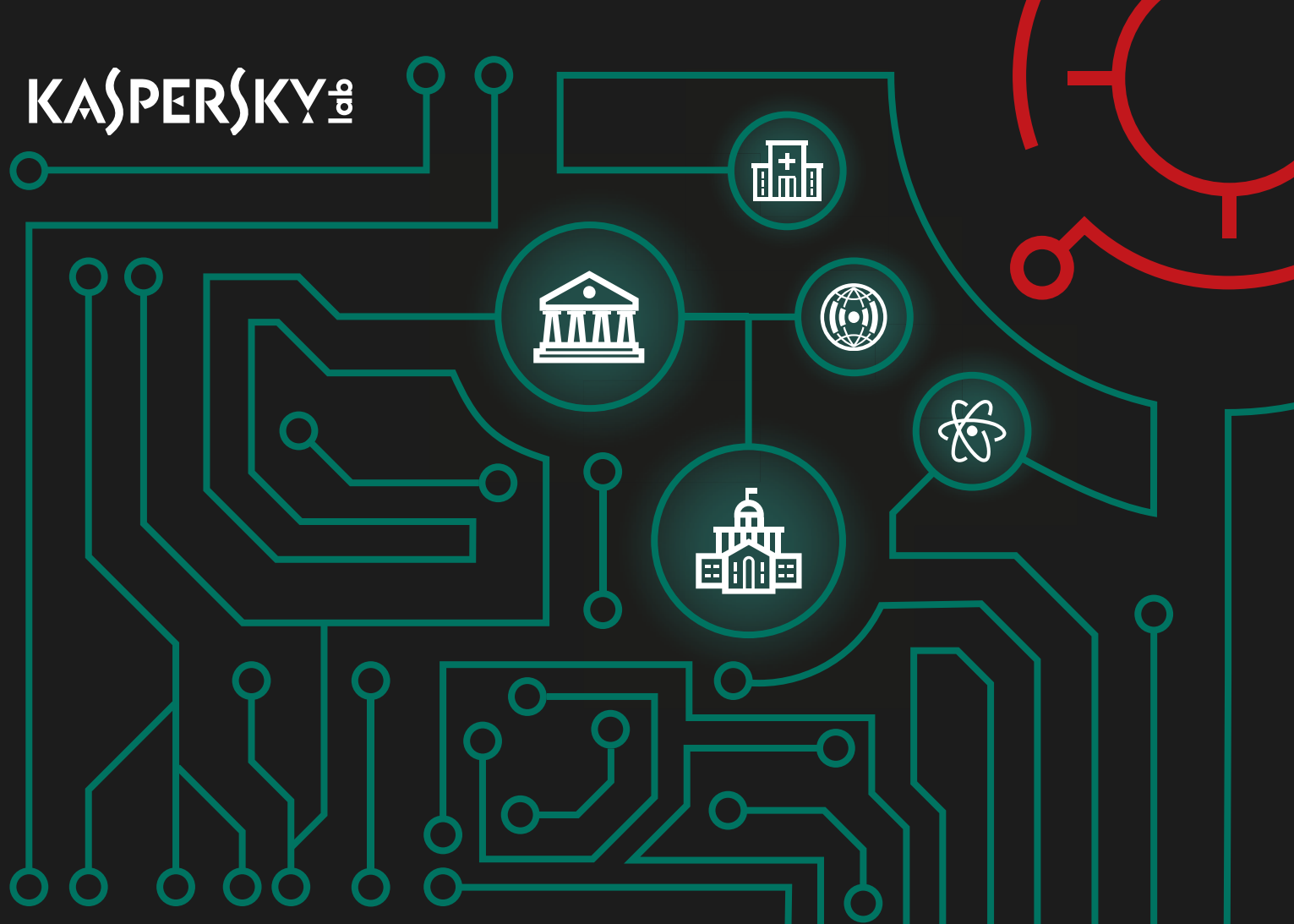
KASPERSKY lab



Kaspersky Security Bulletin:

ПРОГНОЗЫ НА 2018 ГОД

СОДЕРЖАНИЕ

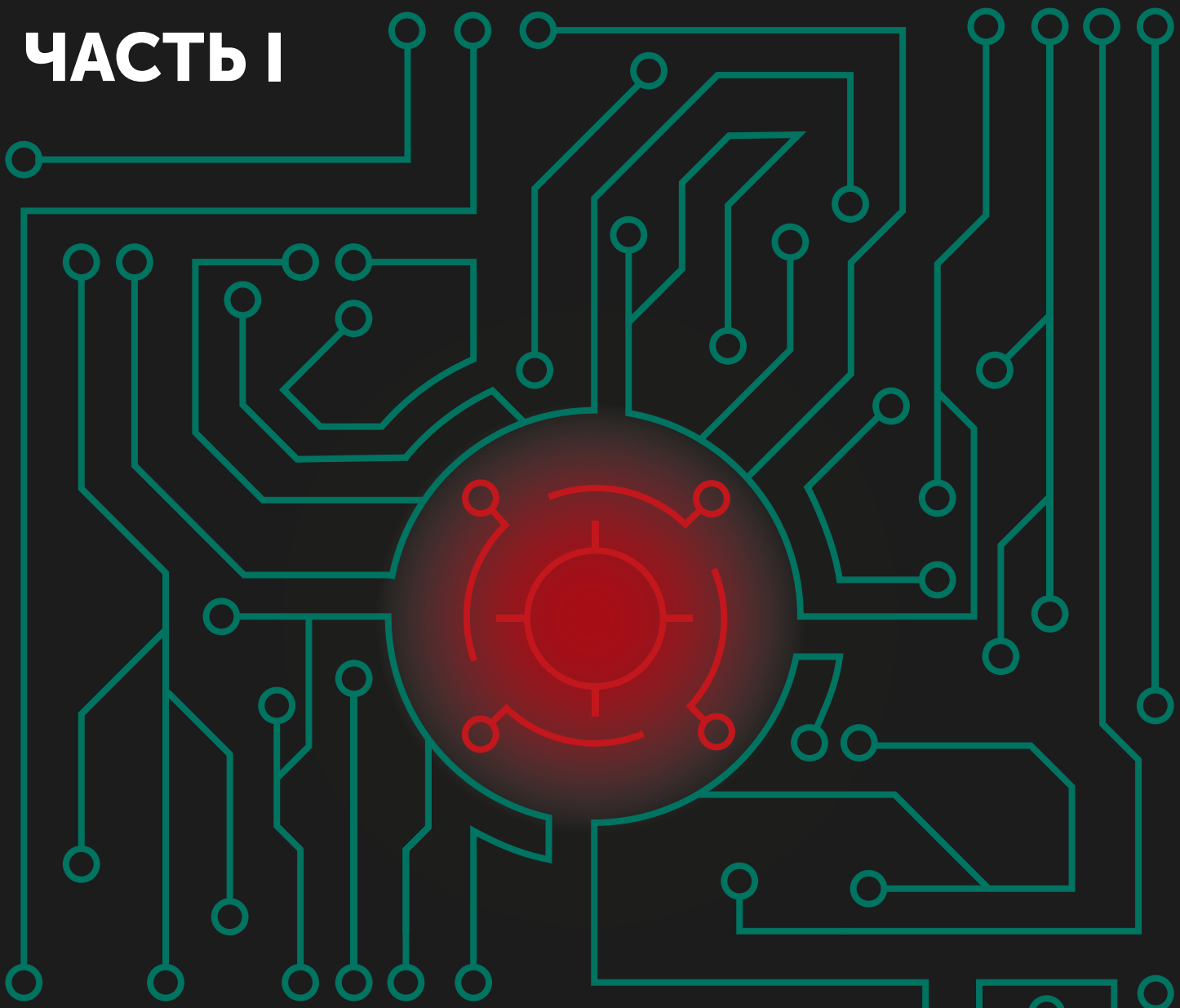
ВВЕДЕНИЕ

В 2017 году опытные злоумышленники и хактивисты продолжили серию дерзких атак и краж, которые прогремели на весь мир. Но в этом году внимание СМИ было приковано и к другой угрозе, распространяющейся молниеносно и заражающей предприятия любых размеров. Масштабные эпидемии программ-вымогателей, происшедшие в мае и июне, выявили уязвимые области пострадавших компаний: бреши в сетевой безопасности, непропатченные приложения и беспечность сотрудников. Некоторые организации потеряли в результате атак сотни миллионов долларов.

Многие компании хотят лучше понимать ландшафт киберугроз в своей сфере, чтобы быть готовыми к атакам. Для этого мы включили в отчет *Kaspersky Security Bulletin: Прогнозы на 2018 год* не только обобщенные прогнозы, подготовленные командой GReAT, но и новый раздел с отдельными прогнозами по отраслям и технологиям.

Все прогнозы основаны на исследованиях и опыте экспертов «Лаборатории Касперского» за 2017 год. Мы попытались как можно точнее спрогнозировать грядущие угрозы на основе имеющихся сведений и надеемся, что наш отчет поможет вам лучше разобраться в ситуации и побудит предпринять необходимые меры.

