Google Play Store

Наряду с тем что после заражения рекламные троянцы использовали эксплойты для получения прав суперпользователя, было зарегистрировано несколько случаев, когда вредоносное ПО использовало эксплойты для распространения.

Наши коллеги из Bluecoat обнаружили Trojan-Ransom.AndroidOS.Fusob, который распространялся с помощью эксплойтов. Набор эксплойтов мог скачивать и устанавливать вредоносные приложения. Чуть позже мы засекли киберпреступников, пытающихся эксплуатировать хорошо известные уязвимости для распространения вредоносных программ.

Троянцы распространялись и через рекламные сети

Распространение Trojan-Banker.AndroidOS.Svpeng было еще одним необычным способом заразить пользователя. В этом случае злоумышленники использовали рекламную сеть Google AdSense, через которую распространяли этот банковский троянец. Svpeng может красть данные о банковской карточке пользователя, подменяя открытое окно банковского приложения фишинговым, а также перехватывает, удаляет и отправляет SMS. Распространение через одну из самых популярных рекламных онлайн-сетей сделало Svpeng самым популярным банковским троянцем для Android в 2016 году. Кроме того, он стал вторым по популярности среди всех троянцев-рутовальщиков.

Обход механизмов защиты

Как упоминалось выше, в 2016 году некоторые троянцы нашли для себя новые пути обхода механизмов защиты Android.

Последние версии ОС Android запрашивают подтверждение пользователя при отправке SMS на короткие номера. SMS-троянец Tiny поверх этого диалогового окна показывает свое, не закрывая при этом кнопку в исходном окне.

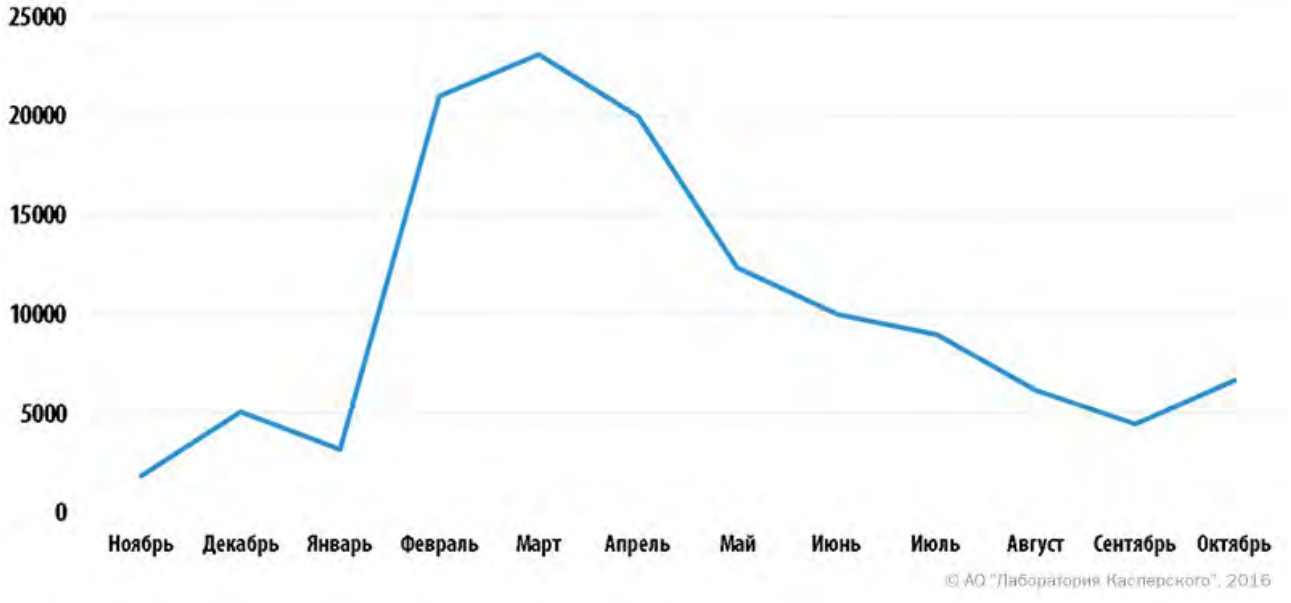
Та же технология использовалась банковским троянцем Trojan-Banker.AndroidOS.Asacub. Он перекрывает стандартное системное окно запроса прав администратора устройства своим окном с кнопками. Таким образом троянец скрывает от пользователя запрос на получение дополнительных прав в системе и обманом вынуждает его подтвердить эти права. Более того, троянец Asacub приобрел функционал SMS-мессенджера и начал предлагать свои сервисы вместо стандартных SMS-приложений, установленных на устройстве. Это позволяет троянцу обойти системные ограничения, впервые появившиеся в версии Android 4.4, а также удалять с устройства или скрывать от пользователя любое входящее SMS-сообщение.

