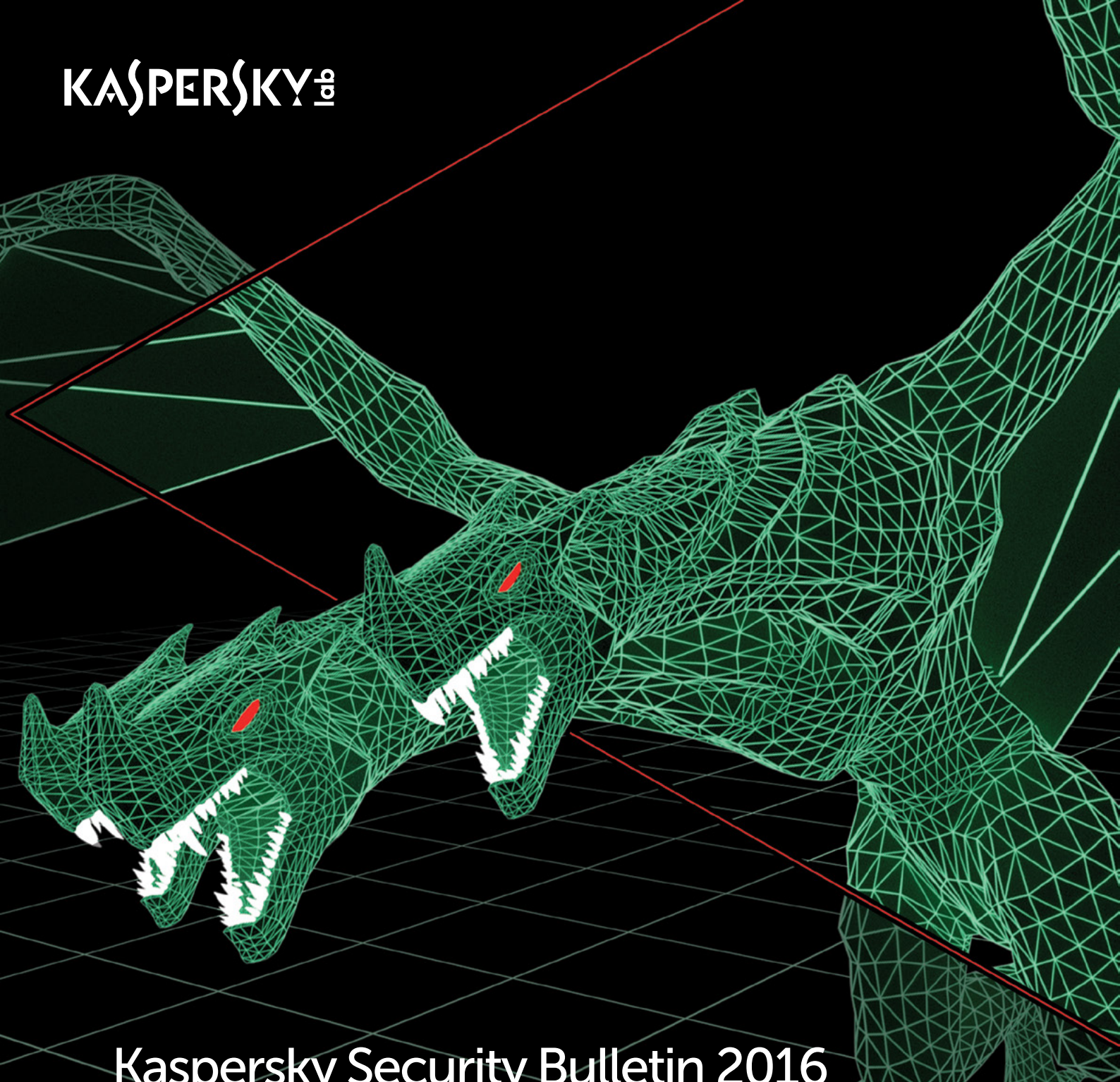
KASPERSKY lab



Kaspersky Security Bulletin 2016

ПРОГНОЗЫ НА 2017 ГОД: КОНЕЦ «ИНДИКАТОРОВ ЗАРАЖЕНИЯ»