ЧАСТЬ I



ПРОГНОЗИРУЕМЫЕ АРТ-УГРОЗЫ

GREAT

ВВЕДЕНИЕ

Хотите верьте, хотите нет, но мы снова будем говорить об APT-угрозах. Прошедший 2017 год вызвал противоречивые эмоции у ИБ-экспертов. С одной стороны, на наших глазах «оживают» проблемы, прежде считавшиеся теоретическими, а каждая новая атака открывает новое поле для исследований. На примере APT мы можем лучше оценить реальную поверхность атаки, вычислить тактику злоумышленника и, как результат, еще эффективнее выслеживать и отражать новые угрозы. С другой стороны, целью нашей работы по-прежнему остается безопасность пользователей, для которых атака порой оборачивается катастрофой. Мы не рассматриваем каждый новый инцидент как вариацию уже пройденного материала. Вместо этого мы наблюдаем, как постепенно ослабевает безопасность пользователей, интернет-магазинов, финансовых и правительственных учреждений, и пытаемся представить, какое будущее наш ждет.

Как мы уже отмечали в прошлом году, наш отчет — не завуалированная реклама. Мы строим прогнозы на основе наблюдений за прошлый год и выделяем тенденции, которые могут обостриться в новом году.

ОГЛЯДЫВАЯСЬ НАЗАД

Сбылись ли наши прогнозы?

В качестве подтверждения реалистичности наших прогнозов за прошлый год давайте перечислим некоторые из них и приведем примеры.

Шпионаж и APT-угрозы

Распространение пассивных имплантов, практически не оставляющих следов заражения – Сбылось!

Короткие заражения / вредоносные программы, скрывающиеся в оперативной памяти – Сбылось!

Шпионаж станет мобильным – Сбылось!

Финансовые атаки

Будущее финансовых атак – Сбылось!

Программы-вымогатели

Грязное и лживое вымогательство – Сбылось!

Угрозы в промышленности

Катастрофа не случилась, и мы очень рады, что ошибались. Однако мы видели, как Industoyer атакует АСУ.

Интернет вещей

Кирпич, как его ни назови – Сбылось! BrickerBot

Информационные войны

Сбылось, масса примеров!

ЧЕГО ЖДАТЬ В 2018 ГОДУ?

Больше атак на цепочки поставок

Глобальный центр исследования и анализа угроз «Лаборатории Касперского» отслеживает более 100 APT-групп и кампаний. Некоторые группировки обладают богатыми возможностями и широчайшим арсеналом, включающим эксплойты нулевого дня и бесфайловые средства атаки. Иногда они используют традиционные методы взлома, а потом передают работу более опытным командам хакеров, которые занимаются эксфильтрацией данных. Нередко мы наблюдали ситуации, когда опытные хакеры долго пытались взломать определенную цель и каждый раз уходили ни с чем. Такую стойкость потенциальной жертвы можно объяснить либо наличием мощного защитного решения и обученных сотрудников, не поддающихся на методы социальной инженерии, либо тщательной проработкой 35 ключевых стратегий по противодействию APT-атакам, подготовленных Управлением радиотехнической обороны Австралии. Как правило, опытные и настойчивые злоумышленники, специализирующиеся на APT-атаках, просто так не сдаются — они продолжают искать бреши в обороне, пока не найдут.

Если все предпринятые меры не приносят плодов, злоумышленники временно отступают, чтобы повторно оценить свою цель. В итоге киберпреступники могут прийти к выводу, что атака на цепочку поставок может оказаться эффективнее прямого наступления. Даже если сеть организации со всех сторон прикрыта наилучшими в мире средствами защиты, ее сотрудникам все равно приходится работать со сторонним ПО. Взломав более простое и уязвимое стороннее решение, можно проскользнуть за надежные рубежи защиты исходной цели.

В 2017 году преступники организовали несколько атак по этому сценарию. Вот некоторые из них:

- Shadowpad
- CCleaner
- ExPetr / NotPetya

По нашим прогнозам, в 2018-м стоит ждать еще больше подобных атак — какие-то из них будут раскрыты, другие так и останутся незамеченными.

Такие атаки порой чрезвычайно трудно обнаружить и обезвредить. Например, в случае с Shadowpad злоумышленники успешно внедрили троянцы в несколько пакетов Netsarang, которые используют в банках и на крупных предприятиях во всем мире. Различить чистые и троянские пакеты крайне сложно — во многих случаях подделку выдает трафик, идущий в командный центр.

По оценкам экспертов, зараженный пакет CCleaner загрузили на более 2 млн. компьютеров — это одна из самых масштабных атак за 2017 год. Мы проанализировали вредоносный код CCleaner и нашли сходство с такими бэкдорами, как APT17 или Aurora, ранее использовавшимися различными APT-группами под общим названием Axiom. Это показывает, насколько далеко готовы зайти APT-группы, чтобы добиться поставленных целей.

Мы полагаем, что количество проведенных атак на цепочки поставок может превзойти наши ожидания: далеко не все атаки были обнаружены и раскрыты общественности. По нашим прогнозам, в 2018-м стоит ждать еще больше подобных атак — какие-то из них будут раскрыты, другие так и останутся незамеченными. Добавление троянцев в специализированное ПО, распространенное в отдельных регионах или отраслях экономики, станет популярным способом для попутного заражения стратегических объектов с охватом конкретной аудитории пользователей.

Больше сложных вредоносных программ для мобильных устройств

В августе 2016 года CitizenLab и Lookout опубликовали анализ Pegasus — недавно обнаруженной передовой шпионской платформы для мобильных устройств. Этот так называемый «набор ПО для законного перехвата данных» израильская компания NSO Group продает государственным и прочим структурам. В сочетании с уязвимостями нулевого дня, позволяющими удаленно обойти системы защиты современных мобильных ОС (например, iOS), эта платформа становится мощным оружием, которому нечего противопоставить. В апреле 2017 года компания Google провела анализ Android-версии Pegasus, которую они окрестили Chrysaor. Помимо вредоносных программ для «законного наблюдения», таких как Pegasus и Chrysaor, ряд других APT-группировок разработали собственные мобильные импланты.

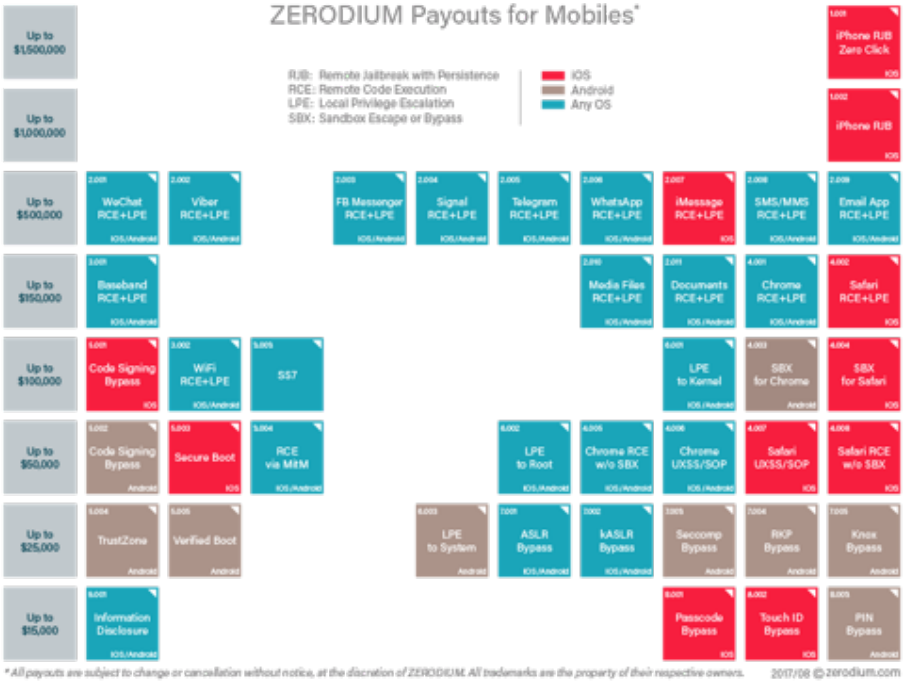
Увеличение частоты атак и совершенствование технологий их обезвреживания приведет к возникновению более сложных APT-зловредов для мобильных платформ.

Учитывая, что в iOS заблокирована возможность анализа системной среды, у пользователя нет возможности убедиться, что его смартфон не заражен. Экосистема Android оказалась более уязвимой, но все же ситуация там менее плачевная, так как пользователи могут защитить устройство решениями вроде Kaspersky Internet Security для Android.

По нашей оценке, общее количество реально действующего вредоносного ПО на мобильных устройствах намного выше официальных показателей. Ограниченные возможности телеметрии не позволяют отследить и уничтожить все зловреды. Мы считаем, что в 2018 году увеличение частоты атак и совершенствование технологий их обезвреживания приведет к возникновению более сложных APT-зловредов для мобильных платформ.

Больше атак с учетом веб-профилирования через платформы типа BeEF

В операционные системы изначально встраивают неплохие средства безопасности и предотвращения атак, из-за чего цены на эксплойты нулевого дня взлетели в 2016 и 2017 годах. К примеру, в свежайшем списке выплат Zerodium за полный удаленный устойчивый джейлбрейк iOS, т. е. удаленное заражение без какого-либо взаимодействия с пользователем, предлагают заплатить 1,5 млн долларов США.