Троянцы Gugi и Asacub нашли новые способы обхода механизмов защиты Android

В июне 2016 года мы обнаружили новую модификацию Trojan-Banker.AndroidOS.Gugi, способную обходить два новых механизма защиты, реализованные в Android 6: запрос у пользователя разрешения при попытке приложения отобразить свое окно поверх других и динамически запрашиваемые разрешения на потенциально опасные действия приложений, такие как отправка СМС или набор номера. Эта версия троянца не использует никаких уязвимостей, в ход пускается только социальная инженерия.

Мобильные программы-вымогатели

Самым популярным троянцем-вымогателем в 2016 году стал Trojan-Ransom.AndroidOS.Fusob. Наиболее активно он распространяется в Германии, США и Великобритании, а в СНГ и некоторых соседних странах он вообще не работает. Зловред блокирует устройство пользователя и за разблокировку требует выкуп в размере 100–200 долларов, который нужно заплатить в виде кодов от предоплаченных карт iTunes. Пик популярности этого троянца-вымогателя пришелся на ноябрь 2015 — март 2016 года: в этот период количество атакованных им пользователей выросло в 12 раз, а затем его популярность пошла на спад и вернулась практически к показателю прошлого года.



Количество уникальных пользователей, атакованных троянцем-вымогателем Trojan-Ransom.AndroidOS.Fusob

Хотя по количеству атакованных пользователей мобильные банковские троянцы опережают мобильных троянцев-вымогателей, по числу установочных пакетов ситуация обратная: со второго квартала 2016 года лидируют троянцы-вымогатели.

Мобильные программы-вымогатели перекрывают окна других программ своими, а не зашифровывают данные, которые чаще всего имеют резервные копии в облаке

Первые мобильные троянцы-вымогатели зашифровывали файлы пользователей и требовали выкуп за их расшифровку. Современные программы-вымогатели для Android не зашифровывают файлы пользователей, они просто показывают свое окно поверх других приложений, перекрывая даже диалоговые окна системы. Мобильные шифровальщики не слишком популярны в основном потому, что данные пользователей мобильных устройств, как правило, имеют резервные копии в облачных сервисах. Обычные программы-вымогатели, которые перекрывают другие окна своим окном, работают вполне эффективно, и кроме того, от них не так просто избавиться, как от троянцев.

Одно из наиболее популярных в Китае семейств мобильных программ-вымогателей — Trojan-Ransom.AndroidOS.Congur — блокирует зараженное устройство иначе: после запуска устройства троянец запрашивает права администратора и затем меняет PIN-код или устанавливает свой, если до этого PIN-кода на устройстве не было. И далее он предлагает пользователю связаться с киберпреступниками через QQ-мессенджер, чтобы узнать новый PIN-код. Метод простой, и тем не менее эффективный.

Троянцы-вымогатели — технически один из самых простых, но очень эффективных видов троянцев. Поэтому в следующем году мы ожидаем дальнейшего роста их числа и появления новых семейств.

УТЕЧКА ДАННЫХ

Частная информация — это ценный товар, так что неудивительно, что киберпреступники атакуют различные онлайн-ресурсы, пытаясь украсть побольше данных «оптом», в течение одной атаки. Мы привыкли к постоянному потоку сообщений в СМИ о взломах и прочих нарушениях безопасности; этот год не стал исключением: были сообщения об утечке данных на beautifulpeople.com, Tumblr, хакерском форуме nulled.io (подчеркнем тот факт, что атаки происходят не только на легитимные сервисы), Kiddicare, VK.com, Sage, официальном форуме DotA 2, Yahoo, Brazzers, Weebly и Tesco Bank.

Некоторые атаки закончились кражей огромных объемов данных; это обнаружило тот факт, что многие компании не принимают адекватных мер, чтобы защитить себя. Речь идет не только о защите периметра корпоративной сети.

Стопроцентной безопасности не бывает, и нельзя гарантировать, что система не может быть взломана, особенно если взлом происходит с помощью инсайдера или сотрудника компании, которого обманом заставили делать то, что угрожает корпоративной безопасности.