GREAT

ОГЛАВЛЕНИЕ

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

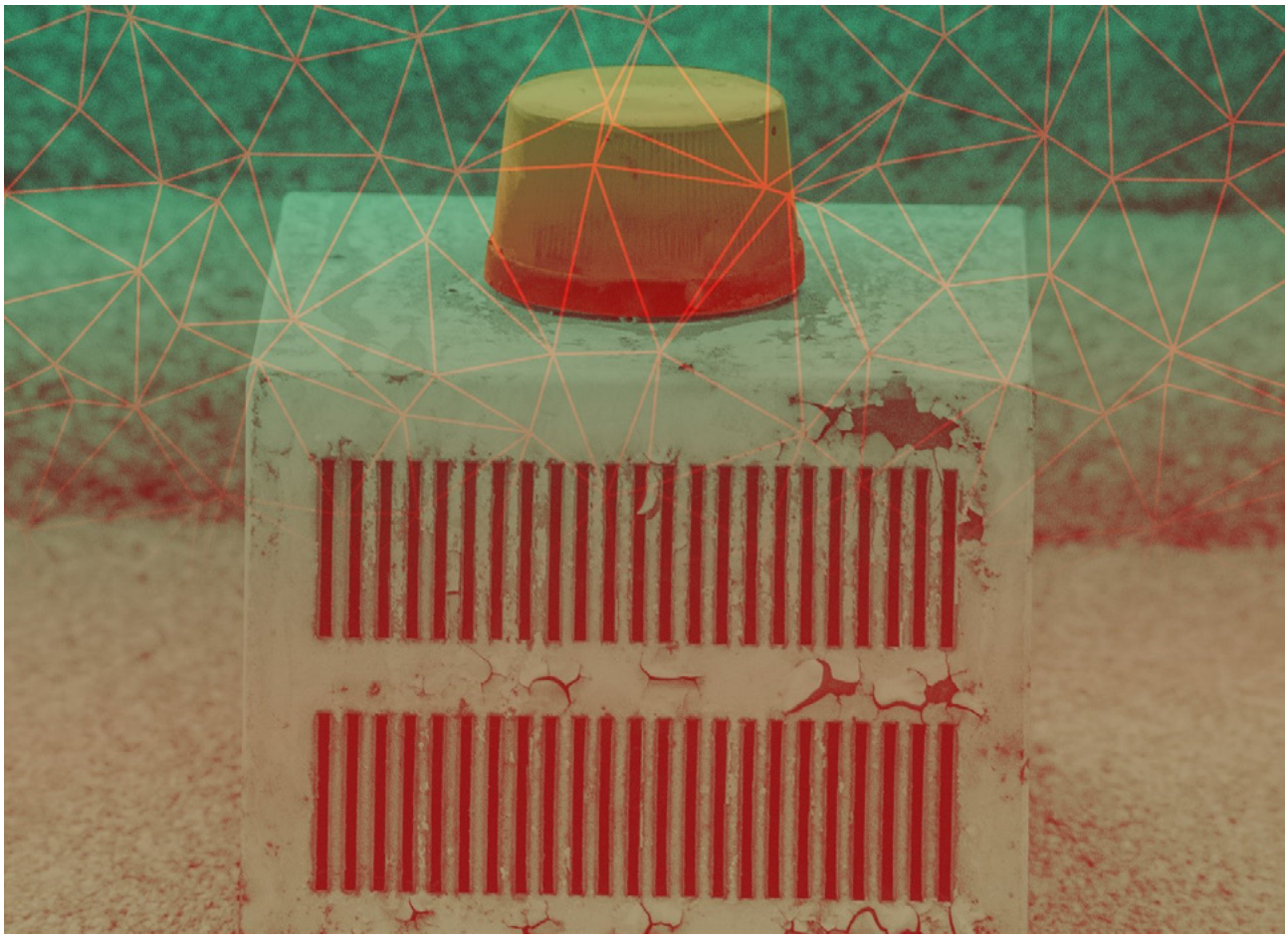
Хотя все мы ненавидим программы-вымогатели (и не без оснований), надо понимать, что в большинстве случаев успех вымогателей строится на своеобразных доверительных отношениях между жертвой и атакующей стороной. Киберпреступная экосистема основывается на посылке, что злоумышленник будет соблюдать молчаливое 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.

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