Чтобы заполучить такие эксплойты, некоторые государственные заказчики готовы расстаться с невероятными суммами. Как следствие, все больше усилий тратится на защиту эксплойтов такого класса от случайного разглашения. Для этого злоумышленники затрачивают на порядок больше времени на разведку перед реальной атакой. В ходе разведки киберпреступник может попытаться точно определить версии браузера, операционной системы, плагинов и стороннего ПО на компьютере жертвы. С этими сведениями исполнитель атаки может слегка изменить эксплойт, чтобы он использовал уязвимости первого или энного дня, и без необходимости не применять свои самые *ценные разработки*.

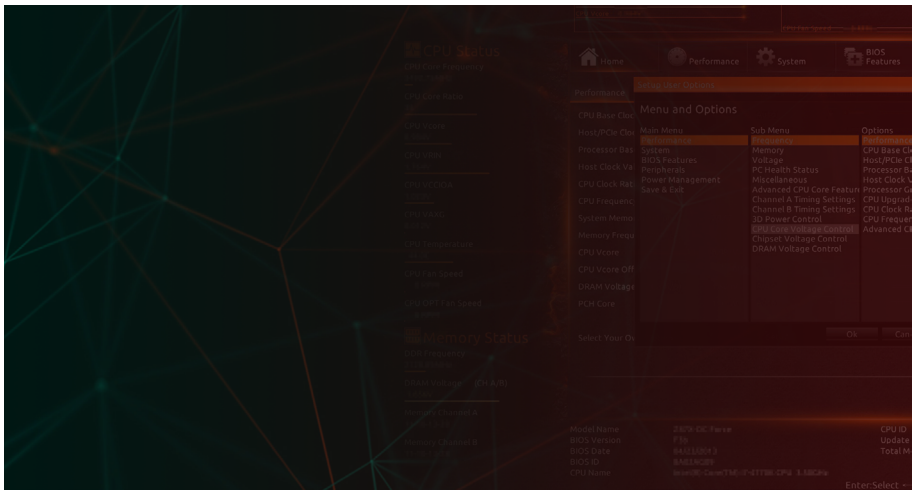
В 2018 году наборы инструментов для профилирования наподобие BeEF, как общедоступные, так и самодельные, еще больше распространятся среди хакеров.

Такие APT-группировки, как Turla, Sofacy и Newsbeef (еще известны как Newscaster, Ajax Security Team или Charming Kitten) почти никогда не брезгуют профилированием. Некоторые APT-группы создают свои платформы для профилирования, такие как Scanbox. Учитывая широкую распространенность таких платформ и острую необходимость в защите дорогостоящих средств нападения, мы прогнозируем, что в 2018 году наборы инструментов для профилирования наподобие BeEF, как общедоступные, так и самодельные, еще больше распространятся среди хакеров.

Продвинутые атаки на UEFI и BIOS

Unified Extensible Firmware Interface (UEFI) — это программный интерфейс, выступающий прослойкой между прошивкой и ОС современных компьютеров. Этот стандарт в 2005 году был принят альянсом ведущих разработчиков программного и аппаратного обеспечения, в числе которых и Intel, после чего он стремительно начал вытеснять классический стандарт BIOS. Его популярность обусловлена наличием отсутствующих в BIOS расширенных функций, таких как возможность устанавливать и запускать исполняемые файлы, доступ к сети и Интернету, шифрование, процессоронезависимая архитектура и драйверы и пр. Такая широкая функциональность, ставшая коньком платформы UEFI, породила совершенно новый класс уязвимостей, невозможных в ограниченной среде BIOS. Например, благодаря поддержке сторонних исполняемых модулей можно создавать зловреды, запускаемые напрямую из UEFI до загрузки любых защитных решений и даже ОС.

Первое коммерческое вредоносное ПО под UEFI появилось в 2015 году в виде модулей UEFI команды Hacking Team. Удивительно, что серьезных зловредов на UEFI обнаружили немного, что можно объяснить сложностью обнаружения подобного ПО. Как мы полагаем, в 2018 году мы будем чаще сталкиваться с UEFI-зловредами.



Продолжение разрушительных атак

В 2018 году разрушительные атаки станут более распространенными и закрепят свой статус наиболее заметного кибероружия.

Начиная с ноября 2016 года, эксперты «Лаборатории Касперского» наблюдают за новой волной вайпер-атак, охвативших множество целей на Ближнем Востоке. В новой серии атак применялась разновидность одиозного червя Shamoon, фигурировавшего в атаке на компании Saudi Aramco и Rasgas в 2012 году. После четырехлетней спячки один из самых загадочных вайперов в истории вернулся. Червь Shamoon, также известный как Disttrack, представляет собой семейство зловредов большой разрушительной силы, эффективно уничтожающих все данные на компьютере жертвы. Ответственность за атаку на Saudi Aramco взяла на себя хакерская группа «Рассекающий меч правосудия» (The Cutting Sword of Justice), опубликовавшая свое послание на сервисе Pastebin в день атаки в 2012 году. Свой поступок они мотивировали протестом против монархии в Саудовской Аравии.

Атаки с участием Shamoon 2.0 в ноябре 2016 года были направлены на ключевые отраслевые и финансовые учреждения Саудовской Аравии. Как и у предыдущей версии зловреда, задачей Shamoon 2.0 был массовый вывод из строя компьютерных систем зараженных организаций. В ходе расследования атак с применением Shamoon 2.0 специалисты «Лаборатории Касперского» также натолкнулись на ранее неизвестную разновидность вайперов, нацеленную на предприятия Саудовской Аравии. Мы назвали ее StoneDrill. Вероятнее всего, авторами этого вайпера являются хакеры из APT-группировки Newsbeef.

Кампании Shamoon и StoneDrill не были единственными разрушительными атаками в 2017 году. Атака ExPetr/NotPetya, на первый взгляд казавшаяся вымогательством, на деле оказалась грамотно завуалированным вайпером. Вслед за ExPetr прошли новые волны атак с псевдовымогателями, оставившие жертв практически без надежды на восстановление данных. Все они пополнили список «вайперов-вымогателей». Мало кто знает, но в 2016 году APT-группировка CloudAtlas запустила серию аналогичных атак с псевдовымогателями, направленную на финансовые учреждения России.

Мы ожидаем, что в 2018 году разрушительные атаки станут более распространенными и закрепят свой статус наиболее заметного кибероружия.

Скомпрометированное шифрование

В 2018 году будут обнаружены и исправлены новые серьезные уязвимости в шифровании как в самих стандартах, так и в отдельных реализациях.

В марте 2017 года эксперты заподозрили неладное в реализации шифрования по методам Simon и Speck для IoT-устройств, подготовленной АНБ. После этого обе заявки на сертификацию ISO отозвали, а их подачу перенесли во второй раз.

В августе 2016 года компания Juniper Networks заявила об обнаружении двух загадочных бэкдоров в сетевых экранах NetScreen. Пожалуй, самое интересное в этой парочке то, что они основаны на незначительном изменении констант в генераторе случайных чисел Dual_EC, узнав которые, злоумышленник сможет расшифровывать VPN-трафик с устройств NetScreen. Оригинальный алгоритм Dual_EC был спроектирован в АНБ и утвержден Национальным институтом стандартов и технологий США. Еще в 2013 году в расследовании Reuters высказывалось предположение, что АНБ заплатила компании RSA 10 миллионов долларов, чтобы та применяла в своих устройствах несовершенный алгоритм, допускающий компрометацию шифрования. Хотя о возможном существовании этого бэкдора узнали еще в 2007 году, некоторые компании, например Juniper, все равно продолжили пользоваться этим алгоритмом. Они лишь использовали другой набор констант, что в теории должно было обеспечить защиту их данных. По всей видимости, такой подход серьезно раздосадовал некоего APT-хакера. Он взломал системы Juniper и заменил константы на свой набор, чтобы управлять VPN-подключениями и расшифровывать трафик.

Все эти попытки скомпрометировать шифрование не остались незамеченными. В сентябре 2017 года международная команда экспертов в области криптографии вынудила АНБ отказаться от двух новых алгоритмов шифрования, которые агентство хотело стандартизировать.

В октябре 2017 года появилась новость о недоработке в криптографической библиотеке, на которой компания Infineon основывала генерацию простых чисел RSA-шифрования в своих чипах. Хотя свидетельств в пользу умышленного саботажа нет, поневоле задумаешься, а так ли безопасны ключевые технологии шифрования смарт-карт, беспроводных сетей или интернет-трафика. Мы считаем, что в 2018 году будут обнаружены и исправлены новые серьезные уязвимости в шифровании как в самих стандартах, так и в отдельных реализациях.

Кризис пользовательской идентификации в электронной коммерции

Последние несколько лет запомнились растущим числом масштабных и даже катастрофических утечек данных, идентифицирующих личность (PII). Свежайший пример — утечка из компании Equifax, которая затронула 145,5 миллионов американцев. Постоянные утечки уже давно никого не удивляют. Впрочем, нужно понимать, что масштабное разглашение PII ставит под удар фундаментальные основы электронной коммерции и целесообразность пересылки важных документов через Интернет. Все мы слышали о случаях мошенничества и кражи личных данных, но что будет, если широко распространенные средства идентификации пользователей в какой-то момент окажутся абсолютно ненадежными? Коммерческие и государственные структуры, особенно в США, станут перед выбором. Им придется либо отказаться от использования Интернета в повседневных делах, либо разориться на внедрение других многофакторных решений. Возможно, опасения напрасны и стандартом безопасности личных данных и транзакций станут более надежные методы идентификации, такие как ApplePay. Но пока этого не случилось, интернет может сдать свои позиции ключевого средства оптимизации скучных бюрократических процессов и сокращения операционных расходов.

Больше взломанных роутеров и модемов

Зачастую роутеры и модемы работают на базе проприетарного ПО, за которым никто не следит и которое никто не обновляет.

Еще один известный рассадник уязвимостей, который стараются не замечать, — роутеры и модемы. Повсюду, дома и на работе, мы полагаемся на них в решении повседневных задач. Но зачастую эти устройства работают на базе проприетарного ПО, за которым никто не следит и которое никто не обновляет. Эти крохотные компьютеры — привратники, открывающие нам дверь в Интернет. Это делает их главной целью злоумышленников, которые хотят незаметно и надолго закрепиться в вашей сети. Одно недавнее интересное исследование продемонстрировало, что в некоторых случаях киберпреступники могут имитировать различных пользователей Интернета, маскируя свои действия совершенно другим адресом подключения. Это серьезное преимущество, особенно с учетом популярности тактик запутывания и операций «под чужим флагом». Мы не сомневаемся, что углубленный анализ подобных устройств неизбежно приведет к новым удивительным открытиям.

Социальный хаос

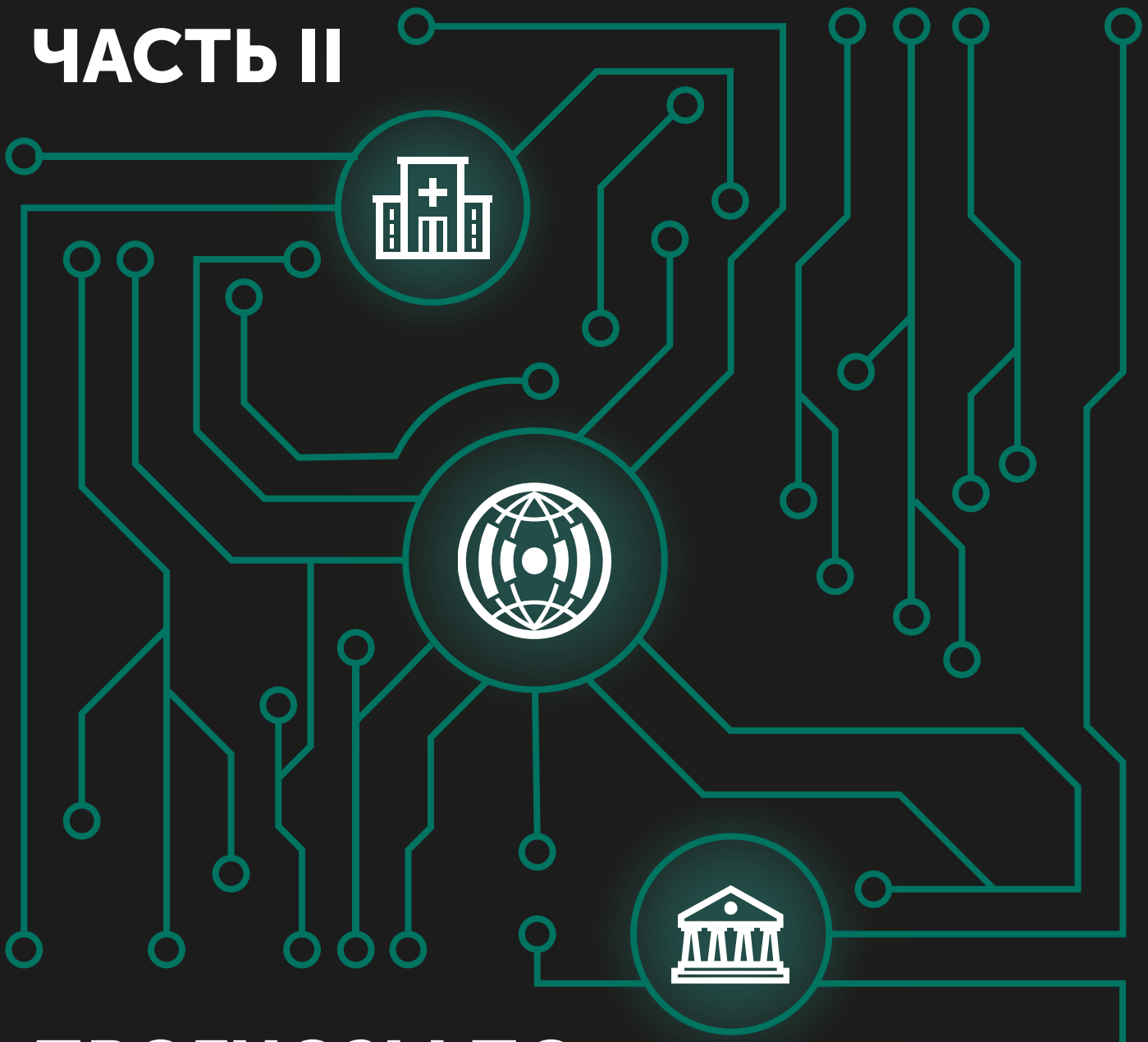
Любовь к информационным войнам в прошлом году вылилась в ряд громких утечек информации и политических скандалов. Никто и представить не мог, что социальные сети станут столь мощным политическим орудием. Неважно, кто его использует — политические «эксперты» или авторы «Южного Парка», публикующие юмористические выпады в адрес гендиректора Facebook. Очевидно лишь то, что рядовые пользователи ждут от администрации популярных соцсетей хотя бы проверки фактов в публикуемых сообщениях и зачистки подставных пользователей или ботов, пытающихся добиться несоразмерного социального влияния. К сожалению, владельцы соцсетей, оценивающие свою успешность по ежедневному числу активных пользователей, не слишком торопятся устранять ботов. Их эта проблема не интересует, даже если боты действуют в открытую или с легкостью вычисляются независимыми экспертами. Мы ожидаем, что явные злоупотребления будут продолжаться и что крупные ботсети станут еще доступнее. Кроме того, само общение в соцсетях станет восприниматься публикой в более негативном ключе, что спровоцирует отток посетителей в другие сервисы, где не пренебрегают комфортом участников ради прибыли и красивой статистики.

ВЫВОД

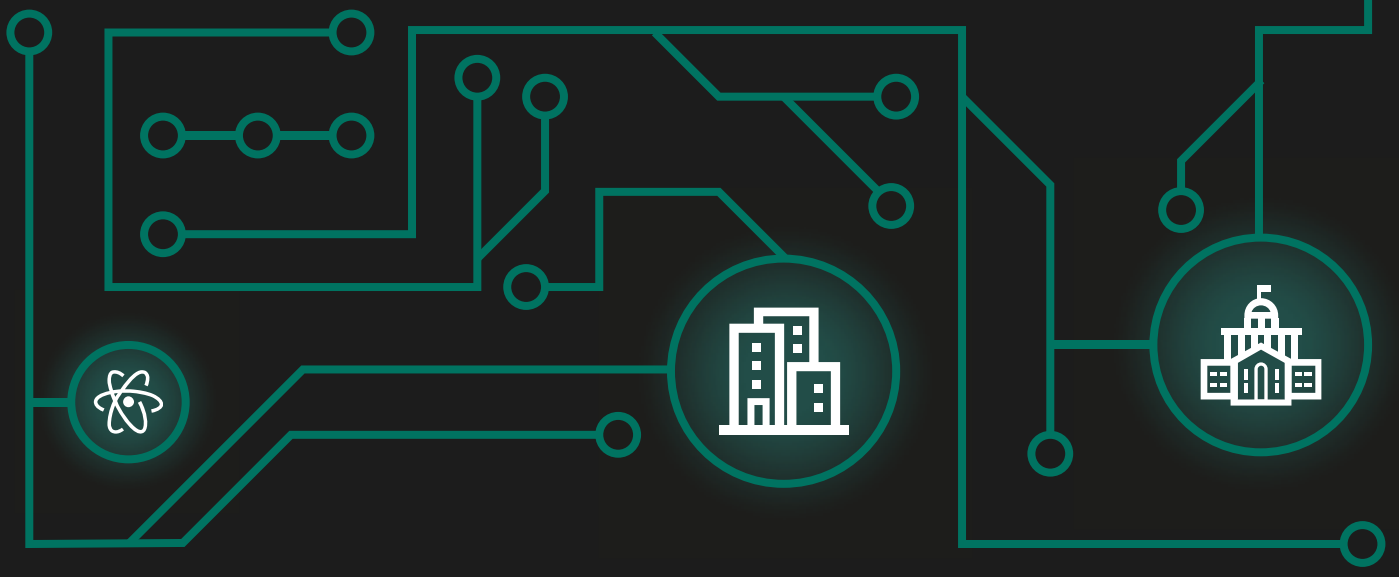
В 2017 году мы предрекли конец индикаторов заражения. Мы считаем, что в 2018 году опытные киберпреступники будут проводить оригинальные и необычные атаки, осваивая новый, устрашающий арсенал. Ежегодные темы и тренды не стоит рассматривать отдельно друг от друга – они тесно взаимодействуют, образуя ландшафт угрозы безопасности, актуальный для всех, от пользователей до бизнеса и правительств. Мы не знаем, когда это закончится, но знания об угрозах и их понимание будут мощными инструментами в ваших руках.

Наши прогнозы относительно APT-угроз охватывают основные тренды, но отдельные отрасли промышленности столкнутся с собственными вызовами. Мы хотим пролить свет на некоторые из них, которые будут актуальны в 2018 году.

ЧАСТЬ II



ПРОГНОЗЫ ПО ОТРАСЛЯМ И ТЕХНОЛОГИЯМ



Прогнозируемые угрозы в автомобильной отрасли

ЛАНДШАФТ УГРОЗ В 2017 ГОДУ

Современные автомобили — это уже не просто электромеханический транспорт. С каждым последующим поколением происходит интеграция интеллектуальных и коммуникационных технологий в автомобили, что, в свою очередь, делает их умнее, эффективнее, комфортнее и безопаснее. Рынок «подключенных» автомобилей увеличивается, демонстрируя годовой темп роста в 45% — в 10 раз быстрее общего рынка автомобилей.

Рынок «подключенных» автомобилей увеличивается, демонстрируя годовой темп роста в 45% — в 10 раз быстрее общего рынка автомобилей.

В некоторых регионах, таких как ЕС или Россия, в целях безопасности и мониторинга повсеместно внедряются двусторонние системы связи (eCall, ERA-GLONASS). Все крупные производители предлагают своим клиентам услугу удаленного управления автомобилем через веб-интерфейс или мобильное приложение.

Удаленная диагностика неисправностей, телематика и информационно-развлекательные системы с выходом в Интернет значительно повышают комфорт и безопасность водителя, но вместе с тем представляют новый вызов для всей автомобильной отрасли, так как превращают автомобиль в очередную цель для кибератак. С учетом растущего риска взлома автомобиля, ставящего под удар приватность водителя, его безопасность и сохранность вложений, производителям важно понять уровень угрозы и заняться IT-безопасностью. В течение нескольких последних лет мы выявили (здесь, здесь и здесь) типичные уязвимости «подключенных» автомобилей.

ЧЕГО ЖДАТЬ В 2018 ГОДУ?

Компания Gartner прогнозирует, что уже до конца 2020 года на дорогах будет четверть миллиарда «подключенных» автомобилей. Другие исследования говорят о том, что примерно 98% автомобилей будут подключены к Интернету. Уже имеющиеся и ожидаемые в следующем году угрозы говорят об одном — чем больше «подключенных» автомобилей, тем больше возможностей и пространства для атаки.

В ближайшие 12 месяцев автомобильная отрасль столкнется со следующими угрозами:

Уязвимости, возникающие по невнимательности или некомпетентности производителя, усугубляемые конкурентным давлением. Спектр подключенных мобильных сервисов будет расти столь же стремительно, как и количество поставщиков, разрабатывающих и предоставляющих эти сервисы. Растущие объемы поставок (и возможное непостоянство качества продуктов/поставщиков) в сочетании с жесткой конкуренцией на рынке могут привести к уязвимостям и брешам, облегчающим задачу злоумышленникам.

Уязвимости, возникающие по причине повышенной сложности продукта и сервисов. Производители автомобилей будут стремиться предоставить клиентам как можно больше взаимосвязанных сервисов. Каждый новый компонент может скрывать в себе лазейку, которой непременно воспользуются преступники. Злоумышленнику достаточно найти лишь одну незащищенную область — Bluetooth-гарнитуру или систему загрузки музыки, — через которую он сможет захватить контроль и нанести ущерб критически важным электрическим компонентам, таким как тормоза или двигатель.

Ни один программный код нельзя на 100% защитить от багов, а там, где есть баги, будут и эксплойты. В автомобилях уже сейчас насчитывается более 100 миллионов строк кода. Даже в текущем виде это огромная поверхность атаки для киберпреступников. По мере установки новых элементов в автомобили объем кода вырастет, что повлечет за собой увеличение количества багов. Некоторые представители автомобильной отрасли, включая Tesla, уже организовали специальные программы по отлову багов.

ПО будут создавать разные разработчики, устанавливать разные поставщики, и оно будет опираться на различные платформы управления. В итоге ни у кого из участников не будет полной картины исходного кода автомобиля. И такая ситуация поможет злоумышленникам избежать обнаружения.

Приложения работают на киберпреступников. Мобильных приложений, в том числе для владельцев автомобилей, становится все больше. С помощью таких приложений водители могут удаленно открывать автомобиль, определять его местоположение или проверять статус двигателя. Исследователи уже на практике доказали уязвимость подобных приложений. Вскоре стоит ждать появления приложений с троянцами, способных закинуть зловред в самое сердце автомобиля ничего не подозревающей жертвы.

«Подключенные» компоненты все чаще разрабатываются и внедряются компаниями, более знакомыми с аппаратным, чем с программным обеспечением. Как правило, такие компании недооценивают важность постоянных обновлений. Удаленное исправление известных проблем станет если не невозможным, то весьма затруднительным. На отзыв автомобилей будет уходить много времени и средств, и многие автолюбители останутся беззащитными.

«Подключенные» автомобили будут создавать и обрабатывать еще больше информации как о самом автомобиле, так и о водителе. Злоумышленники будут продавать эти данные на черном рынке или использовать их для шантажа и вымогательства. Уже сейчас на производителей автомобилей давят маркетинговые компании, жаждущие получить законный доступ к информации о пассажире и его путешествии, чтобы рекламировать свои услуги в реальном времени с учетом местоположения автомобиля.

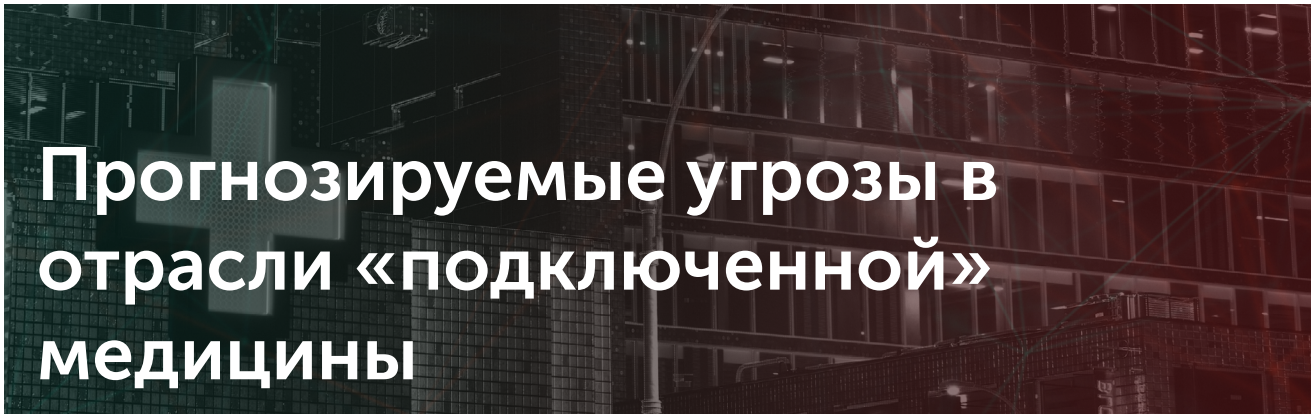
К счастью, за счет растущей осведомленности и осознания важности угроз безопасности на рынке появятся первые аппаратные средства защиты для удаленной диагностики и телематики.

В дальнейшем законодателями будут разработаны требования и рекомендации по обязательному внедрению средств киберзащиты во все «подключенные» автомобили.

Наконец, существующие сертификаты безопасности дополнят новые организации, ответственные за сертификацию по кибербезопасности. Они будут оценивать степень устойчивости «подключенных» автомобилей к кибератакам по четко сформулированным критериям.

Рекомендованные действия

Адекватным ответом на все риски станет внедрение стандартов безопасности на этапах проектирования и разработки. Эти стандарты будут сосредоточены на различных частях экосистемы «подключенного» автомобиля. Защитные программные решения могут быть локально установлены на индивидуальные электрические компоненты, например тормозную систему. Программное решение сможет защитить всю внутреннюю сеть автомобиля путем проверки сетевых коммуникаций, отмечая любые изменения в стандартном поведении автомобильной сети и предотвращая распространение атак. Главное — разработать решение, которое позволит защитить все компоненты с внешним доступом к Интернету. Облачные службы безопасности могут отслеживать и отражать угрозы еще до того, как они достигнут автомобиля. Кроме того, через них «по воздуху» в режиме реального времени могут распространяться различные обновления и другие сведения. Все эти средства должны быть спроектированы с высокой степенью надежности и соответствовать всем стандартам индустрии.



Прогнозируемые угрозы в отрасли «подключенной» медицины

ЛАНДШАФТ УГРОЗ В 2017 ГОДУ

Мы обнаружили в открытом доступе около 1500 устройств, обрабатывающих снимки пациентов.

В 2017 году исследование «Лаборатории Касперского» показало незащищенность медицинской информации и данных пациента, размещенных в «подключенной» инфраструктуре здравоохранения. Как оказалось, информация лежит в открытом доступе в Интернете, где ее без проблем могут найти киберпреступники. К примеру, мы обнаружили в открытом доступе около 1500 устройств, обрабатывающих снимки пациентов. Более того, значительная часть «подключенного» медицинского ПО и веб-приложений содержит уязвимости, для которых уже известны эксплойты.

Ставки высоки, ведь киберпреступники все больше осознают ценность медицинской информации, ее доступность и готовность медицинских учреждений платить за восстановление данных.

ЧЕГО ЖДАТЬ В 2018 ГОДУ?

Количество угроз в отрасли здравоохранения будет возрастать одновременно с количеством «подключенных» устройств и уязвимых веб-приложений. Развитие отрасли «подключенной» медицины обусловлено рядом факторов. Это потребность в ресурсах и их эффективном использовании; острая необходимость в удаленном, домашнем уходе при хронических заболеваниях, таких как диабет, или заботе о пожилых людях; желание людей вести здоровый образ жизни; польза совместного доступа разных учреждений к данным и отслеживаемым показателям пациента, что значительно улучшает качество и эффективность медицинского ухода.

Количество угроз в отрасли здравоохранения будет возрастать одновременно с количеством «подключенных» устройств и уязвимых веб-приложений.

В ближайшие 12 месяцев в этой отрасли мы столкнемся со следующими угрозами:

Увеличение количества атак на медицинское оборудование для организации вредоносных сбоев, вымогательства или других преступных действий. Количество специализированного медицинского оборудования с подключением к компьютерным сетям будет только расти. Большинство таких сетей изолированы, но даже одного внешнего интернет-соединения достаточно, чтобы пробить защиту и распространить вредоносную программу в «закрытой» сети. Атака на оборудование может прервать уход за пациентом или вообще оказаться фатальной. Как следствие, медучреждения с готовностью будут платить преступникам.

Вырастет количество целевых атак с целью кражи данных. С каждым днем растет количество медицинской информации и данных о пациенте, которые хранятся и обрабатываются «подключенной» системой здравоохранения. Информация подобного рода очень ценится на черном рынке и может быть использована для шантажа и вымогательства. Такие данные заинтересуют не только киберпреступников: работодатель жертвы или ее страховая компания могут получить информацию, влияющую на выплату премий или даже на безопасность труда.

Возникнет еще больше инцидентов, связанных с атаками программ-вымогателей на учреждения здравоохранения. Это приведет к блокировке устройств и шифрованию данных: «подключенное» медицинское оборудование стоит немалых средств, и от него зависят жизни людей, что делает его целью номер один для атак и вымогательства.

В медицинских учреждениях станет еще сложнее соблюдать четко заданный корпоративный периметр, так как все больше рабочих станций, серверов, мобильных устройств и оборудования будут подключены к Интернету. Каждое такое устройство открывает злоумышленникам новые направления атаки для доступа к медицинским сетям и всей сопутствующей информации. Обеспечение обороны и защита конечных точек станет настоящим испытанием для отделов безопасности учреждений здравоохранения, ведь теперь каждое новое устройство образует очередную точку входа в корпоративную инфраструктуру.

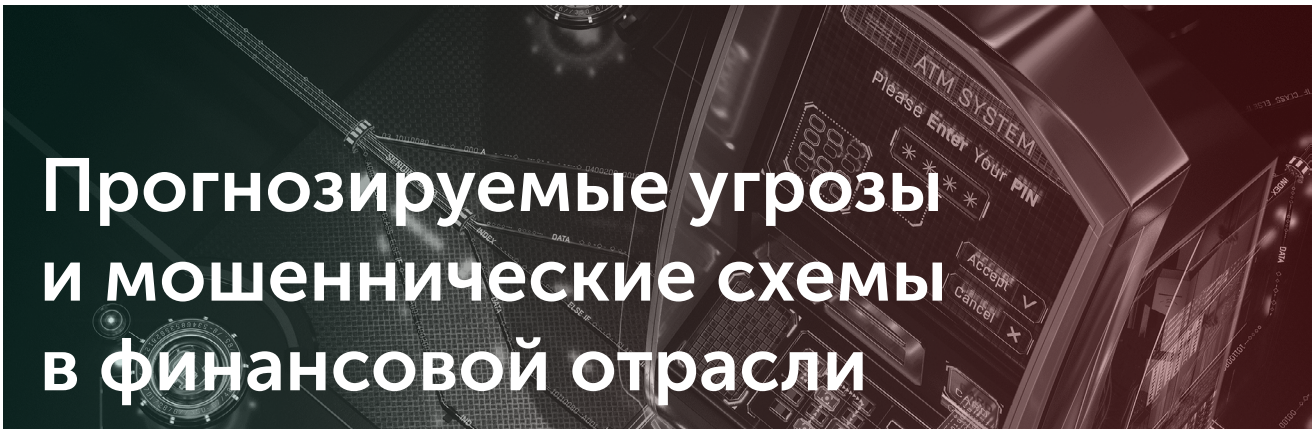
Целью преступников станет перехват личных и конфиденциальных данных между «умными» носимыми устройствами, например имплантами, и медработниками. Использование таких устройств в целях медицинской диагностики, лечения и профилактики растет с каждым днем. Электрокардиостимуляторы и инсулиновые помпы — наиболее показательные примеры.

Общегосударственные и региональные системы здравоохранения, передающие в незашифрованном или незащищенном виде данные между частными специалистами, больницами, клиниками и другими учреждениями, — легкая мишень для злоумышленников, которые перехватывают данные в обход корпоративных сетевых экранов. Это же относится к данным, которыми обмениваются медицинские учреждения и страховые компании.

Широкая распространенность фитнес-гаджетов и других «подключенных» устройств для здорового образа жизни позволяет киберпреступникам похищать персональные данные, преодолев минимальную защиту. Популярность «подключенного» здорового образа жизни привела к тому, что фитнес-браслеты, трекеры и смарт-часы хранят и передают огромное количество конфиденциальной информации при достаточно слабой защите — и киберпреступники не упустят возможности использовать это в своих целях.

Деструктивные атаки, будь то DoS-атаки или уничтожение данных через программы-вайперы (такие как WannaCry), станут серьезной угрозой цифровым системам медицинских учреждений. Постоянно увеличивающееся количество рабочих станций, электронное управление записями и цифровые бизнес-процессы — это фундамент любой современной организации, который расширяет поверхность атаки для киберпреступников. В такой сфере, как здравоохранение, скорость работы играет решающую роль, и любое вмешательство может поставить жизнь пациента под угрозу.

Развивающиеся технологии, такие как интеллектуальные искусственные конечности и импланты для физиологических улучшений или встроенной дополненной реальности, не только позволяют людям с ограниченными возможностями приспособиться, почувствовать себя лучше и сильнее, но и несут в себе угрозу. Именно поэтому крайне важно интегрировать системы безопасности в эти технологии на ранних этапах проектирования.



Прогнозируемые угрозы и мошеннические схемы в финансовой отрасли

ЛАНДШАФТ УГРОЗ В 2017 ГОДУ

В 2017 году мы видели, что атаки на финансовые учреждения все чаще были направлены на счета клиентов.

В 2017 году мы видели, что атаки на финансовые учреждения все чаще были направлены на счета клиентов. Благодаря множеству успешно организованных утечек киберпреступники заполучили персональные данные, которые позволяют получить доступ к банковским счетам и проводить атаки с использованием поддельной личности. Такие атаки приводят не только к утере данных, но и к потере доверия клиентов. Решение этой проблемы — в интересах как финансовых организаций, так и их клиентов.

ЧЕГО ЖДАТЬ В 2018 ГОДУ?

Следующий год в стремительно развивающемся сегменте финансовых услуг будет годом инноваций. Появление новых каналов взаимодействия и видов финансовых услуг приведет к возникновению новых угроз. Представителям финансового сектора нужно сосредоточиться на предотвращении мошенничества по всему периметру, чтобы успешно пресекать мошеннические операции, мигрирующие с онлайн-счетов в новые каналы взаимодействия. По мере роста прибыльности успешных атак недавно появившиеся популярные платежные системы будут все чаще отбиваться от нападений злоумышленников.

Сложности обработки платежей в реальном времени

Появление новых каналов взаимодействия и видов финансовых услуг приведет к возникновению новых угроз.

С повышением спроса на обрабатываемые в реальном времени и международные финансовые транзакции компании будут вынуждены еще быстрее оценивать риски. Клиенты платежных систем не терпят задержек, что дополнительно усложняет задачу. Финансовым учреждениям придется переосмыслить процесс «знай своего клиента» (KYC), сделав его более эффективным. Ключевым инструментом для быстрого обнаружения мошеннических операций и оценки рисков станет машинное обучение и решения на базе ИИ.

Социальная инженерия

Финансовые организации не должны упускать из виду старые методы атаки. На фоне более серьезных и передовых угроз по-прежнему процветают фишинг и социальная инженерия. Они до сих пор остаются простейшим и наиболее прибыльным видом атак, эксплуатирующих человеческие слабости. Чтобы этому противостоять, нужно повышать осведомленность своих клиентов и персонала об актуальных атаках и мошеннических схемах.

Угрозы на мобильных устройствах

Согласно последним данным индекса кибербезопасности Kaspersky Cybersecurity Index, пользователи все чаще проводят онлайн-операции с мобильных устройств. Например, в настоящее время 35% людей пользуются интернет-банками на своих смартфонах и 29% — системами онлайн-платежей (в предыдущем году — 22% и 19% соответственно). Пользователи, отдающие предпочтение мобильным устройствам, или Mobile First, станут одной из главных целей мошеннических схем. Киберпреступники найдут новые хитроумные способы кражи банковских учетных данных, применяя как проверенные, так и новые семейства зловредов. В 2017-м мы обнаружили модифицированного представителя семейства зловредов Svpeng. В 2018 году появятся другие семейства мобильного вредоносного ПО, ориентированные на кражу банковских реквизитов более изощренными способами. Одной из ключевых задач финансовых организаций станет раннее обнаружение и удаление мобильных зловредов.

В настоящее время 35% людей пользуются интернет-банками на своих смартфонах и 29% — системами онлайн-платежей.

Утечки данных

В 2018 году общественность всколыхнут очередные новости об утечках данных, после чего финансовые организации будут разбираться с подставными клиентами и захватом банковских счетов. Несмотря на сложность организации утечки данных, преступникам намного выгоднее за один раз украсть огромные объемы данных клиентов, чем атаковать отдельных пользователей. Учреждения финансовой отрасли обязаны регулярно тестировать свои защитные системы и пользоваться решениями для раннего обнаружения подозрительных действий учетных записей.

Кража криптовалюты

Все больше организаций экспериментируют с криптовалютами, привлекая к себе внимание киберпреступников. 2017 год ознаменовался расцветом вредоносного майнерского ПО, и в 2018 году злоумышленники не оставят попыток нажиться на криптовалюте. Организациям нужно применять решения для обнаружения современных семейств вредоносных программ и основывать свою стратегию предупреждения угроз на актуальных аналитических данных. [Подробные сведения об этой угрозе см. в разделе «Прогнозируемые угрозы для криптовалют».]

Захват платежных счетов

Более защищенные методы физических платежей на основе чипов и другие улучшения в кассовых терминалах вынудили мошенников плотнее заняться онлайн-платежами. Но и тут прогресс не стоит на месте — за безопасность онлайн-платежей отвечают токены, биометрическая идентификация и другие технологии, из-за которых преступники переключились на кражу учетных данных. Отраслевые эксперты полагают, что мошенничество подобного типа может вылиться в многомиллиардные убытки. Поставщики финансовых услуг должны переосмыслить методы цифровой идентификации и перейти на инновационные решения, безошибочно подтверждающие подлинность клиентов в любой ситуации.

Вынужденные инновации

В 2018 году все больше предприятий будут инвестировать в платежные системы и решения на основе «открытого банкинга». Лишь благодаря инновациям финансовые организации смогут выделиться из огромной толпы конкурентов. Но в погоне за клиентами инноваторы могут не разобраться во всех тонкостях нормативных требований и не гарантировать защищенность новых каналов. Мошенники будут под микроскопом изучать каждое новое решение сразу после его выпуска, и если новинка изначально не проектировалась с акцентом на безопасность, скорее всего, она без проблем будет скомпрометирована киберпреступниками.

Мошенничество как услуга

Теневые международные каналы связи между киберпреступниками позволяют им быстро обмениваться знаниями и стремительно развертывать атаки по всему миру. В «подпольном» Интернете доступны самые разные мошеннические услуги — от ботнетов и фишинговых атак до средств удаленного доступа. Подобные услуги и инструменты приобретают менее опытные киберпреступники, а значит, финансовым организациям придется отражать еще большее число атак. Чтобы противостоять таким атакам, нужно обмениваться знаниями между отделами и пользоваться сервисами анализа угроз.

Взлом банкоматов

Банкоматы, как и раньше, будут привлекать повышенное внимание киберпреступников. В 2017 году специалисты «Лаборатории Касперского» обнаружили атаки на системы банкоматов с применением новых зловредов, удаленных и бесфайловых операций, а также специализированный банкоматный зловред Cutlet Maker, который открыто продавался за несколько тысяч долларов на «подпольном» интернет-рынке вместе с пошаговой инструкцией по применению. «Лаборатория Касперского» опубликовала отчет о прогнозируемых сценариях атак на банкоматы, сосредоточенных на взломе систем аутентификации.

Прогнозируемые угрозы в сфере промышленной безопасности

ЛАНДШАФТ УГРОЗ В 2017 ГОДУ

Наиболее значительной угрозой для промышленных систем в 2017 году стали атаки шифровальщиков-вымогателей.

2017 год был одним из самых насыщенных в плане инцидентов, связанных с информационной безопасностью промышленных систем. Эксперты по безопасности обнаружили сотни новых уязвимостей, исследовали новые векторы атаки на АСУ ТП и технологические процессы, собрали и проанализировали статистику случайных заражений промышленных систем и обнаружили целевые атаки на промышленные предприятия (в частности, Shamoon 2.0/StoneDrill). Кроме того, впервые после Stuxnet был обнаружен и исследован вредоносный инструментарий, предназначенный для проведения атак на физические системы – CrashOverride/Industroyer. Некоторые специалисты стали относить его к категории кибероружия.

Однако наиболее значительной угрозой для промышленных систем в 2017 году стали атаки шифровальщиков-вымогателей. По данным Kaspersky Lab ICS CERT, в первой половине года промышленные информационные системы в 63-х странах мира подверглись множественным атакам с использованием программ-шифровальщиков, относящихся к 33 различным семействам. Судя по всему, разрушительные атаки программ-вымогателей WannaCry и ExPetr навсегда изменили отношение промышленных предприятий к проблеме защиты ключевых производственных систем.

ЧЕГО ОЖИДАТЬ В 2018 ГОДУ?

Рост числа случайных заражений вредоносным ПО

За редкими исключениями киберпреступные группировки пока не нашли простых и надежных схем монетизации атак на промышленные информационные системы. В 2018 году продолжатся случайные заражения и инциденты в промышленных сетях, вызванные «обычным» вредоносным ПО, предназначенным для атак на традиционные мишени, такие как корпоративные сети. Вероятно, в будущем последствия таких заражений для индустриальных сред будут все более серьезными. Проблема регулярного обновления ПО в промышленных системах по образцу корпоративных сетей остается нерешенной, несмотря на многократные предупреждения экспертов по информационной безопасности.

Увеличение риска целевых атак с применением программ-вымогателей

Атаки WannaCry и ExPetr показали как экспертам по безопасности, так и киберпреступникам, что технологические сети могут быть даже более уязвимыми для подобных атак, чем корпоративные, и также могут быть доступны из интернета. Более того, ущерб от активности вредоносного ПО в технологической сети может превышать вред, наносимый этим же ПО в корпоративной сети, а «тушить пожар» в промышленной сети гораздо труднее. Хуже всего, наверное, то, что, по опыту инцидентов стало понятно, насколько на промышленных предприятиях плохо организованы и неэффективны действия персонала в случае кибератаки на технологическую инфраструктуру. Все эти факторы делают промышленные системы привлекательными мишенями для атак с применением программ-вымогателей.

Увеличение числа инцидентов, связанных с промышленным кибершпионажем

Интерес киберпреступников к целевым атакам на промышленные компании с применением программ-вымогателей может стать локомотивом развития еще одного направления киберпреступной деятельности – кражи данных из промышленных информационных систем для подготовки и реализации целевых атак (в том числе с применением программ-вымогателей).

Новые сегменты подпольного рынка, обслуживающие атаки на промышленные системы

В последние годы на черном рынке растет спрос на эксплойты нулевого дня для систем АСУ ТП. Это говорит о том, что преступники готовят целевые атаки на промышленные предприятия. В 2018 году мы ожидаем активизации злоумышленников в этом направлении, что, вероятно, приведёт к появлению новых сегментов киберкриминального рынка, ориентированных на кражу сведений о конфигурации систем АСУ ТП и данных для доступа к этим системам. Кроме того, возможно, на рынке появятся предложения ботнетов с «промышленными» узлами. Подготовка и реализация сложных кибератак на физические объекты и системы требует экспертных знаний об АСУ ТП и о специфике отраслей, в которых они применяются. Спрос на такие дефицитные экспертные знания, вероятно, приведет к развитию таких услуг как «вредоносное ПО как сервис», «разработка векторов атаки как сервис», «организация атак на заказ» и т.д., ориентированных именно на атаки на промышленные предприятия.

Появление новых видов вредоносного ПО и вредоносных инструментов

Вероятно, появится новое вредоносное ПО, предназначенное для промышленных сетей и систем. Это ПО будет действовать скрытно, оставаясь в неактивном состоянии в корпоративных сетях, чтобы избежать обнаружения. Оно будет переходить в активный режим в технологической инфраструктуре, уровень защищенности которой значительно ниже. Возможно также появление программ-вымогателей, нацеленных на устройства полевого уровня АСУ ТП и физических систем (насосов, переключателей и т.п.).

Использование преступниками результатов анализа угроз, обнародованных исследователями безопасности

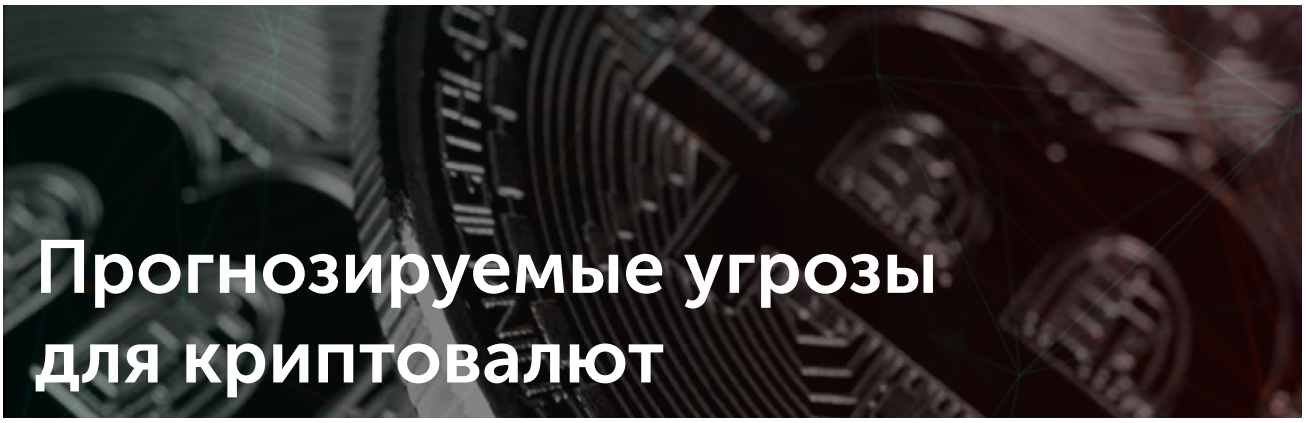
В 2017 году исследователи хорошо поработали: мы узнали о множестве новых векторов атак на промышленные системы и инфраструктуру, был проделан глубокий анализ обнаруженного вредоносного инструментария. Всё это, безусловно, полезно для защиты промышленных объектов. Но, возможно, этой информацией воспользуются и преступники. Например, хактивисты могут использовать опубликованные сведения об инструментах CrashOverride/Industroyer для организации DoS-атак на энергосистемы; преступники могут создать программы-вымогатели, предназначенные для проведения целевых атак или даже придумать схемы монетизации сбоев в электроснабжении. Концепт червя для ПЛК может вдохновить преступников на создание полнофункциональных вредоносных червей, распространяющихся с одного ПЛК на другой, а другие, возможно, попытаются создать вредоносное ПО с помощью одного из стандартных языков программирования для ПЛК. Возможно даже, что кто-то из злоумышленников попытается создать вредоносное ПО для ПЛК, работающее на низком уровне, используя подход, продемонстрированный исследователями ИБ. Оба последних подхода, вероятно, могут создать серьёзную проблему для разработчиков существующих защитных решений.

Изменения в нормативной базе

В 2018 году вступают в силу многие новые инициативы регуляторов, касающиеся промышленных систем автоматизации – как в России, так и в некоторых других странах. В числе прочих последствий это заставит компании, владеющие критически важными объектами инфраструктуры и промышленными объектами, уделять больше внимания оценке их киберзащищенности. Можно ожидать, что результатом этого станет обнаружение новых уязвимостей промышленных систем. Возможно, мы также узнаем об инцидентах на промышленных предприятиях и ранее неизвестных атаках.

Формирование рынка страхования промышленных предприятий от кибер-рисков и рост инвестиций в этот вид страхования

Страхование от рисков, связанных с киберугрозами, становится неотъемлемой частью системы управления рисками на промышленных предприятиях. До недавнего времени риски, связанные с инцидентами кибербезопасности, исключались из контрактов страхования – фактически, страховые компании ставили киберинциденты в один ряд с террористическими атаками. Однако ситуация меняется, и появляются новые инициативы – как со стороны компаний, специализирующихся на кибербезопасности, так и со стороны основных игроков страхового бизнеса. Как следствие, в 2018 году вырастет число проводимых аудитов/оценок защищенности промышленных систем автоматизации и число зарегистрированных и исследованных инцидентов кибербезопасности.



Прогнозируемые угрозы для криптовалют

ЛАНДШАФТ УГРОЗ В 2017 ГОДУ

В первые восемь месяцев 2017 года продукты «Лаборатории Касперского» защитили от криптовалютных майнеров-зловредов 1,65 миллиона пользователей, а к концу года это число превысит два миллиона.

Криптовалюта сегодня интересует не только компьютерных гиков и IT-специалистов. Она начинает влиять на нашу повседневную жизнь больше, чем кажется, и вместе с тем быстро становится лакомым кусочком для киберпреступников. Некоторые киберугрозы в этой сфере унаследованы от электронных платежей: например, подмена адреса целевого счета во время транзакций или кража электронного кошелька. Но при этом криптовалюта открыла совершенно новые способы монетизировать вредоносную деятельность.

В 2017 году главной угрозой для пользователей по всему миру были программы-вымогатели: чтобы восстановить файлы и данные, зашифрованные злоумышленниками, жертвы должны были заплатить выкуп в криптовалюте. В первые восемь месяцев 2017 года продукты «Лаборатории Касперского» защитили от криптовалютных майнеров-зловредов 1,65 миллиона пользователей, а к концу года это число превысит два миллиона. Более того, в 2017 году, после нескольких лет в тени, на арену вновь вышли биткойн-воры.

ЧЕГО ЖДАТЬ В 2018 ГОДУ?

Рост количества, распространения и рыночной ценности криптовалюты не только продолжит притягивать к ней внимание преступников, но и приведет к использованию все более продвинутых приемов и инструментов для ее генерации. Киберпреступники быстро сосредоточатся на наиболее прибыльных схемах добычи денег. Так что 2018 год, по-видимому, станет годом вредоносного веб-майнинга.

Атаки программ-вымогателей заставят пользователей покупать криптовалюту

Злоумышленники продолжат требовать выкупы в криптовалюте, поскольку этот рынок не регулируется и почти анонимен: не нужно передавать никуда данные, адрес никто не заблокирует, а преступника не выследят и не поймают. В то же время дальнейшее упрощение методов монетизации будет способствовать распространению шифровальщиков.

Целевые майнерские атаки

Мы прогнозируем рост целевых атак на компании с целью установки майнерского ПО. В отличие от программ-вымогателей, позволяющих получить потенциально большой, но разовый куш, майнерские программы гарантируют хоть и меньший, зато стабильный доход. Посмотрим в следующем году, что перевесит.

Продолжится рост числа майнеров с вовлечением все новых участников

В следующем году майнинг продолжит расползаться по миру, привлекая больше людей. Вовлечение новых майнеров будет зависеть от их возможностей получить доступ к бесплатным и стабильным источникам электроэнергии. Так, мы будем наблюдать рост «внутреннего майнинга»: все больше служащих госучреждений начнут майнить при помощи казенных компьютеров, и все больше сотрудников производственных предприятий — эксплуатировать корпоративное оборудование.

Веб-майнинг

Веб-майнинг — это метод майнинга криптовалюты непосредственно в браузере с помощью установленного на веб-странице специального скрипта. Киберпреступники уже показали, как легко можно загрузить такой скрипт на взломанный сайт, вовлечь компьютеры посетителей в процесс добычи цифровых денег и в конечном итоге пополнить кошельки злоумышленников. В следующем году веб-майнинг значительно повлияет на саму суть Интернета, открывая все новые способы монетизации веб-сайтов. Один из способов заменит рекламу: за удаление майнингового скрипта сайты будут предлагать пользователям подписаться на платный контент. С другой стороны, в обмен на майнинг пользователи смогут получить бесплатный доступ к развлекательному контенту, например кино. Еще один способ основан на системе проверки безопасности: метод Captcha, позволяющий отличить людей от ботов, будет заменен специальным режимом веб-майнинга. Тогда будет неважно, бот ли посетитель или человек, пока он «платит» майнингом.

Спад системы инвестирования ICO

В 2017 году система ICO (Initial Coin Offering, первичное размещение криптовалюты) пережила стремительный взлет, было собрано более трех миллиардов долларов в различных проектах, большинство из которых так или иначе связаны с технологией блокчейна. Ожидается, что в следующем году эта истерия с ICO пойдет на убыль: череда провальных проектов (когда невозможно создать финансируемый через ICO продукт) заставит более тщательно выбирать объекты для инвестирования. Множество неудачных ICO-проектов может негативно отразиться на обменном курсе криптовалют (биткойны, Ethereum и др.), который в 2017 году продемонстрировал беспрецедентный рост. Таким образом, нас ждет уменьшение абсолютного числа фишинговых и хакерских атак, направленных на ICO, смарт-контракты и кошельки.

Securelist

Kaspersky Daily

Threatpost

Блог Евгения Касперского

Kaspersky Lab ICS CERT

KASPERSKY lab