Но при этом любая организация, которая хранит персональные данные, обязана заботиться об их безопасности и делать это эффективно. Практически это включает хеширование и «соление» пользовательских паролей и шифрование прочих конфиденциальных данных.

Пользователи не могут самостоятельно контролировать безопасность личных данных, которые они предоставляют интернет-провайдерам. Но они могут ограничить ущерб от возможного взлома провайдера онлайн-услуг, выбирая уникальные сложные пароли: идеальный пароль не короче 15 символов и состоит вперемешку из букв, цифр и символов всей клавиатуры. Если это покажется вам сложной задачей, здесь вы можете найти полезные советы о том, как создать безопасные, но легко запоминающиеся пароли. Разумная альтернатива — использовать менеджер паролей: он справится с созданием таких сложных паролей автоматически.

Кража почтовых адресов и паролей из LinkedIn выявила миллион аккаунтов, использующих пароль «123456»

К сожалению, зачастую люди используют простые пароли, которые легко подобрать, а также используют одни и те же пароли в учетных записях разных онлайн-сервисов — в этом случае один взломанный пароль делает уязвимыми все учетные записи пользователя. Об этой проблеме заговорили в мае 2016 г., когда хакер под ником Peace попытался продать 117 миллионов почтовых адресов и паролей из LinkedIn, которые были украдены несколькими годами раньше. Более миллиона из этих паролей были «123456».

В июле мы еще раз вернулись к событиям, связанным со взломом сайта Ashley Madison, через год после атаки, которая привела к утечке пользовательских данных, и предложили ряд полезных советов тем, кто собирается искать любовных приключений в Сети (и неплохие рекомендации на тему, как управлять любым онлайн-аккаунтом).

Вопрос о паролях продолжает подниматься снова и снова. Если мы используем простые пароли, которые легко подобрать, мы делаем себя уязвимыми для кражи наших личных данных. Проблема усугубляется, если использовать одни и те же пароли в учетных записях разных онлайн-сервисов. Именно поэтому многие провайдеры, в том числе Apple, Google и Microsoft, теперь предлагают двухфакторную аутентификацию, т.е. для доступа к сайту или внесения изменений в настройки учетной записи пользователей просят ввести код, сгенерированный аппаратным ключом или присланный на мобильное устройство. Двухфакторная аутентификация, безусловно, повышает уровень безопасности — если только она является обязательной, а не опциональной.

Учитывая потенциальный ущерб, который может нанести взлом систем провайдера, никто не удивляется тому, что регулирующие органы уделяют этой проблеме все больше внимания. Управление Комиссара по информации Великобритании (UK Information Commissioner's Office, ICO) недавно наложило рекордный штраф размером 400 000 фунтов стерлингов на компанию TalkTalk за «отсутствие элементарных мер по обеспечению кибербезопасности» в связи с атакой на компанию, имевшей место в октябре 2015 года. По мнению ICO, рекордный штраф — это «предупреждение остальным, что кибербезопасность — это не прерогатива IT-департамента, а сфера ответственности совета директоров».

Принятые в ЕС Общие правила защиты данных (General Data Protection Regulation, GDPR), которые вступят в силу в мае 2018 года, требуют, чтобы компании сообщали об утечке данных регулирующему органу, и предусматривают серьезные штрафы за отсутствие надлежащей защиты личных данных. Общую информацию о Правилах можно найти здесь. Предполагается, что это заставит компании сообщать об утечках своевременно. Необходимость такого подхода со всей очевидностью была продемонстрирована в этом году, когда веб-сервис Dropbox разослал многим своим клиентам уведомления с требованием сменить пароль. В 2012 году взлом Dropbox привел к утечке не только адресов электронной почты, но и паролей. Однако тогда Dropbox уведомил своих клиентов лишь о краже адресов электронной почты, умолчав о паролях. К счастью, пользовательские пароли хранились в виде посоленных хешей, а кроме того, Dropbox предлагает двухфакторную аутентификацию.

Есть несколько компаний, которые надеются вообще упразднить потребность в паролях. Apple позволяет авторизоваться по отпечаткам пальцев для совершения покупок в iTunes и осуществления платежей через Apple Pay. Samsung объявил, что введет авторизацию по отпечаткам пальцев, по голосу и радужной оболочке глаза. Amazon объявил о методе аутентификации selfie-pay. MasterCard и HSBC объявили о введении авторизации транзакций путем распознавания лица и голоса пользователя. Главный плюс всех этих нововведений — это то, что они замещают что-то, что пользователю приходится держать в памяти (пароли), чем-то, что у пользователя и так есть, и при этом пользователь не имеет возможности упростить процесс аутентификации (как, например, в случае, когда пользователь выбирает слабый пароль).

Аутентификация в дополнение к паролю повышает уровень безопасности

Многие рассматривают биометрию как перспективу. Однако она не является панацеей для безопасности: как мы уже говорили (здесь, здесь и здесь), биометрию можно подделать, а еще биометрические данные можно украсть. Лучше рассматривать биометрию не как пароль, а как замену имени пользователя. В итоге существенно необходима многофакторная аутентификация — совмещающая что-то, что *вы знаете*, что-то, что *вы имеете*, и что-то, что *является частью вас самих*.

КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ: УГРОЗЫ И ИНЦИДЕНТЫ

Мы не можем назвать 2016 год выдающимся с точки зрения количества или критичности инцидентов кибербезопасности в промышленных средах. Тем не менее, упомянем в отчете несколько интересных случаев.

Инциденты

В этом году дважды поднималась тема кибербезопасности на атомных электростанциях. Первый раз — в конце апреля, когда компания-оператор АЭС Gundremmingen сообщила об обнаружении червя Kido (известного также как Conficker) на компьютерах системы управления энергоблока B. Эта система управления используется механизмом перемещения топливных стержней. К счастью, червь не оказал влияния на технологический процесс и никак не повредил системы электростанции.

Об инциденте были уведомлены соответствующее надзорное ведомство и Федеральное управление по информационной безопасности (BSI). Были проверены все критически важные системы и устройства, и на них не было обнаружено никаких следов заражения. В результате происшествия были усилены меры безопасности. По принятым в Германии критериям данный инцидент был классифицирован по категории N (Normal). В соответствии с Международной шкалой оценки ядерных событий (INES) он относится к нулевому уровню (ниже основной шкалы, отсутствующее или очень малое значение для безопасности).

Источник заражения не раскрывается, но представитель пресс-службы АЭС сказал, что в офисной сети электростанции было обнаружено около 18 USB-носителей, зараженных тем же червем Kido. По словам сотрудника АЭС, это не могло нанести ущерб, поскольку все критически важные для электростанции системы управления физически изолированы, а архитектура системы построена на принципе избыточности для предотвращения отказа в обслуживании и защищена от несанкционированного вмешательства.

Несмотря на то что в данном случае заражение червем Kido, к счастью, не причинило серьезного вреда, было бы глупо считать, что только специально созданное вредоносное ПО и целевые атаки могут нанести значительный ущерб. В самом конце 2015 года на Украине была проведена тщательно скоординированная кибератака на подстанции электрической сети. Злоумышленники отправили фишинговые сообщения с эксплойтом сотрудникам, компьютеры которых были подключены к офисной сети энергокомпаний. Сразу же после заражения первых компьютеров атакующие сумели проникнуть в технологическую сеть и вывести из строя систему электроснабжения. Кроме того, в ходе атаки был полностью заблокирован удаленный доступ к технологической сети. Удалив часть технологического ПО и повредив загрузочные секторы дисков, киберпреступники сделали невозможным удаленное управление и восстановление системы.

Это демонстрирует, что даже если вредоносное ПО не затрагивает непосредственно технологический процесс, но вызывает отказ в обслуживании со стороны критически важных вспомогательных систем, таких как SCADA, шлюзы технологической сети, системы удаленного доступа и т.д., то АСУ, возможно, и будет продолжать работать, используя последние известные настройки, но при этом не будет возможности управлять технологическим процессом и корректировать его в случае аварии или чрезвычайной ситуации.

Атаки на АСУ, о которых эксперты по безопасности не получают адекватной информации, невозможно проанализировать, а значит, нельзя принять меры для повышения безопасности

Несколько месяцев назад Юкия Амано (Yukiya Amano), глава Международного агентства по атомной энергии (МАГАТЭ), сообщил, что за 2–3 года до этого была проведена хакерская атака на атомную электростанцию. «Это действительно произошло и вызвало некоторые проблемы. Электростанцию не пришлось останавливать, однако потребовались определенные меры предосторожности», — сказал Амано. Но дело не только в том, что проблемы, связанные с кибербезопасностью, способны нарушить нормальную работу электростанции. Очевидно, есть более серьезная проблема в отсутствии взаимодействия и прозрачности во взаимоотношениях между специалистами по промышленным системам управления и экспертами по кибербезопасности. В результате специалисты по безопасности не имеют возможности полноценно анализировать ситуацию, а владельцы и производители АСУ ТП не в состоянии осуществлять превентивные меры, способные минимизировать возможный ущерб.

Концептуальное вредоносное ПО для ПЛК

В августе этого года на конференции Black Hat 2016 исследователи из группы OpenSource Security представили концептуальный (proof-of-concept) червь для ПЛК. Червь был написан как программа, способная самостоятельно находить в сети программируемые логические контроллеры (ПЛК) и распространяться с одного ПЛК на другой. Кроме того, он способен подменять данные на входе и на выходе ПЛК, вызывать отказ ПЛК в обслуживании, соединяться с командными серверами и выполнять функции прокси-сервера при распространении атаки по сети.

В том что касается этого концепта, наибольший интерес представляют приемы, применяемые для заражения ПЛК. Концептуальная вредоносная программа написана для контроллеров Siemens S7-1200, в которых реализована функция защищенного доступа. Эта функция, если она включена, позволяет устанавливать пароль, необходимый для доступа к ПЛК через протокол S7CommPlus. Таким образом, она не позволяет не прошедшему авторизацию злоумышленнику читать и вносить изменения в код на ПЛК. Однако по умолчанию функция защищенного доступа отключена. Если же она действует, единственный способ для червя заразить ПЛК — это подобрать пароль методом полного перебора или каким-то образом украсть/захватить его.

С другой стороны, если функция защищенного доступа отключена, действуют еще два защитных механизма, предназначенных для ограничения доступа к ПЛК:

- Know-how protection — защита, которая не позволяет извлекать программное обеспечение с ПЛК и модифицировать его.
- Copy protection — защита, которая не позволяет переносить копии программного кода с одного ПЛК на другой.

Проверка прав доступа в обоих защитных механизмах — Know-how protection и Copy protection — реализована на стороне клиента (в составе портала TIA). Это означает, что возможно считывать и записывать блоки данных на ПЛК, минуя аутентификацию, с помощью простого инструмента собственной разработки. Компания Siemens опубликовала бюллетень по безопасности и выпустила патч для встроенного ПО контроллера S7-1200.

Важный урок в данном случае состоит в том, что любое вредоносное устройство или злоумышленник с доступом к сети АСУ имеет возможность без особых проблем полностью взламывать системы управления. Более того, ПЛК особенно уязвимы для атак (прежде всего DoS), поскольку они рассчитаны на обмен данными только с системой SCADA и технологическим ПО, и в них почти или совсем отсутствует защита от несанкционированного доступа, ввода некорректных данных или подмены данных киберпреступниками.

Уязвимости нулевого дня в программном и аппаратном обеспечении АСУ

По данным центра US ICS CERT, в 2015 финансовом году (с октября 2015 по сентябрь 2016 года) было получено 427 сообщений об уязвимостях в АСУ, а в предыдущем году таких сообщений было 245. Около 25% указанных уязвимостей связано с отсутствием надлежащей валидации входных данных, еще 27% — с недостаточно эффективным контролем доступа. Производители зачастую отказываются признавать существование еще одной важной категории уязвимостей — тех, что связаны с особенностями конфигурации и функционирования систем. Такие уязвимости, как использование установленных по умолчанию учетных данных и стандартных настроек безопасности (учитывая, что функции безопасности зачастую отключены по умолчанию), скрытых API или недокументированного функционала очень опасны, потому что они дают широкие возможности доступа к системам управления, причем их эксплуатация не требует серьезных технических навыков.

Временной разрыв между сообщением о наличии уязвимости в АСУ и выпуском патча зачастую слишком велик

Печально, что от предоставления производителю отчета об обнаружении уязвимости до выпуска патча, закрывающего эту уязвимость, проходит очень много времени. Иногда патч не выпускается вовсе — производитель заявляет, что уязвимый продукт снят с производства. Владельцу АСУ в такой ситуации приходится выбирать между огромными затратами на модернизацию и огромным риском взлома системы.

В заключение мы хотели бы подчеркнуть важность вклада различных сообществ экспертов по безопасности в дело повышения уровня кибербезопасности автоматизированных систем управления. Последние несколько лет мы наблюдаем серьезный рост заинтересованности в проблемах безопасности АСУ. Каждый год появляется значительное число новых экспертных отчетов, инструментов и комплексов. Например, в прошедшем году мы опубликовали наш собственный обзор киберугроз для промышленных систем. Это позволяет специалистам по кибербезопасности из других областей (не связанных с АСУ) быстро включиться в работу и поделиться своим опытом и знаниями.

Securelist

Ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy