Октябрь 2018

group-ib.ru

THE HI-TECH CRIME TRENDS 2018

СОДЕРЖАНИЕ

1. КЛЮЧЕВЫЕ ВЫВОДЫ

Аппаратные уязвимости и безопасность BIOS/UEFI

- Если в прошлом году основное внимание специалистов по безопасности было связано с эпидемиями WannaCry, NotPetya, BadRabbit, то в 2018 году самой значительной проблемой стали side-channel атаки и новые уязвимости, обнаруженные в микропроцессорах разных вендоров. Эти уязвимости невозможно эффективно устранить при помощи программных обновлений, они открывают совершенно новые возможности для атакующих и через несколько лет могут сильно повлиять на рынок безопасности.
- Для эксплуатации некоторых аппаратных уязвимостей достаточно выполнения JS-кода, например в случае с уязвимостями Spectre и Glitch.
- Эксплойты для аппаратных и UEFI уязвимостей являются рабочими Proof of Concept (PoC), эксплуатация их в реальных атаках не выявлена. Однако это не значит, что они не используются злоумышленниками уже сегодня: в настоящий момент на рынке кибербезопасности нет решений, которые могли бы выявлять подобного рода угрозы.
- Исследования в этой области, а также разработка реальных эксплойтов — достаточно трудоемкие и дорогие процессы, поэтому «рядовыми» киберпреступниками такие уязвимости пока не эксплуатируются. Проправительственные группировки более заинтересованы и способны инвестировать в подобные исследования и инструменты.

Саботаж и шпионаж

- Фокус перспективной разработки и инноваций в создании сложных вирусов, а также проведении многоступенчатых целевых атак сместился от финансово-мотивированных киберпреступников к проправительственным хакерам. Их действия направлены на обеспечение долговременного присутствия в сетях объектов критической инфраструктуры с целью саботажа и шпионажа за компаниями энергетического, ядерного, водного, авиационного и других секторов.
- Значительная часть атак была направлена на энергетический сектор. Помимо первого специализированного ПО для атак на энергосети Industroyer, обнаруженного в 2016 году, объектам отрасли угрожает Triton — фреймворк, воздействующий на систему безопасности производственных процессов (Safety Instrumented System — SIS) от Schneider Electric.
- В 2017 и в 2018 годах были выявлены две угрозы с нечеткой целью: шифровальщик BadRabbit и вредоносная программа для роутеров VPNFilter. Массовая и наиболее резонансная часть атаки BadRabbit носила эффект дымовой завесы и была призвана скрыть факт целевого вывода из строя объектов, которые были скомпрометированы заранее. VPNFilter удалось выявить на этапе подготовки атаки. Ее цели до сих пор неизвестны, однако один из модулей VPNFilter предназначен для обнаружения SCADA-систем. Обе угрозы связывают с группой BlackEnergy.
- В феврале 2018 года атака с помощью вредоносной программы Olympic Destroyer вывела из строя официальный сайт Зимних Олимпийских игр в Пхенчхане, Wi-Fi на стадионе и вызвала сбой в прямой трансляции церемонии открытия. Этот прецедент демонстрирует потенциал кибератак на объекты, имеющие не только инфраструктурное, но и имиджевое значение для страны.
- Банки также являются объектом критической инфраструктуры, поэтому наличие инструментов и опыта вывода банков из строя является одним из приоритетов атакующих. Такие инструменты активно используют две группы: BlackEnergy и Lazarus.
- Многие группы наряду с собственными разработками начали использовать общеизвестные программы для тестирования на проникновение, а также новые методы сокрытия взаимодействия зараженных устройств с сервером управления. Эти приемы сильно усложняют процесс криминалистического анализа и атрибуции.
- В развитии своих хакерских наборов атакующие

уделяют внимание не только Windows платформам, но и MacOS, а также мобильным операционным системам.

- Все больше интереса проправительственные хакеры проявляют к уязвимостям в домашних маршрутизаторах. Это позволяет им не только шпионить за пользователями, не заражая их девайсы, но и поддерживать более развет-вленную и динамическую инфраструктуру.
- Юго-Восточная Азия — самый активно атакуемый регион. Всего за год в нем была зафиксирована активность 21 APT-группы, что больше, чем в США и Европе.

Сведения об атаках APT-групп поступают в публичный домен крайне избирательно и с большой задержкой. Каждый год всплывают обстоятельства старых атак уже известных групп; на момент обнаружения новых игроков оказывается, что они были активны уже несколько лет, но по разным причинам оставались незамеченными (например, Orangeworm и группа Slingshot, которую связывают с США). Кроме того, данные об активности проправительственных хакеров ряда стран появляются только из утечек (публикации Wikileaks, взлом подрядчиков АНБ США Equation Group и др). Это ставит потенциальных жертв в позицию вечно догоняющих, затрудняет обнару-жение и реагирование на угрозы, упрощая злоумыш-ленникам задачу по обеспечению долгосрочного присутствия в сетях интересующих объектов.

Хищения

Оценка рынка высокотехнологичных хищений в России

H2 2017 – H1 2018, данные Group-IB

Сегмент рынка в России	Кол-во групп	Успешных атак в день	Средняя сумма одного хищения (в RUR)	Средняя сумма хищений в день (в RUR)	H2 2017 - H1 2018 (в RUR)	H2 2017 - H1 2018 (в USD)	Процент изменения
Хищения у юридических лиц с троянами для ПК	**3**	**2**	**1 100 000**	**2 200 000**	**547 800 000**	**$9 130 000**	**-12%**
Хищения у физических лиц с Android-троянами	**8**	**110**	**7 000**	**770 000**	**191 730 000**	**$3 195 500**	**-77%**
Целевые атаки на банки	**3**	**-**	**118 000 000**	**-**	**1 303 900 000**	**$21 731 667**	**-20%**
Фишинг	**26**	**108**	**1 000**	**1 008 000**	**250 992 000**	**$4 183 200**	**6%**
Обналичивание похищаемых средств				**1 336 500**	**919 543 500**	**$15 325 725**	**-34%**
Итого				**5 314 500***	**3 213 965 500**	**$53 556 092**	**-32%**

* Обновлено 1 ноября 2018 года

Целенаправленные атаки на банки

- На текущий момент существует 4 группы, которые представляют реальную угрозу и задают тренды в атаках на банки: они способны не только проникнуть в сеть, добраться до изолированных финансовых систем, но и успешно вывести деньги через SWIFT, АРМ КБР, карточный процессинг и банкоматы. Речь идет о группах Cobalt, MoneyTaker, Silence, состоящих из русскоговорящих хакеров, а также о северокорейской Lazarus.
- В среднем в России каждый месяц киберограблениям подвергались 1-2 банка. Средний ущерб от одного успешного ограбления составляет 132 млн рублей ($2 млн).
- Количество целенаправленных атак на банки с целью хищения через SWIFT увеличилось в три раза. Если за прошлый прошлый период было всего три атаки в Гонконге, Украине и Турции, то в этом произошло девять успешных атак в Непале, Тайване, России, Мексике, Индии, Болгарии и Чили. Для межбанковской системы SWIFT представляют угрозу только две преступные группы: Cobalt и Lazarus. При совершении хищений через SWIFT и Cobalt, и Lazarus тщательно готовили схему обнала. Вероятно, для оптимизации связанных с обналичиванием затрат хищения проводились сразу из двух банков. Как и в предыдущих атаках на SWIFT, вывод большей части похищенных средств удалось остановить.
- Выводом денег через АРМ КБР (автоматизированное рабочее место клиента Банка России) занимается только MoneyTaker — если в ноябре 2017 года им удалось вывести всего 7 млн рублей, то уже летом 2018 года они успешно похитили из «ПИР Банка» 58 млн рублей. В 2017 и 2018 году хакеры из групп Cobalt и Silence игнорировали российскую систему межбанковских переводов АРМ КБР даже в тех случаях, когда им удавалось получить к ней доступ. Сейчас их внимание привлекают более надежные схемы хищений через банкоматы и карточный процессинг. Вместе с тем, Cobalt интересуется локальными системами межбанковских переводов за рубежом.
- Атаки на карточный процессинг остаются одним из основных способов хищений и проводятся группами Cobalt, MoneyTaker, Silence. В результате такой атаки в феврале 2018 года группе Silence удалось снять с карточек через банкоматы партнера банка 35 млн рублей. Фокусировка атак на банкоматах и карточном процессинге привела к уменьшению среднего ущерба от одной атаки. Однако такие атаки несут меньше рисков для преступников и более безопасны для «дропов», обналичивающих украденные деньги: атакующие находятся в одной стране, их жертва (банк) в другой, а обналичка происходит в третьей.
- В анализируемом периоде атаки на платежные шлюзы проводила только группа Cobalt. При этом в 2017 году преступники похитили деньги у двух компаний, а в 2018 не сделали ни одной попытки. В результате реагирования на один из инцидентов специалисты Group-IB установили, что помощь им оказывали участники группы Anunak, которая не осуществляла подобных атак с 2014 года. Несмотря на арест в Испании лидера группы весной 2018 года, Cobalt по-прежнему остается одной из самых активных и агрессивных группировок, 2-3 раза в месяц атакуя финансовые организации в России и за рубежом.
- Атаки с целью заражения банкоматной сети проводят Cobalt, Silence, а также группа MoneyTaker, которая провела первую атаку такого рода в мае 2018 года.

Атаки на клиентов банков. Россия

- Тренд на снижение угроз со стороны банковских троянов для ПК в России продолжается с 2012 года. Атаки на физических лиц ушли в прошлое, а ущерб для юридических лиц по итогам отчетного периода сократился еще на 12% и составил 547 млн рублей ($8,3 млн).
- Только три группы — Buhtrap2, RTM, Toplel — похищают средства со счетов юридических лиц в России. Основным способом хищения является удаленное управление или автоматические переводы через системы бухгалтерского учета 1С.
- Во второй половине 2017 года тактика атакующих изменилась: вектором распространения троянов стала не традиционная вредоносная рассылка и не взломанные популярные сайты, а создание новых тематических ресурсов, на которых злоумышленники размещали код, предназначенный для загрузки троянов.

- После нескольких лет интенсивного роста рынок хищений с помощью Android-троянов в России значительно сократился. Это связано и с обновлениями операционной сети от Google, и с понижением лимитов на переводы по СМС, и с внедрением банками систем раннего обнаружения фрода с функционалом детектирования активности вредоносных программ на устройстве клиента. Количество проводимых ежедневных хищений с помощью Android-троянов в России снизилось почти в три раза. Стоит отметить и сокращение среднего размера хищений. Если в прошлом отчетном периоде он составлял 11 тысяч рублей, то в этом он опустился до 7 тысяч.
- Новых крупных Android бот-сетей для атак в России не создавалось, за исключением вредоносной программы «Банки на ладони». Троян был замаскирован под финансовое приложение, выполняющее роль «агрегатора» систем мобильного банкинга ведущих банков страны.
- Веб-фишинг — единственный метод хищений, который показал рост ущерба в России в очетном периоде: с его помощью удалось похитить 251 млн рублей, что на 6% больше показателя прошлого года. Этот сравнительно простой способ атаки привлекает все больше новичков: количество групп, которые создают фишинговые сайты под российские бренды выросло с 15 до 26. Ежедневно им удается провести в среднем 1274 мошеннические транзакции. Средняя сумма одного хищения не изменилась и равна 1000 рублей.
- Большую популярность получил фишинг, связанный с переводом с карты на карту. В некоторых случаях атакующие брендируют такие страницы под конкретный банк, но есть и абсолютно независимый от брендов банков фишинг.

Атаки на клиентов банков. Мир

- На мировой арене банковских троянов ландшафт изменился значительно сильнее. Появилось шесть новых троянов для ПК: IcedID, BackSwap, DanaBot, MnuBot, Osiris и Xbot. При этом со сцены ушли Shifu, Qadars, Sphinx, Tinba и Emotet. Последний троян по-прежнему используется, но только в качестве загрузчика. Такое развитие событий может быть связано с работой правоохранительных органов, которые нанесли ощутимый удар арестами авторов банковских троянов Neverquest, GozNym, а также одного из самых популярных загрузчиков — Andromeda.
- В 2017 году были опубликованы исходные коды банковских троянов TinyNuke и AlphaLeon (также известен как Thantaos, Mercury Bot), однако пока их дальнейшего переиспользования не последовало.
- Наибольшую угрозу по-прежнему представляют группы, использующие трояны Dridex, Trickbot, Gozi. Из новых троянов наибольший интерес представляет BackSwap, который изначально атаковал только банки Польши, а затем включил в список целей и банки Испании. BackSwap примечателен тем, что реализовал сразу несколько новых техник внедрения кода для автоподмены платежных реквизитов.
- Новые Android-трояны, предлагаемые на хакерских форумах, ориентированы прежде всего на использование за пределами России. Среди них Easy, Exobot 2.0, Asacub, CryEye, Cannabis, fmif, AndyBot, Loki v2, Nero banker, Sagawa. Исключением из этого списка является только Asacub. Трояны, которые были активны в прошлом периоде (Xbot, Abrvall, Vasya, UfoBot, Reich), перестали использоваться, вероятнее всего из-за плохой поддержки авторами.
- Обычно банковские трояны под Android распространяются через SMS/MMS рассылки. Однако в начале 2018 года троян Exobot 2.0 распространялся через приложения, загруженные из официального магазина Google Play.
- В среднем каждый месяц на кард-шопы загружаются 686 тысяч текстовых данных карт и 1.1 млн дампов (содержимое магнитных полос карт). Основным методом получения дампов банковских карт является использование POS-троянов, которыми заражают компьютеры с подключенными POS-терминалами. Текстовая информация о банковских картах стоит на кардшопах значительно дешевле: суммарно текстовые данные продавали всего за $95.6 млн, что всего лишь 17% от общего рынка. Например, 19.9 млн дампов стоили уже $567.8 млн.
- В отличии от прошлого периода, на международном рынке первую позицию заняли фишеры, нацеленные на облачные хранилища, а не на финансовый сектор. 73% всех фишинговых ресурсов попадают в следующие три категории: облачные хранилища (28%), финансовые (26%), и онлайн-сер-

висы (19%). По объему фишинговых сайтов в мире США занимает 1 место (80%), 2 место — Франция, 3-е — Германия.

Угрозы для криптовалютного рынка

- В 2017 и 2018 годах возросло внимание хакеров к криптобиржам. В результате взломов криптобирж с февраля 2017 по сентябрь 2018 было похищено $877 млн. При этом 60% от общей суммы было украдено в результате атаки на японскую биржу Coincheck. Как минимум 5 из 13 успешных атак на криптобиржи связывают с северокорейскими хакерами из группы Lazarus, чьи жертвы преимущественно находятся в Южной Корее. Основным вектором проникновения в корпоративные сети криптобирж остается целевой фишинг.
- В повышенной группе риска также находятся ICO-проекты, которым хакеры наносят значительный ущерб: атакуют фаундеров, членов коммьюнити, сами платформы. Наиболее популярным инструментом атаки на ICO остается фишинг: на него приходится около 56% украденных средств. Крупная фишинговая группировка похищает около $1 миллиона в месяц.
- Относительно новым методом мошенничества на рынке ICO стала кража White Paper проекта и представление идентичной идеи под новым брендом.
- В 2018 была зафиксирована таргетированная атака с целью манипуляции курсом одной из криптовалют. Подготовка этой атаки заняла 2 месяца.
- Криптоджекинг (скрытый майнинг) — относительно новое направление мошенничества, получившее в отчетном периоде наибольшее развитие. После выхода в сентябре 2017 ПО для скрытого майнинга Coinhive появилось еще 7 программ подобного типа (Crypto-Loot, JSEcoin, Minr, CoinImp, ProjectPoi (PPoi), AFMiner, Papoto). Среди векторов компрометации взлом веб-сайтов, вредоносные расширения для браузеров, взлом третьей стороны, атака типа Man-in-the-Middle. В одном из последних случаев криптоджекинга атакующему удалось найти 0-day уязвимость в маршрутизаторе MikroTik. Используя ее, он смог заразить около 200 000 устройств, которые встраивали в отображаемые страницы скрипт для майнинга от Coinhive.
- В 2017 году не было ни одной успешной «атаки 51%», а в первой половине 2018 года криптоиндустрия столкнулась сразу с пятью успешными атаками такого типа. Сумма прямого финансового ущерба составила от $550 тысяч до $18 миллионов.

2. ПРОГНОЗЫ

Аппаратные уязвимости и безопасность BIOS/UEFI

- Эксплойты и вредоносные программы для эксплуатации аппаратных уязвимостей и заражения BIOS/UEFI по-прежнему останутся прерогативой прогосударственных атакующих.
- Количество заражений UEFI вырастет, в том числе благодаря развитию side-channel атак. В первую очередь таких атак стоит ждать в государственном секторе, где продолжительное время не обновляется парк ПК, и, как следствие, UEFI.
- Приоритетными целями атакующих могут стать производители материнских плат и поставщики оборудования в государственные органы.
- Реальная эксплуатация side-channel атак приведет к новым массовым утечкам из облачных сервисов, что может подорвать доверие к облачным инфраструктурам в случае резонансных инцидентов.

Саботаж и шпионаж

- Фишинг останется основным методом заражения критических инфраструктур, но с развитием отдельных групп этот метод будет замещаться другими, более сложными в обнаружении техниками. В этом году тренд может сместиться в сторону уязвимого сетевого оборудования, с помощью которого эта сеть подключена к Интернет.
- Энергетические объекты останутся главной мишенью группировок, нацеленных на саботаж, однако озаботиться оценкой компрометации своих систем и быть готовыми к атакам необходимо всем объектам критической инфраструктуры, связанным с жизнеобеспечением населения.
- Организациям, которым хотят защитить свои секреты, необходимо думать о безопасности не только своих корпоративных инфраструктур, но и домашних сетей и персональных устройств топ-менеджеров.
- Самораспространяемые трояны-шифровальщики будут использоваться для атак на физически изолированные (“air-gapped”) сети.
- Из-за растущего количества исследований по APT-группам ожидается, что многие из них начнут имитировать уникальные признаки других групп, что будет вводить исследователей в заблуждение и приводить к неправильной атрибуции.

Целенаправленные атаки на банки

- Еще одна группа — Silence — получила необходимый опыт для проведения целенаправленных атак на банки в России. Она успешно применит свои навыки для атак на банкоматы и карточный процессинг за пределами стран СНГ.
- Некоторые группы могут поменять вектор начального проникновения в банковские сети из-за более широкого применения песочниц для анализа почты, отказавшись от целевого фишинга в пользу эксплуатации уязвимостей в веб-приложениях банка, а также поиска уязвимого сетевого оборудования, как это было в случае с группой MoneyTaker.
- Аресты руководителей Cobalt и Fin7 могут привести к тому, что оставшиеся члены этих групп начнут формировать новые команды, что может привести к увеличению общего количества активных групп и обучению новых участников.
- Сегодня все финансово-мотивированные киберпреступные группы, которые занимаются целенаправленными атаками на банки, являются русскоговорящими. Мы ожидаем, что аналогичные группы будут сформированы из хакеров из Латинский Америки, а также стран Азии. Скорее всего, их первыми целями будут банки в их регионах.
- Lazarus продолжит атаковать банки и похищать деньги через SWIFT, однако стоит ожидать, что они опробуют себя и в атаках на системы карточного процессинга. Их основной фокус будет на странах Азиатско-Тихоокеанского региона.
- BlackEnergy и Lazarus кроме хищений будут проводить атаки и с целью саботажа, что может нанести гораздо больший урон, чем несанкционированные денежные переводы.

Атаки на клиентов банков

- Мы по-прежнему считаем, что более активное использование троянов с функцией самораспространения позволит атакующим поднять эффективность проведения атак с помощью банковских троянов для ПК, а также POS-троянов.
- Основным методом проникновения в сети ресторанов и магазинов с POS-терминалами может стать бесплатный Wi-Fi, раздаваемый уязвимыми роутерами.
- Мы ожидаем начала атак на мобильный банкинг для юридических лиц в России. Основным методом методом распространения может стать контекстная реклама в поисковых системах.
- Ущерб от фишинга в России продолжит расти. Для повышения эффективности таких атак могут использоваться домашние роутеры, перенаправляющие пользователей на такие сайты.
- Владельцы бот-сетей Toplel и RTM могут отказаться от хищений у юридических лиц и начать проводить целенаправленные атаки на банки в России и СНГ.
- После распространения исходных кодов основной угрозой для банкоматов без компрометации банковских сетей станет вредоносная программа «Котлета» (Cutlet).
- BackSwap и IcedID могут стать значимыми банковскими угрозами в дополнение к Dridex, Trickbot и Gozi.
- Банковские Android-трояны будут захватывать мировой рынок и продолжат вытеснять банковские трояны для ПК.

Угрозы для криптовалютного рынка и блокчейн-проектов

- Мы ожидаем, что такие группы, как Silence, MoneyTaker и Cobalt могут провести несколько успешных целевых взломов криптобирж.
- «Атаки 51%», а также атаки с целью манипуляции курсом валюты будут касаться только новых и не очень популярных валют.
- Атаки на ICO проекты по-прежнему будут актуальными для всех проектов, которые способны привлечь хорошие инвестиции.
- Бум криптоджекинга прошел, и в новом году мы ожидаем сокращение майнинговой активности как с помощью троянов, так и с помощью криптоджекинга.
- Крупнейшие майнинг пулы в мире могут стать целью не только киберпреступников, но и прогосударственных атакующих. При определенной подготовке это может позволить им взять под контроль 51% мощностей для майнинга и захватить управление криптовалютой.
- Для частных инвесторов, работающих с криптовалютами, основной угрозой останется фишинг и вредоносное ПО.

3. УЯЗВИМОСТИ МИКРОПРОЦЕССОРОВ И ПРОШИВОК

Если в прошлом периоде внимание специалистов по безопасности было приковано к эпидемиям вирусов-шифровальщиков WannaCry, NotPetya, BadRabbit, то в 2018 году самой значительной проблемой стали side-channel атаки и новые уязвимости, обнаруженные в микропроцессорах разных вендоров, которые невозможно полноценно закрыть программными обновлениями.

Другой критически значимой, но менее нашумевшей проблемой являются уязвимости в прошивках UEFI и BIOS, исследования которых становятся все более доступными широкому круг лиц.

Уязвимости микропроцессоров и прошивок открывают совершенно новые возможности для атакующих и через несколько лет могут сильно повлиять на рынок безопасности. Именно поэтому мы ставим информацию об этих трендах на первое место.

99,95%

коэффициент успешности атаки на многоядерные процессоры посредством эксплуатации уязвимостей SpectrePrime

АППАРАТНЫЕ УЯЗВИМОСТИ

Meltdown и Spectre

С середины 2017 года велось закрытое исследование аппаратных уязвимостей, которые затрагивают большинство микропроцессоров Intel, AMD и чипы, использующие процессорные ядра ARM. В январе 2018 года информация об этих уязвимостях была опубликована под названиями Meltdown (CVE-2017-5754) и Spectre (CVE-2017-5753 и CVE-2017-5715). Из-за опасности, которую представляют эти сведения, они вызвали огромный резонанс. Это, в свою очередь, привело к новым исследованиям, связанным со спекулятивными вычислениями, новыми уязвимостями и эксплойтами.

Meltdown позволяет злоумышленникам читать не только память ядра, но и всю физическую память целевых машин, а следовательно и все секретные данные программ и операционной системы. Самой большой опасностью уязвимости специалисты называют её практически полную независимость от операционной системы. Кроме того, Meltdown не оставляет никаких следов, что усложняет задачу поиска вредоносного кода, эксплуатирующего эту уязвимость.

Spectre нарушает изоляцию между различными приложениями, позволяя вредоносной программе заставить любой процесс выдать содержимое собственной памяти. Сразу же был предложен вариант атаки Spectre, использующий JavaScript для получения доступа к памяти браузеров, откуда можно достать данные других сайтов или, например, сохраненные пароли. Атаки Spectre могут использоваться для утечки информации из ядра в пользовательские программы, а также из гипервизоров виртуализации в гостевые системы.

Было опубликовано 4 варианта микроархитектурных багов, связанных со спекулятивными вычислениями:

Variant 1. Bounds Check Bypass
CVE-2017-5753

Variant 2. Branch Target Injection
CVE-2017-5715

Variant 3. Rogue Data Cache Load
CVE-2017-5754

- **Variant 3a.** Rogue System Register Read
  CVE-2018-3640
- **Variant 4.** Speculative Store Bypass
  CVE-2018-3639

MeltdownPrime и SpectrePrime

В феврале 2018 исследователи из NVIDIA и Принстонского университета опубликовали доклад, в котором описали новые типы атак, так же затрагивающие почти все современные центральные процессоры. Принцип атак, получивших название MeltdownPrime и SpectrePrime, схож с оригинальными, **новшество заключается в том, что они нацелены на многоядерные чипы и используют механизм аннулирования линий кеша** в современных протоколах когерентности кэш-памяти при передаче данных между ядрами. Как и в случае с Meltdown и Spectre, успешная атака позволяет получить доступ к закрытой для сторонних приложений информации вроде паролей. Код SpectrePrime, предлагаемый исследователями в качестве доказательства концепции, приводит к успеху атаки в 99,95% случаев исполнения на процессоре Intel (уровень успешности обычной атаки Spectre достигает 97,9%).

Аппаратная проблема заключается в блоке Translation Lookaside Buffers (TLB), который есть во всех современных процессорах. Блок TLB нужен для того, чтобы сократить время обращения к оперативной памяти за счет исключения процедуры трансляции адресов памяти.

TLBleed

В июле 2018 стало известно об еще одной уязвимости, затрагивающей Translation Lookaside Buffers (TLB), которая получила название TLBleed. Уязвимость означает, что процессы, которые используют общее физическое ядро, но разные логические ядра, могут получить доступ к данным друг друга. Было продемонстрировано, что **можно извлекать криптографические ключи и иные важные данные из других запущенных программ, причем коэффициент успешности атаки составляет минимум 98%.** Несмотря на то, что этой уязвимости не был присвоен CVE, разработчики OpenBSD решили отказаться от поддержки технологии Hyper-Threading в процессорах Intel. TLBleed не предполагает спекулятивного исполнения команд, то есть не имеет отношения к нашумевшим процессорным уязвимостям Meltdown и Spectre. В данном случае брешь связана со слабыми местами технологии Hyper-Threading и тем, как процессоры кэшируют данные.

Rowhammer

О Rowhammer заговорили в 2015 году, когда исследователи из Google опубликовали отчет об изучении этого эксплойта. Тогда они оценили Rowhammer как один из самых потенциально опасных сценариев атаки для компьютеров и ноутбуков. Атаки Rowhammer возможны из-за высокой плотности ячеек памяти в современных устройствах и заключаются в многократном повторении доступа к ряду ячеек с тем, чтобы вызвать переключение битов в соседних рядах. В результате **злоумышленник может получить права уровня ядра на компьютере или ноутбуке и root-доступ на мобильном устройстве.**

В марте 2016 исследователи из VUSec Lab при Амстердамском свободном университете (Vrije Universiteit Amsterdam) успешно реализовали атаку на Android через DRAM. Созданный ими **Drammer — первый root-эксплойт для Android, который не полагается на уязвимость в программном обеспечении, а реализует технику Flip Feng Shui**. Она была опробована на 27 различных Android-устройствах, использующих архитектуру ARM (32 бит и 64 бит), в том числе на Samsung Galaxy, LG Nexus, Motorola Moto G и HTC Desire. Как оказалось, для Drammer уязвимы 18 устройств из контрольной выборки.

В октябре 2017 группа ученых из Аделаиды, Пенсильвании, Мэриленда и Технического университета Граца опубликовала исследование, в котором описала **способ обойти защиту от атак Rowhammer, направленных на DRAM-память.** Ученые нашли способ запустить атаку, невзирая на все защитные меры. Для этого злоумышленникам достаточно всего лишь сосредоточить усилия на одном ряду ячеек, а не атаковать сразу несколько. Как показывают эксперименты, с таким подходом атака Rowhammer занимает от 44 до 138 часов.

В мае 2018 команда исследователей из Свободного университета Амстердама представила **новый способ эксплуатации уязвимости Rowhammer,** предусматривающий использование графического процессора и технологии WebGL для атак на память устройства. Метод получил название **GLitch.** Он представляет собой комбинацию атаки по сторонним каналам и классической атаки Rowhammer. В ходе экспериментов специалисты использовали атаку по сторонним каналам для определения структуры физической памяти, а затем с помощью Rowhammer им удалось переключить биты и внедрить вредоносные команды в оперативную память. Для атаки по сторонним каналам исследователи использовали браузеры и реализованную в них поддержку стандарта WebGL.

Исследователи успешно протестировали технику GLitch на Android-смартфоне с установленными браузерами Chrome и Firefox. **Им удалось скомпрометировать устройство всего за две минуты.** Для осуществления атаки требуется лишь загрузить вредоносный код JavaScript на целевое устройство. По словам экспертов, разработанный ими PoC-код был протестирован только на Google Nexus 5, но теоретически должен работать на всех устройствах на базе микропроцессоров Qualcomm Snapdragon 800 и 801.

УЯЗВИМОСТИ BIOS/UEFI

Об уязвимостях BIOS, а теперь и в UEFI известно уже давно. Но, поскольку реализация атаки сложна, а обнаружить факт заражения еще сложнее, специалисты, отвечающие за безопасность корпоративных сетей, не сильно заботятся этой проблемой. Однако ситуация быстро меняется, а **side-channel атаки для аппаратных уязвимостей могут стать новым драйвером ускорения процесс развития угроз для BIOS/UEFI. Возможность пережить переустановку ОС, замену жесткого диска делает исследование таких уязвимостей приоритетным для всех, кто занимается нападением.**

О том, что закладки для BIOS/UEFI используются в реальных атаках, удается узнавать только благодаря утечкам:

2014 Из утечки Эдварда Сноудена стало известно о том, что АНБ США использовало бэкдор **DEITYBOUNCE**, который устанавливали на сервера Dell PowerEdge через BIOS материнской платы и RAID-контроллеры.

Июль 2015 В утечке набора инструментов итальянской компании Hacking Team был обнаружен UEFI BIOS руткит, который проверял и устанавливал в ОС основной бэкдор.

Март 2017 На Wikileaks были опубликованы документы, посвященные ряду проектов ЦРУ, при помощи которых спецслужбы заражают технику Apple (Mac, iPhone) вредоносными программами, которые работают на уровне прошивки даже после переустановки ОС.

Август 2017 Из утечки Equation Group, связанной с АНБ США, стало известно о **BANANABALLOT**, который является имплантом для BIOS.

Информация из этих утечек стимулируют исследователей уделять больше внимания безопасности прошивок и выкладывать результаты своих исследований в открытый доступ.

Из графика ниже видно, что начиная с 2015 года исследовательская активность, посвященная поиску уязвимостей в BIOS/UEFI, значительно возросла. Вместе с тем, выросла и частота обнаружения их использования в целенаправленных атаках.

Август 2016 Дмитрий Олексюк написал и выложил исходный код **PEIBackdoor**. Этот бэкдор, применимый для UIFI совместимых прошивок, позволяет выполнять произвольный код, написанный на C, во время фазы Pre EFI Init (PEI).

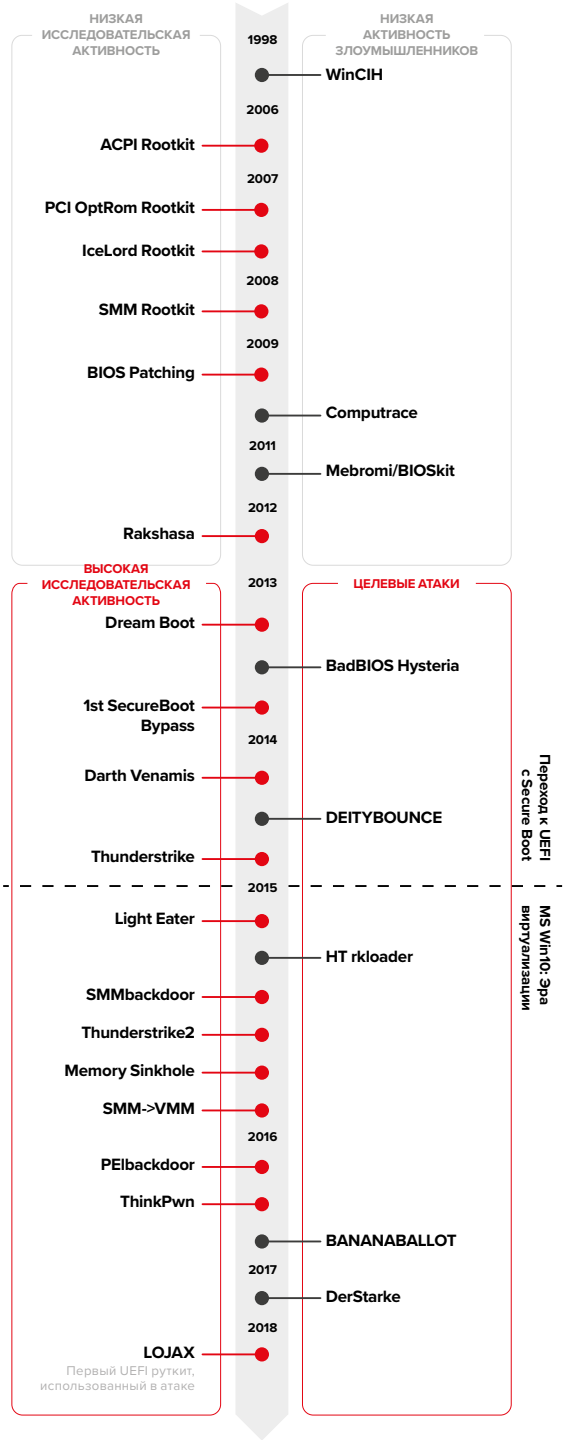
Октябрь 2016 Дмитрий Олексюк написал и выложил исходный код **SMMBackdoor** для UEFI-совместимых прошивок.

Июль 2017 На конференции BlackHat Александр Матросов рассказал о **6 новых обнаруженных им уязвимостях в прошивках производителей материнских плат**. Среди них повышение привилегий на ASUS Vivo Mini (CVE-2017-11315), системах Lenovo ThinkCentre (CVE-2017-3753) и MSI Cubi2 (CVE-2017-11312 и CVE-2017-11316), а также обход защиты Intel Boot Guard на платформе Gigabyte BRIX, вызванный парой уязвимостей, идентифицированных как CVE-2017-11313 и CVE-2017-11314.

Октябрь 2017 Александр Ермолов из Embedi обошел защиту Intel Boot Guard на материнской плате Gigabyte GA-H170-D3H. Ермолов связался с представителями AMI, чтобы уведомить их о проблеме, но ему сообщили, что уязвимости уже были устранены и последняя версия AMI BIOS, доступная для производителей, уже лишена таких недостатков. Когда исследователь решил проверить работу патча, оказалось, что исправление, по сути, лишь ухудшило и без того скверную ситуацию.

Май 2018 Были обнаружены вредоносные версии легитимного программного обеспечения **LoJack**, которое было модифицировано хакерами. Оригинальная программа Computrace LoJack предназначена для противодействия физическим кражам и позволяет удаленно отключить возможность перезагрузки украденного мобильного компьютера, превратив его в кирпич. Как и UEFI руткит, **LoJack переживает переустановку операционной системы и смену жесткого диска.** Как заявили исследователи, модифицированные версии LoJack содержали небольшие изменения в коде программы, заставлявшие ее связываться с C&C-сервером хакеров вместо легитимного центрального сервера LoJack. По адресу C&C-серверов исследователи связали эти атаки с APT28 (также известна как Fancy Bear, Sofacy, Pawn storm, Sednit и Strontium), но не смогли выяснить, как вредоносная версия LoJack была установлена на компьютеры.

Исследование уязвимостей в BIOS/UEFI и целевые атаки



В упомянутых выше утечках говорится, что для установки UEFI бэкдоров может требоваться физический доступ. Но есть и сценарии для удаленной установки. Для этого атака разбивается на 4 этапа:

- **Этап 1.** В результате эксплуатации уязвимости в приложении ОС на систему загружается установщик, который повысит привилегии до уровня system.
- **Этап 2.** Обходится политика проверки подписи приложения ядра, вредоносная программа загружается в ядро ОС.
- **Этап 3.** Выполняется SMM эксплойт, повышаются привилегии для SMM и запускается вредоносная нагрузка.
- **Этап 4.** Обходится защита от записи в флеш-память, после чего руткит устанавливается в прошивку.

Последние два этапа делают проведение такой атаки особенно сложным, но недавно обнаруженные уязвимости и эксплойты позволяют упростить задачу:

Угроза	**Описание** (источник: GitHub)
SMI Handlers	Повреждение памяти может привести к произвольному выполнению кода SMM.
S3BootScript (VU #976132)	Произвольная модификация прошивки. Позволяет злоумышленнику произвольно читать и записывать в область SMRAM.
ThinkPwn (LEN-8324)	Эксплойт для выполнения произвольного SMM кода для нескольких поставщиков BIOS. Позволяет атакующему отключить защиту от флэш-записи и модифицировать прошивку.
Aptiocalypsis (INTEL-SA-00057)	Эксплойт для выполнения произвольного SMM кода для прошивки AMI Aptio. Позволяет атакующему отключить защиту от флэш-записи и модифицировать прошивку.

Несмотря на то, что указанные уязвимости были обнаружены в 2015-2016 годах, они по-прежнему актуальны. Обновление UEFI в корпоративных сетях, как правило, отсутствует, более того, некоторые вендоры не выпускают обновлений. Ухудшает картину и то, как реализуются производителями материнских плат меры безопасности по умолчанию на разных BIOS/UEFI.

Например, некоторые вендоры не включают по умолчанию:

- SMM_BWP — SMM BIOS Write Protect
- PRx — SPI Write Protection
- BLE — BIOS Lock Bit

Vendor Name	**BLE**	**SMM_BWP**	**PRx**	**Authenticated Update**
ASUS	+	+	-	-
MSI	-	-	-	-
Gigabyte	+	+	-	-
Dell	+	+	-+	+
Lenovo	+	+	RP	+
HP	+	+	RP/WP	+
Intel	+	+	-	+
Apple	-	-	WP	+

4. САБОТАЖ И ШПИОНАЖ

Как мы и предполагали в отчете за прошлый год, ландшафт угроз для критических инфраструктур продолжает усложняться за счет активности хакерских групп, связанных с государством. **Центр инноваций в целевых атаках сместился в сторону проправительственных группировок.** Если раньше прогосударственные хакеры следили за целевыми атаками, разработками и тактиками финансово-мотивированных киберпреступников, то теперь киберпреступники внимательно следят за более продвинутыми прогосударственными атакующими.

Ландшафт APT-угроз уникален для каждого региона мира и постоянно меняется. Знакомые группы пропадают с радаров, меняют тактики атак и спектр целей, проявляются ранее неизвестные группировки. Как правило, на момент обнаружения новые игроки были активны уже несколько лет, но по разным причинам оставались незамеченными. **Поэтому отсутствие данных об атаках в отдельной стране или секторе экономики с большей степенью вероятности говорит о том, что о них пока не известно, нежели о том, что их не было.**

Ниже мы приводим данные о наиболее активных APT-группах и их предположительной атрибуции, а также отмечаем тренды в тактиках атакующих.

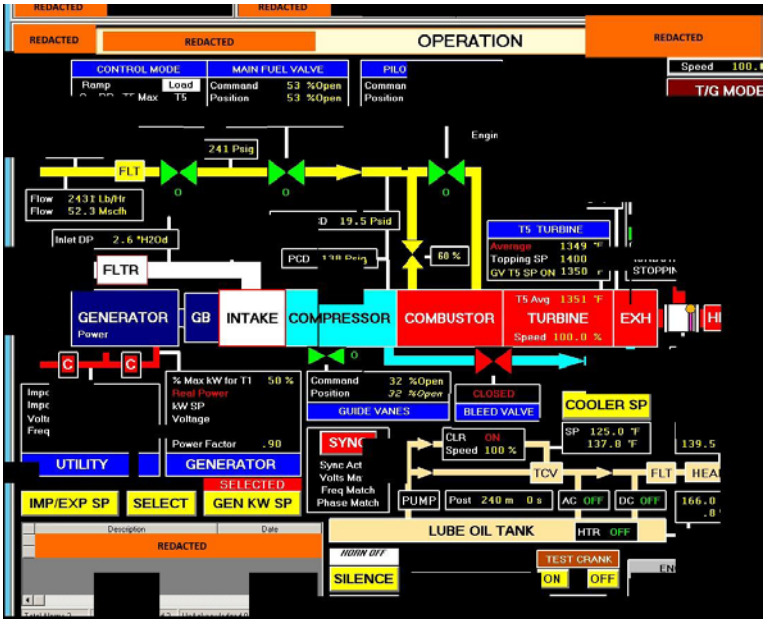
США и Латинская Америка	Европа	Юго-Восточная Азия	Ближний Восток и Африка	Россия
APT28 — Russia	Lazarus — North Korea	DarkHotel — North Korea	OilRig — Iran	Equation — USA
Turla — Russia	APT28 — Russia	Lazarus — North Korea	APT37 — North Korea	APT10 — China
Lazarus — North Korea	APT15 — China	Thrip — China	Slingshot — USA	APT17 — China
APT15 — China	Tick — China	APT32 — Vietnam	Newscaster Team — Iran	PlugX — China
Thrip — China	BlackEnergy — Russia	Andariel — North Korea	APT34 — Iran	Prikormka — Ukraine
Charming Kitten — Iran	Dragonfly — Russia	Mustang Panda — China	APT33 — Iran	APT28 — Russia
Mustang Panda — China	TEMP.Periscope — China	APT37 — North Korea		BlackEnergy — Russia
Dragonfly — Russia	Gorgon Group — Pakistan	Slingshot — USA		PowerPool
Gorgon Group — Pakistan	Orangeworm	Kimsuky — North Korea		
TEMP.Periscope — China	PowerPool	Tick — China		
Newscaster Team — Iran		BlackEnergy — Russia		
Orangeworm		Charming Kitten — Iran		
		APT28 — Russia		
		MuddyWater — Iran		
		Sidewinder — India		
		Chafer — Iran		
		TEMP.Periscope — China		
		APT17 — China		
		Orangeworm		
		Rancor		

На основании атрибуции, сделанной в результате исследований Threat Intelligence компаниями в области кибербезопасности и правоохранительными органами.

ЦЕЛЕВЫЕ АТАКИ НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Одной из наиболее продвинутых угроз для объектов критической инфраструктуры остается **Industroyer** или **CRASHOVERRIDE**, с помощью которого в декабре 2016 были выведены из строя объекты энергетической сети Украины. В 2017 году этот инструмент был подробно описан компанией ESET, а его создание связали с группой Black Energy. **Основной особенностью Industroyer является возможность удаленного управления remote terminal units (RTU), которые отвечают физическое размыкание/замыкание сети.** Такие элементы используются не только в энергетических, и водоснабжающих, газовых и других промышленных системах.

В конце 2017 и начале 2018 в результате совместного исследования Министерства внутренней безопасности США и ФБР были выпущены оповещения с индикаторами об атаках со стороны России, с которой связывают группу BlackEnergy, на компании энергетического, ядерного, коммерческого, водного, авиационного и критически важных производственных секторов. Оповещения подтверждали, что атакующие успешно получили доступ к системе управления SCADA, и демонстрировали один из скриншотов, сделанных атакующими.



В то же время в результате инцидента на одном из предприятий критической инфраструктуры стало известно еще об одном инструменте — **TRITON** — фреймворке, которые позволяет взаимодействовать с Triconex Safety Instrumented System (SIS, система безопасности производственных процессов) от компании Schneider Electric.

Атакующий получил удаленный доступ к рабочей станции оператора SIS и развернул TRITON для перепрограммирования контроллеров SIS. Во время инцидента некоторые контроллеры SIS вошли в безопасный режим, который автоматически отключает промышленный процесс, что и побудило пострадавшую компанию начать расследование. Анализ показал, что контроллеры SIS инициировали безопасное завершение работы, когда код приложения между резервными процессорами не прошел проверку, что привело к сообщению об ошибке диагностики.

TRITON позволяет управлять контроллерами SIS Triconex: останавливать их, считывать содержимое памяти, перепрограммировать и добавлять вредоносный функционал. При этом вредоносный код на контроллере работает вместе с легитимным, чтобы контроллер мог продолжить работу. Если из-за перепрограммирования контроллера происходит сбой, TRITON попытается вернуть его в рабочее состояние. Если контроллер не восстановился в течение определенного временного окна, вредоносный код заменит себя недействительными данными, чтобы скрыть свои следы.

Обладая такими возможностями, атакующий может остановить работу предприятия одним из следующих образов:

- Перепрограммировать контроллер безопасности производственных процессов так, чтобы он считал, что один из процессов перешел в критическое состояние, что приведет к его остановке.
- Перепрограммировать контроллер, чтобы он игнорировал реально критические состояния процессов, и ждать, когда критическое состояние наступит само.
- Перепрограммировать контроллер, чтобы он игнорировал реально критические состояния процессов, и спровоцировать наступление таких состояний, манипулируя другими производственными системами.

КЕЙС: OLYMPIC DESTROYER

Саботаж Зимних Олимпийских игр 2018 в Южной Корее

В феврале 2018 года в результате атаки с помощью вредоносной программы Olympic Destroyer были выведены из строя официальный сайт Олимпиады в Пхенчхане, Wi-Fi на стадионе и вызван сбой в прямой трансляции во время церемонии открытия. Ряд исследователей связало атаку с группой Sofacy, также известной как Fancy Bear и APT28.

Программа совершала следующие шаги для вывода системы из строя:

1. После запуска извлекала из себя два модуля для сбора логинов и паролей.
2. Первый модуль собирал сохраненные в веб-браузере логины и пароли.
3. Второй модуль получал логины и пароли из процесса LSASS таким же образом, как это делает известная утилита Mimikatz.
4. Используя извлеченные логины и пароли, а также эксплойт EternalRomance из утечки The Shadow Brokers, программа начинала самораспространяться по сети.
5. На зараженных компьютерах программа приступала к выводу их из строя следующим образом:
    a. Удаляла теневые копии, вызывая стандартную утилиту vssadmin.exe.
    b. Удаляла резервные копии, вызывая стандартную утилиту wbadmin.exe.
    c. Отключала восстановление системы, вызывая стандартную утилиту bcdedit.exe.
    d. Удаляла системные журналы с помощью стандартной утилиты wevtutil.exe.
    e. Отключает все службы на системе.
    f. Перечисляла подключенные сетевые папки и затирала файлы нулями.

МАССОВЫЕ АТАКИ С НЕЧЕТКОЙ ЦЕЛЬЮ ОТ BLACK ENERGY

BadRabbit

После атак WannaCry и NotPetya 24 октября 2017 года новый массовый удар нанесла угроза с именем BadRabbit. Group-IB первой подтвердила связь между BadRabbit и эпидемией вируса NotPetya, атаковавшего в июне 2017 года энергетические, телекоммуникационные и финансовые компании на Украине. Мы обнаружили, что **код BadRabbit был скомпилирован из исходников NotPetya,** схожи уникальные функции вычисления хэша, способ распространения по сети и удаление журналов. Логика извлечения модулей и сами модули также подтверждают эту связь.

Распространение BadRabbit было массовым, хотя жертв оказалось гораздо меньше, чем в случае с NotPetya. На Украине в результате атаки BadRabbit пострадали несколько стратегических объектов (аэропорт, метро, госучреждения), в России — редакции федеральных СМИ. Также были зафиксированы попытки заражения банковских инфраструктур, правда, неудачные.

В отличие от NotPetya, BadRabbit распространялся методом drive-by download, а не watering hole attack. Для распространения использовались несколько популярных информационных интернет-ресурсов на Украине и в России. Исследование подтвердило, что доступ к сайтам был получен в результате целенаправленной атаки: как минимум в одном из случаев был взломан компьютер разработчика сайта, а через него был скомпрометирован сайт.

Группа внесла изменения в свой инструмент и попыталась замаскироваться под обычную криминальную группировку. Если NotPetya содержал один кошелек для перевода выкупа, что позволяло предположить, что авторы и не собирались расшифровывать файлы, а их основная задача заключалась в саботаже, то BadRabbit предусматривал автоматическую генерацию уникального ключа для каждого компьютера и создание индивидуального кошелька под каждый ключ. Также в атаке BadRabbit было задействовано доменное имя, которое ранее использовалось в атаках обычной киберпреступностью для фишинга и сбора трафика.

Но эта массовая атака была лишь отвлекающим маневром. **Объекты, которые на самом деле собирались выводить из строя были скомпрометированы заранее.**

VPNFilter

Еще одну угрозу удалось обнаружить до начала массовой атаки: в мае 2018 стало известно, что вредоносной программой VPNFilter было заражено около 500 тысяч роутеров Linksys, MikroTik, NETGEAR и TP-link, а также NAS производства QNAP в 54 странах мира.

В отличии от подавляющего большинства вредоносных программ для роутеров, **VPNFilter способен пережить перезагрузку.** Процесс заражение состоит из трех этапов, задействующих индивидуальные модуль. Первый модуль прост и отвечает за закрепление на устройстве даже в случае его перезагрузки. Второй модуль выводит устройство из строя. Третий модуль обеспечивает загрузку дополнительных плагинов, которые могут **перехватывать трафик жертвы, а также обнаруживать SCADA-системы.**

Даже после того, как ФБР сообщило о том, что они «перехватили» контроль над сервером управления, **сканирование и поиск новых уязвимых роутеров не остановились.**

АТАКИ НА БАНКИ С ЦЕЛЬЮ САБОТАЖА

Банки часто не осознают себя частью критической инфраструктуры, однако нарушение их работы может привести к дестабилизации финансовых рынков и социально-экономической ситуации. Поэтому **наличие инструментов и опыта вывода банковских систем из строя является одним из приоритетов у атакующих, заинтересованных в саботаже**. Такие инструменты активно используют группы BlackEnergy и Lazarus.

ONI Ransomware

С марта по август 2017 атакам подвергся целый ряд банков и других организаций в Японии, в чьих сетях оказался вирус ONI Ransomware. Заражение шифровальщиком — результат длительной и сложной атаки, которая происходила по следующей схеме:

1. Рассылка вредоносных электронных писем с вложением 領収証.doc (Квитанция.doc), содержащим VBA-макрос.
2. В результате открытия файла устанавливалась модифицированная версия средства удаленного управления Ammyy Admin, разработанного российским разработчиком.
3. Далее проходила разведка на зараженном устройстве, исследование сети, хищение аутентификационных данных (логины, пароли).
4. Компрометация других устройств в этой сети, в том числе контроллера доменов (DC) с целью получения полного контроля над сетью. При этом злоумышленники также использовали эксплойт EternalBlue. Стоит отметить, что для заражения по сети не использовался механизм самораспространения.
5. Очистка логов, распространение криптолокера ONI по сети с использованием групповых политик.

Специалисты Group-IB предполагают, что **за данной атакой стоит хакерская группа BlackEnergy.** На это указывают несколько признаков:

- В конце 2016 года и январе-феврале 2017 года были зафиксированы целевые атаки на финансовые организации в Украине. Злоумышленники распространяли бэкдор TELEBOT, управление которым осуществлялось через Telegram Bot API. В финальной стадии этой атаки используется деструктивный компонент KillDisk. Программа удаляет важные системные файлы, после чего компьютер перестает загружаться, а также переписывает файлы некоторых типов. Таким образом, злоумышленники удаляли следы своего присутствия, как и в атаках в Японии.
- Атаки на банки Японии начались в марте 2017, то есть сразу после атак в Украине.
- В атаках в Японии, как и в Украине, злоумышленники не использовали механизм самораспространения.
- Как и в атаках в Украине, а затем и в атаках NotPetya и BadRabbit, в Японии использовался шифровальщик, модифицирующий MBR.
- В атаках на японские организации в шифровальщике ONI использовался исходный код DiskCryptor, позднее также использованный в NotPetya и BadRabbit.
- Использованная в атаках программа Ammyy Admin разработана российской компанией.
- Наличие комментариев на русском языке в коде шифровальщика.

Атаки Lazarus

Северокорейская проправительственная группировка Lazarus неоднократно отмечалась атаками с целью саботажа в Южной Корее. В 2018 году, используя доступ в локальные сети банков Banco de Chile и Bancomext, хакеры смогли вывести деньги через систему межбанковских переводов SWIFT. На финальном этапе атаки они использовали новую версию программы для перезаписи master boot record (MBR) для вывода сети банка из строя. В СМИ просочилась информация о том, что атака в Banco de Chile затронула около 9000 компьютеров и более 500 серверов.

АТАКИ НА РОУТЕРЫ И ДРУГИЕ УСТРОЙСТВА

В дополнение к упомянутому выше VPNFilter, в 2018 году была обнаружена еще одна угроза для роутеров. Точно не установлено, каким образом **Slingshot**, остававшийся незамеченным на протяжении шести лет, заразил свои первые цели, однако известно, что создатели вируса внедрили вредоносный код в роутеры латвийской компании MikroTik.

Группа **Orangeworm** также была обнаружена только в 2018 году, хоть сами атаки, направленные на организации здравоохранения США, Европы, Азии, длились с 2015 года. При реализации атаки злоумышленники заражают машины, на которых установлено программное обеспечение для использования и управления высокотехнологичными устройствами обработки изображений (рентгеновский аппарат, МРТ-аппарат), а также те, которые применяются для оказания помощи пациентам в заполнении форм согласия на процедуры.

ТРЕНДЫ В ТАКТИКАХ АТАК С ЦЕЛЬЮ ШПИОНАЖА И САБОТАЖА

Предотвращение обнаружения и контрфорензика

Важной тактикой усложнения детектирования атаки является сокрытие взаимодействия зараженных устройств с сервером управления. Традиционно для этих целей используется шифрование, но **некоторые группы используют интересные техники, чтобы усложнить обнаружение:**

- Летом 2018 года была раскрыта активность группы Turla с использованием программы для шпионажа **Turla Outlook backdoor**, использующей в качестве канала для связи с C&C PDF-вложения к письмам, передаваемым через Microsoft Outlook или почтовый клиент The Bat!. Бэкдор восстанавливает контейнер – BLOB-объект со специальным форматом, который содержит зашифрованные команды для исполнения бэкдором, – из PDF-документов. Команды находятся в последней части структуры контейнера, зашифрованы с помощью MISTY1 и сжаты с помощью bzip2. Эта техника позволяет избегать детектирования вредоносной активности. Интересовавшие преступников данные также шифровались с использованием MISTY1 в обычный PDF-файл. Перед зашифрованным BLOBом документ содержал белое изображение 1x1 пиксель в jpeg, жестко закодированное во вредоносной программе. Такой метод позволял создавать PDF, который при открытии отображал пустую страницу. Затем бэкдор прикреплял PDF к письму и отправлял его на адрес атакующих одновременно с легитимными письмами, что снижало шансы на детектирование «утечки».
- Хакеры из группы Turla также использовали комментарии в Instagram Бритни Спирс, чтобы получить актуальный адрес сервера управления. Для этого вредоносная программа читала комментарии, вычисляла хэши и, обнаружив комментарий с хэш-суммой, равной 183, извлекала адрес сервера в виде короткой ссылки.
- Группа APT15 использует трояны **RoyalCli** и **BS2005**, которые взаимодействуют с C&C через Internet Explorer с помощью COM-интерфейса IWebBrowser2. Из-за характера метода IE-инжектирования это приводит к тому, что ряд команд для C&C кэшируются на диск с помощью IE-процесса.
- Троян **Rokrat**, используемый с группой APT37, взаимодействует с сервером управления и получает команды от своих операторов через Twitter.
- С октября 2017 киберпреступники из Rancor добавили в арсенал собственную разработку **PLAINTEE**, отличительной чертой которой является использование специализированной вариации протокола UDP для связи с удаленными серверами злоумышленников.

Использование общедоступных инструментов

Многие APT-группы не привносят ничего нового, а используют уже известные техники и уязвимости. Большая часть из них продолжает использовать ранее созданные ими инструменты и прежний код в новых инструментах, что облегчает корреляцию с прошлыми атаками. Но есть и исключения, когда **APT-группы начинают использовать инструменты общего назначения, что усложняет атрибуцию.**

- Группа APT28 начала использовать троян **Koadic** — это RAT с открытым исходным кодом, который позиционируется как инструмент для тестирования на проникновение.
- Группы Turla, Lazarus, OilRig, Charming Kitten, Newscaster Team, APT32, MuddyWater начали более активно применять **Metasploit**, популярный фреймворк для проведения тестов на проникновение. Группы APT10, APT17, APT-32 и TEMP. Periscope начали использовать другой популярный фреймворк — **Cobalt Strike**.
- Группа OilRig начала использовать **Invoke-Obfuscation** — инструмент с открытым исходным кодом, доступный через репозиторий Github.
- Для атак на правительственные организации группа Gorgon Group использует фишинговые письма с документами Microsoft Word, эксплуатирующими уязвимость CVE-2017-0199. В ходе атак на компьютеры жертвы загружался один из широко распространенных троянов **NanoCoreRAT, QuasarRAT и NJRAT**.

Разработка и покупка 0-day уязвимостей

Эффективный шпионаж невозможен без использования 0-day уязвимостей, поэтому **APT-группы тратят много ресурсов на их разработку и покупку.**

- В начале июня 2018 года специалисты обнаружили новую волну атак с использованием уязвимости нулевого дня **CVE-2018-5002**. Брешь в Adobe Flash Player 29.0.0.171, связанная с переполнением буфера в стеке, позволяет атакующим выполнить на машине жертвы произвольный код. Было обнаружено, что эту уязвимость активно использовали для таргетированных атак на Ближнем Востоке, главной целью которых был Катар. На настоящий момент не установлено, какая именно APT-группа стоит за ними.
- Недавно обнаруженная группа PowerPool начала использовать во вредоносной кампании уязвимость **CVE-2018-8440**, затрагивающую версии Microsoft Windows с 7 по 10, а именно интерфейс Advanced Local Procedure Call (ALPC) в Планировщике заданий Windows. Уязвимость обеспечивает локальное повышение привилегий (Local Privilege Escalation), что позволяет атакующему повысить права до уровня system. Хакеры взяли исходник Proof-of-Concept кода эксплойта с репозитория GitHub и частично модифицировали его.

В частности, с уязвимостями нулевого дня активно работают группировки, ассоциируемые с Северной Кореей.

- DarkHotel использовали уязвимость нулевого дня **CVE-2018-8174** и **CVE-2018-8373**:
  - CVE-2018-8174 — уязвимость use-after-free (UAF), которая затрагивает реализацию VBScript в Internet Explorer и Microsoft Office. Изначально эта 0-day уязвимость получила название «double kill». Она использует технику, суть которой в «повреждении» двух объектов памяти и изменении типа одного объекта на Array для возможности чтения и записи адресного пространства, а другого объекта — на Integer для получения адреса произвольного объекта.
  - CVE-2018-8373 также затрагивает движок VBScript в последних версиях Windows. Злоумышленники эксплуатировали уязвимость типа UAF, находящуюся в библиотеке vbscript.dll, которая оставалась непропатченной в последнем движке VBScript.
- В 2018 исследователи обнаружили новую кампанию по кибершпионажу от Andariel с использованием как минимум девяти брешей в платформе ActiveX, в числе которых уязвимость нулевого дня. Исследователи высказали предположение, что последняя связана с одним из десктопных приложений от Samsung — Samsung SDS Acube, которое пользуется большой популярностью среди южнокорейских компаний.
- Атакующие из APT37 начали использовать уязвимость нулевого дня в Adobe Flash Player **CVE-2018-4878** начиная с середины ноября 2017 года. О самой уязвимости CERT Южной Кореи сообщил только в конце января 2018 года, а закрыли уязвимость лишь в феврале. Уязвимость, позволяющая злоумышленнику удаленно выполнить произвольный код, затронула текущую версию продукта 28.0.0.137 и более ранние версии.

APT-группы тратят много ресурсов на разработку и покупку сведений об узявимостях нулевого дня.

5. ХИЩЕНИЯ

ОЦЕНКА РЫНКА ВЫСОКОТЕХНОЛОГИЧНЫХ ХИЩЕНИЙ В РОССИИ

Финансовая оценка активности киберпреступников является ярким индикатором смены приоритетов хакеров. Большая часть атакующих следуют за деньгами и, если они находят новые более эффективные способы заработка, они инвестируют время и средства именно туда, создавая новые инструменты, услуги, схемы проведения атак.

За прошедший период полностью ушли со сцены трояны для ПК, а хищения с помощью Android-троянов после нескольких лет взрывного роста резко сократились благодаря обновлениями операционной сети от Google, понижению лимитов на переводы по SMS, и с внедрением банками систем раннего обнаружения фрода с функционалом детектирования активности вредоносных программ на устройстве клиента.
На подъеме фишинг – относительно простая тактика атак привлекает на рынок все больше злоумышленников. Основной угрозой для российских банков остаются хорошо подготовленные группы с практикой успешных целевых атак. В среднем в России каждый месяц они грабили 1-2 банка. Впрочем, в 2018 году было 4 месяца, когда мы не зафиксировали ни одного ограбления (январь, февраль, май и июнь).

Далее мы подробно остановимся на группах, стоящих за этими атаками.

Сегмент рынка в России	Кол-во групп	Успешных атак в день	Средняя сумма одного хищения (в RUR)	Средняя сумма хищений в день (в RUR)	H2 2017 - H1 2018 (в RUR)	H2 2017 - H1 2018 (в USD)	Процент изменения
Хищения у юридических лиц с троянами для ПК	**3**	**2**	**1 100 000**	**2 200 000**	**547 800 000**	**$9 130 000**	**-12%**
Хищения у физических лиц с Android-троянами	**8**	**110**	**7 000**	**770 000**	**191 730 000**	**$3 195 500**	**-77%**
Целевые атаки на банки	**3**	**-**	**118 000 000**	**-**	**1 303 900 000**	**$21 731 667**	**-20%**
Фишинг	**26**	**108**	**1 000**	**1 008 000**	**250 992 000**	**$4 183 200**	**6%**
Обналичивание похищаемых средств				**1 336 500**	**919 543 500**	**$15 325 725**	**-34%**
Итого				**5 314 500**	**3 213 965 500**	**$53 556 092**	**-32%**

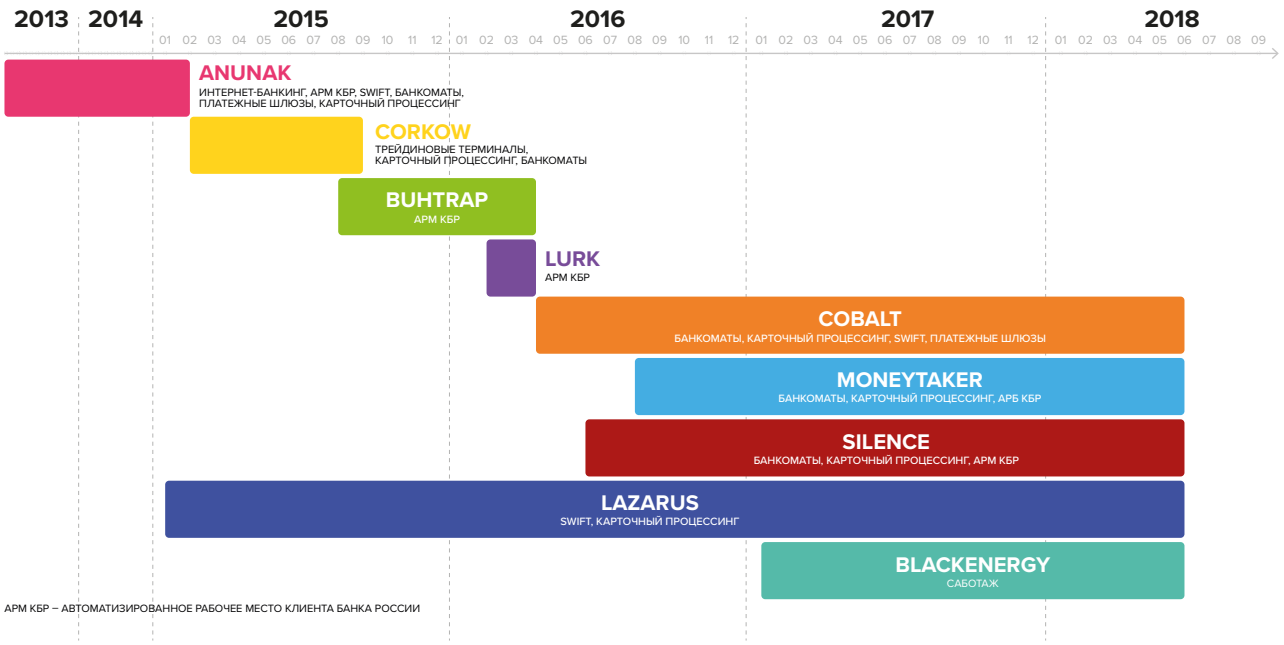
H2 2017 – H1 2018, данные Group-IB (обновлено 1 ноября 2018 года)

ЦЕЛЕВЫЕ АТАКИ НА БАНКИ

На графике ниже показаны группы, которые проводят целенаправленные атаки на банки с целью хищений. **На текущий момент существует всего четыре группы, которые способны взломать банк, добраться до изолированных финансовых систем и вывести деньги.**

Каждая из этих групп имеет более глубокую историю, на графе отмечены моменты начала и завершения попыток ограбить именно банки. Группы, которые занимаются саботажем и шпионаже, на иллюстрации не представлены.

Cobalt, MoneyTaker, Silence состоят из русскоговорящих финансово-мотивированных хакеров, Lazarus принято считать спонсируемой Северной Кореей. **Именно эти группы являются центром инноваций и формируют тренды в сложных атаках на банки.** По каждой из этих киберпреступных групп Group-IB первой выпускала отчеты.



SWIFT И ЛОКАЛЬНЫЕ МЕЖБАНКОВСКИЕ СИСТЕМЫ

Количество целенаправленных атак на банки с целью хищения через SWIFT увеличилось в три раза. Если за прошлый период было всего три атаки (Гонконг, Украина, Турция), то в этом году прошло успешных атак было уже девять: в Непале, Тайване, России, Мексике, Индии, Болгарии и Чили.

По этим инцидентам можно сделать вывод, **что для межбанковской системы SWIFT представляют угрозу только две преступные группы: Cobalt и Lazarus.** Первая известная успешная атака Lazarus на SWIFT была проведена в феврале 2016 года в центральном банке Бангладеш. Буквально через два месяца группа Cobalt совершила сразу две успешных атаки на SWIFT в банках Гонконга и Украины.

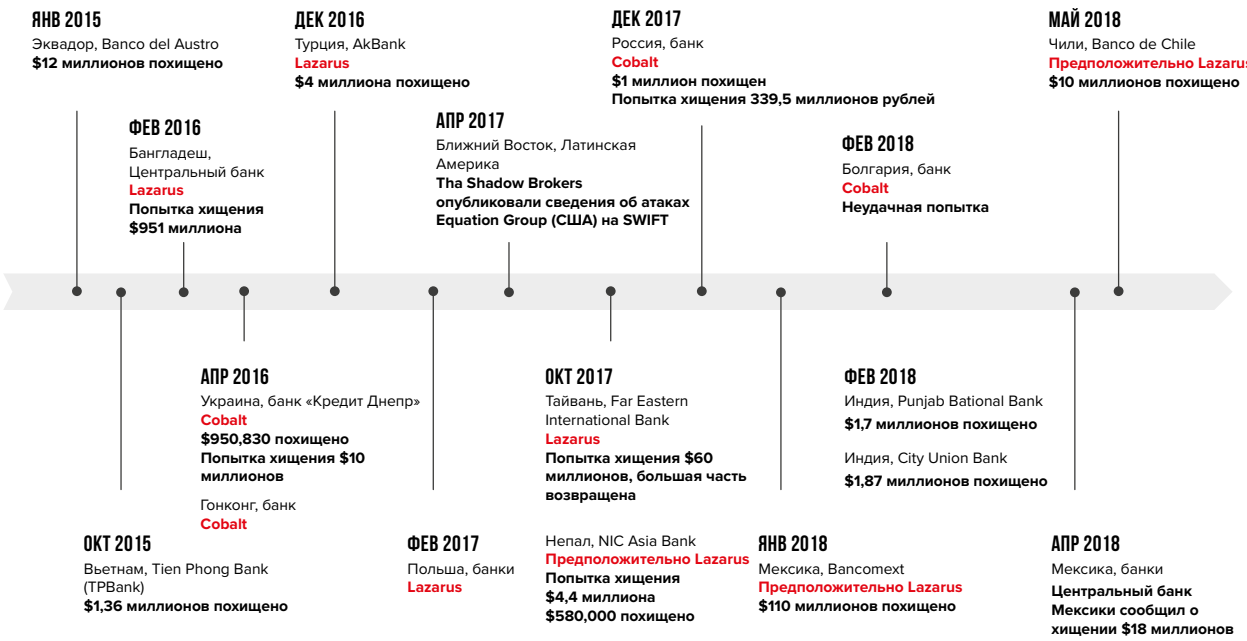
В некоторые месяцы и Cobalt, и Lazarus совершают хищения сразу в двух банках. Возможно, это связано с общей подготовкой схем обнала. Однако в случае со SWIFT большую часть похищенных средств удается остановить и вернуть пострадавшим банкам.

Посмотрев на атакованные банки и связанные с ними группы, можно заметить, что **Lazarus сосредоточила усилия на Азиатско-Тихоокеанском регионе, а Cobalt — на странах Восточной Европы**.

Атаки на SWIFT в России и Болгарии проводились без специальных инструментов, использовался только стандартный набор Cobalt. Получив в доступ в сеть банка и логины легитимных пользователей, они просто сделали несколько транзакций, большая часть из которых была успешно заблокирована.

Несмотря на то, что Lazarus в этом году достаточно активно пытался похищать деньги через SWIFT, гораздо больших успехов в экономическом смысле они добились, атакуя криптовалютные биржи, о чем мы пишем в соответствующем разделе отчета. Фактов, подтверждающих что эта группа интересуется локальными системами межбанковских переводов не обнаружено.

В одном из инцидентов было установлено, что Cobalt интересуется не только SWIFT, но и локальными системами межбанковских переводов в разных странах. Так, попав в сеть одного из банков, они попробовали вывести деньги и через локальный межбанкинг более 20 миллионов евро, но попытка была неуспешной.



Атаки на АРМ КБР

В 2016 году основную угрозу для банков в России представляли атаки на АРМ КБР (Автоматизированное рабочее место клиента Банка России). Однако в 2017 и 2018 году хакеры из групп Cobalt и Silence игнорируют данные системы даже в том случае, когда успешно получают к ним доступ. Сейчас их внимание привлекают более надежные схемы хищений через банкоматы и карточный процессинг. И только группа MoneyTaker сделала одно успешное хищений в ноябре 2017 года через АРМ КБР. Тогда сумма ущерба составила всего 7 миллионов рублей, а в 2018 они успешно вывели из другого банка уже 58 миллионов рублей.

В начале июля 2018 пользователь под псевдонимом **Bobby.Axelrod опубликовал на андеграундных форумах фреймворк Pegasus для автоматизации атак на АРМ КБР** путем автоматической подмены платежных реквизитов. В архив также входили инструкции и исходные коды. Этот фреймворк использовался группой Buhtrap в 2016 году и все данные из архива относятся к тому периоду. Ранее часть исходных кодов, используемых Buhtrap, уже утекали в сеть. Стоит отметить, что реализованная в данном фреймворке автозамена платежных реквизитов уже не актуальна для последних версий АРМ КБР, однако архив представляет большую ценность для автоматизации других шагов по компрометации банковских сетей.

КАРТОЧНЫЙ ПРОЦЕССИНГ

Атаки на карточный процессинг по-прежнему являются одним из основных способов хищений и проводятся группами Cobalt, MoneyTaker, Silence. Этот метод х обеспечивает самый безопасный способ обналичивания и максимальную финансовую выгоду. Рекордсменом в этой области стала группа Cobalt: в 2017 году в европейском банке они попытались похитить 25 миллионов евро. В других регионах суммы ущерба как правило значительно ниже.

Эта схема хищений начала набирать популярность в 2016 году. В сентябре 2016 года группа Cobalt получила доступ в один из банков Казахстана и начала подготовку к новому для них типу хищений — через карточный процессинг. Процесс изучения занял 2 месяца, и в ноябре они успешно похитили около $600 тыс. **С тех пор Cobalt — лидер по количеству успешных атак этого типа.**

Параллельно вместе с ними схему атак на карточный процессинг начала прорабатывать и группа MoneyTaker. Самая первая атака, с которой мы связываем эту группу, была проведена весной 2016 года, когда в результате получения доступа к системе карточного процессинга STAR компании FirstData был ограблен National Bank of Blacksburg (США). В январе 2017 этот банк подвергся еще одной успешной атаке, о чем стало известно только спустя 7 месяцев после публичного релиза нашего отчета об атаках этой группы. В течение 2017 MoneyTaker взломала еще 9 банков в США.

Группа Silence провела свою первую атаку на карточный процессинг только в марте 2018 года и сразу успешно похитила 35 млн рублей в одном из банков в России.

Для успешного хищения через карточный процессинг атакующим не нужен специализированный софт, как например для атак на банкоматы или для автоподмены платежей в системах межбанковских переводов. **Поэтому этот метод доступен всем преступным группам, у которых есть опыт проникновения в банковские сети.**

ПЛАТЕЖНЫЕ ШЛЮЗЫ

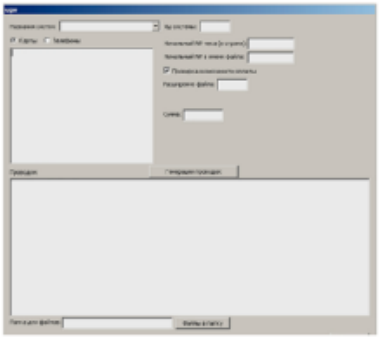
В этом периоде атаки на платежные шлюзы проводила только группа Cobalt. При этом во второй половине 2017 они похитили деньги у двух компаний, а в 2018 не сделали ни одной попытки. В результате реагирования на второй инцидент в 2018 году мы установили, что помощь в проведении этой атаки им оказывали участники из группы Anunak, которая не проводила подобных атак с 2014 года.

Логика работы шлюза подразумевает обработку двух каталогов In и Out, куда помещаются файлы, которые содержат данные в формате, соответствующем транзакциям, полученным от платежных терминалов. Файлы платежей в каталоге In принимаются к исполнению и денежные средства переводятся согласно данным, указанным в файле.

Чтобы изучить формат данных, атакующие воспользовались программой FileLogger.exe, позволяющей отслеживать изменения заданного каталога (создание новых файлов) и запись содержимого новых файлов в заданный текстовых файл. Каталог и файл задаются при запуске программы в качестве входных аргументов.

Через такие шлюзы осуществляются переводы небольших сумм, поэтому для крупного хищения необходимо создать множество мелких транзакций. Чтобы автоматизировать работу, атакующие создали уникальную программу **ugw.exe**.

Интерфейс ugw



Содержимое файла «ugw.ini»

```
[Config]
typeData=0
numchek=4919
numfilename=114320
dur=0
bad=0
ext=dnr
outfolder=D:\host\Gateway\In
```

При запуске программа запрашивает файл с именем «terminals.txt», в котором указываются идентификаторы терминалов, от имени которых якобы должны приходить запросы на перевод. Далее в программе указываются счета получателей в виде номеров телефонов и карт, а также суммы переводов.

В результате происходит генерация поддельных файлов-платежей, которые сразу помещаются в каталог In платежного шлюза. Таким образом, атакующим удалось перевести более $2 миллионов.

Подробнее об атаках Cobalt в отчетах Group-IB

group-ib.ru/reports

БАНКОМАТЫ

Атаки на банки с целью заражения их банкоматной сети проводят Cobalt, Silence, а также MoneyTaker. Последняя группа начала тестировать новый уникальный троян в мае 2018 года.

Cobalt

В 2016 году группа Cobalt провела серию успешных атак на банки и их банкоматные сети в России и за рубежом. Однако с осени 2016 года по декабрь 2017 года все их усилия были направлены на хищения другими способами. После продолжительной паузы, в декабре 2017 года они снова провели атаки на банкоматы в России.

При этом использовался все тот же троян **ATMSpitter**, которые преступники задействовали в атаках и на Тайване, и в Европе и в России. Никаких значимых изменений в код самой программы внесено не было. Она по-прежнему является консольной и использует стандартные функции по интерфейсу XFS через XFS Manager (eXtensions for Financial Services).

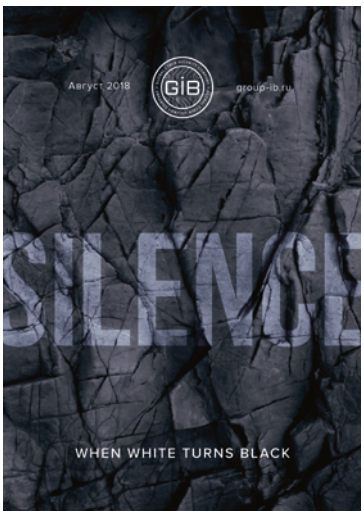
На вход программе передаются следующие параметры:

Параметр	Описание
ServiceLogicalName	Имя службы, которое будет использовано для функции WFSOpen. Например, Cash Dispenser Module.
Cassettes Count	Количество кассет в банкомате. Значение может быть от 1 до 15.
Cassette Number	Номер кассеты из которой надо выдать наличные. Значение может быть от 1 до 15.
Banknotes Count	Количество банкнот, которые надо выдать из кассеты. Значение может быть от 1 до 60.
Dispenses Count	Сколько раз операция выдачи должна повториться. Значение может быть от 1 до 60.

Silence

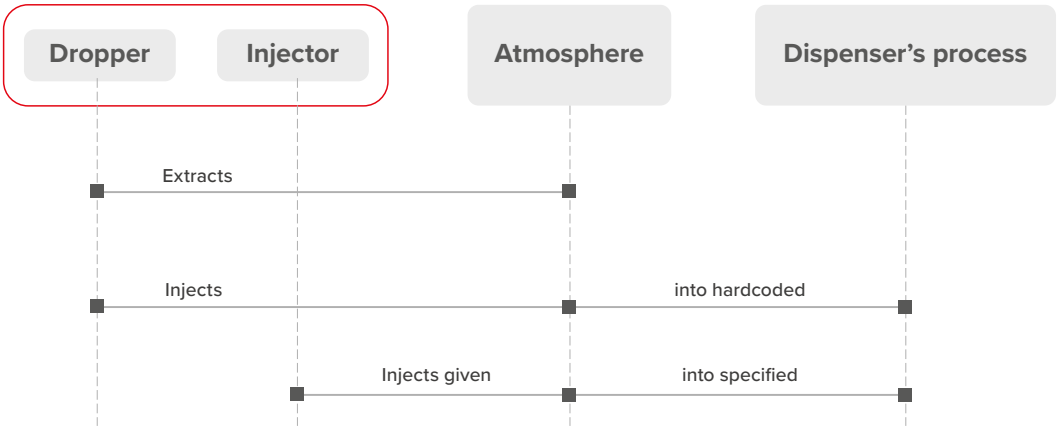
Для управления диспенсером банкоматов Silence использует уникальную программу **Atmosphere**. На протяжении всей видимой нам деятельности группы троян модифицировался, чтобы соответствовать требованиям атакующих. Так, троян изменил логику внедрения в процессы, автор добавил ему гибкий инжектор, что позволило расширить перечень поддерживаемых банкоматов, с которыми работала группа.

В дальнейшем троян был избавлен от ненужных функций, которые мешали или не использовались при работе преступников. Например, в последней версии программа не обрабатывала команды с пинпада, а генерируемый лог стал меньше. На начальном этапе развития программу перекомпилировали множество раз, что, скорее всего, и привело к нескольким безуспешным попыткам извлечь наличность.



Подробнее о самой перспективной новой хакерской группировке Silence в отчете Group-IB

group-ib.ru/reports



Хакеры удаленно устанавливают на банкомат Atmosphere.Dropper, в ресурсах которого содержится библиотека .DLL — основное тело трояна Atmosphere. После извлечения тела дроппер внедряет библиотеку в процесс с именем fwmain32.exe. Уже внутри управляющего процесса библиотека предоставляет возможность удаленного управления диспенсером. В первых версиях присутствовала возможность управления диспенсером с помощью пинпада, но позже эти функциональные возможности были удалены.

Параметр	Описание
“B”	Получает информацию о содержимом кассет ATM. Помимо этого в лог записывается строка «cash units info received».
“A”	Получает информацию о содержимом кассет без логирования.
“Q”	Получает информацию о содержимом кассет ATM.
“D”	Одноразовая выдача купюр конкретного номинала из банкомата.
“H”	Приостанавливает все потоки в процессе, кроме собственного, и при помощи функций GetThreadContext + SetThreadContext перенаправляет их выполнение на собственную функцию.
"M", "R", "S", "P", "T", "L"	Запись результата выполнения последней команды в файл «C:\intel\<chrs>.007» Эта команда также по умолчанию выполняется в конце любой другой.

Команды передаются программе через файлы с определенным расширением. После считывания и исполнения команд программа, по задумке автора, должна переписывать файл мусором и удалять его для затруднения работы форензик-экспертов. Однако логика программы содержит ошибку, вследствие чего мусор не пишется поверх файла, а дописывается в конец.

В ходе мероприятий по реагированию на инцидент информационной безопасности в одном из банков, команда криминалистов Group-IB обнаружила порядка 11 программ Atmosphere, скомпилированных в разное время и с незначительными изменениями. В одной директории с программами были найдены сценарии для командного интерпретатора, а также отдельный Injector, который принимал на вход в виде аргументов путь до библиотеки DLL и идентификатор процесса, куда должен был внедрить указанную библиотеку. Однако сценарии передавали не идентификатор процесса, а имя целевого процесса, что в итоге привело к безуспешной попытке получить контроль над диспенсером.

MoneyTaker

В мае 2018 года была произведена первая атака в России на банкоматы группой MoneyTaker. Для управления диспенсером была использована уникальная программа xfs_test.exe. Атакам подвергались банкоматы различных производителей.

Известно, что после проникновения в сеть злоумышленники пользовались набором скриптов PowerSploit, а также средством удаленного управления Radmin. Для начального перемещения в сети использовался фреймворк Metasploit — на машинах остались следы запуска Meterpreter стейджера через утилиту sc.exe.

В заголовке файла xfs_test.exe остался путь до отладочной информации:
M:\Work\atm\xfs_test\Release\xfs_test.pdb.

Программа позволяет при помощи XFS API взаимодействовать с диспенсером в ATM и давать команду на опустошение кассет. Исследованный специалистами Group-IB образец функционировал в соответствии с аргументом, передаваемым при запуске. Если указано неправильное значение аргумента, программа выводила в стандартный поток вывода сообщение об ошибке и завершала свою работу.

Передаваемый аргумент может иметь следующие значения:

Подробнее об атаках MoneyTaker в отчете Group-IB
group-ib.ru/reports

Параметр	Описание
info	Создать файл с именем «atm_info.log» и записать в него информацию о кассетах с наличностью и об их содержимом.
test	Несколько раз проверить возможность выдачи наличности из доступных кассет, при этом создать файл с именем «atm_test.log» и записать в него информацию о наличности, которая может быть выдана.
disp	Несколько раз осуществить выдачу наличности из доступных кассет (интервал между выдачами составляет 30 секунд), при этом создать файл с именем «atm_test.log» и записать в него информацию о выданной наличности.

АТАКИ НА КЛИЕНТОВ БАНКОВ

АТАКИ С ПОМОЩЬЮ ТРОЯНОВ ДЛЯ ПК

В России

Тренд на снижение угроз со стороны банковских троянов для ПК в России продолжается с 2012 года. За прошедший период ущерб сократился еще на 12% и составил 547 800 000 руб. Как и за предыдущий год, не появилось ни одного нового банковского трояна для ПК для хищений в России. Более того, **не осталось ни одной группы, которая бы занималась хищениями средств у физических лиц в России с использованием таких программ.**

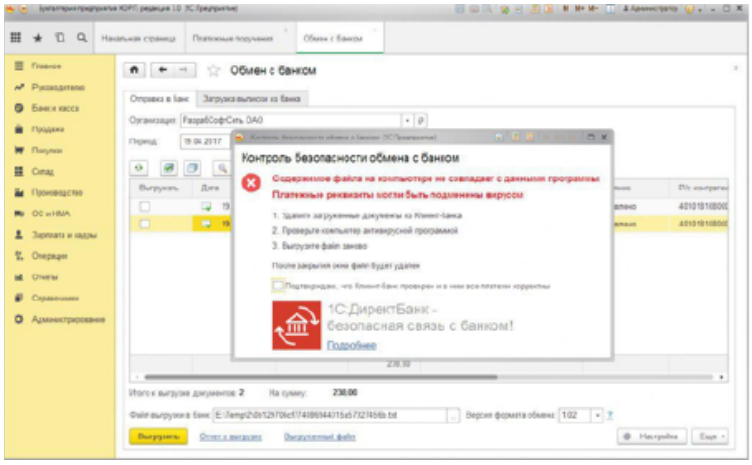
Активность проявляют только группы, которые используют банковские трояны для хищений у компаний. Таких команд осталось всего три: Buhtrap2, RTM, Toplel. При этом ни одна из них не использует атаку «человек-в-браузере» (Man-in-the-browser).

Buhtrap2

В 2016 года бот-сеть Buhtrap была продана и теперь используется другими злоумышленниками. Основным методом распространения в первой половине 2017 года был метод Drive-by: преступники взламывали легитимные сайты финансовой тематики (например, www.glavbukh.ru), при посещении которых загружался JavaScript, после чего происходила эксплуатация уязвимости браузера. В результате запускался PowerShell-скрипт, загружающий и приводящий в действие загрузчик Buhtrap.

Во второй половине 2017 года тактика атакующих изменилась: **вектором распространения троянов стала не традиционная вредоносная рассылка и не взломанные популярные сайты, а создание новых тематических ресурсов**, на которых злоумышленники размещали код, предназначенный для загрузки троянов.

Владельцы этой бот-сети активно использовали автоматические переводы через системы бухгалтерского учета 1С. После того, как разработчики 1С реализовали защиту от атак этого типа, включив проверку замены реквизитов, хакеры изменили свой код. **Новый Buhtrap способен обходить защиту «1С:Предприятие» «Контроль безопасности обмена с банком»** путем сокрытия отображаемого предупреждения.



RTM

Банковский троян RTM начал свою активность в 2016 году и остается востребован преступниками. В конце 2016 года мы видели, что при распространении трояна RTM использовался загрузчик из утекших исходных кодов Buhtrap. Такая связь нередко сбивает специалистов по информационной безопасности при атрибуции.

Как и в случае Buhtrap2, основными способами совершения хищения являются удаленное управление или автоматические переводы через системы бухгалтерского учета 1С. Однако мы не видели атак, которые бы обходили реализованную «1С:Предприятие» защиту от автоподмены реквизитов, как это сделано в Buhtrap.

Toplel

Преступная группа Toplel была обнаружена специалистами Group-IB в феврале 2015 года. В результате исследования было установлено, что она действует минимум с августа 2014 года и использует доменные имена, регистрируемые в зоне .SU. На тот момент для совершения хищений злоумышленники задействовали программу, известную как **RDPdoor (xTerm)**. Она предоставляет злоумышленнику удаленный доступ к компьютеру, что позволяет **совершать транзакции с рабочего места пользователя в тот момент, когда подключен токен с электронной цифровой подписью**, необходимой для подтверждения переводов. Программа распространялась преимущественно через письма с вредоносным вложением.

Основной целью злоумышленников были клиенты банков России и Украины. Модули трояна RDPdoor определяли следующие системы интернет-банкинга Ibank, bifit, Промсвязь, Альфабанк, Diasoft, Сбербанк, Комита, Tiny, Fobos, ClntW32, cbsmain, BCClient, Tival, cbs, Севергазбанк, Ibc, Interbank, RS.

Кроме трояна RDPdoor, преступники работают с модифицированной версией вредоносной программы Pony, которая может быть использована для сбора логинов и паролей на системах, не имеющих отношение к интернет-банкингу.

В мире

Глобальный ландшафт угроз со стороны банковских троянов изменился значительно сильнее. **Появилось шесть новых целевых троянов для ПК: IcedID, BackSwap, DanaBot, MnuBot, Osiris и Xbot**. Такое же количество троянов появилось и в прошлом году. Однако использование новых банковских троянов носит преимущественно локальный характер. Трояны Osiris и Xbot изначально предлагались на русскоговорящих хакерских форумах и пока не получили широкого распространения.

При этом со сцены ушли Shifu, Qadars, Sphinx, Tinba и Emotet. Последний по-прежнему используется, но только в качестве загрузчика, а не как полноценный банковский троян. Такое развитие событий может быть связано с работой правоохранительных органов, которые нанесли по рынку ощутимый удар арестами авторов банковских троянов Neverquest, GozNym, а также одного из самых популярных загрузчиков — Andromeda.

В 2017 году были опубликованы исходные коды банковских троянов **TinyNuke** и **AlphaLeon** (aka Thantaos, Mercury Bot), однако их дальнейшего использования не последовало.

Мы все еще видим использование банковских троянов, основанных на **Zeus (ZeusVM, Atmos, Panda)**, но значительно реже и без какого-либо значимого развития. Можно сказать, что они доживают последние дни.

Наиболее значимыми банковскими угрозами по-прежнему остаются группы, использующие трояны **Dridex, Trickbot, Gozi**.

КЕЙС: BACKSWAP

Новые техники автоподмены реквизитов

Из новых троянов наибольший интерес представляет BackSwap, который изначально атаковал только банки Польши, но затем стал работать и по испанским банкам. BackSwap интересен тем, что реализовал сразу несколько новых техник внедрения кода для автоподмены платежных реквизитов. Внедренный код заменяет оригинального получателя денежного перевода, но, чтобы жертва не заметила подмены, он демонстрирует поддельное поле ввода с первоначальным получателем платежа.

Консоль разработчика

В старых образцах BackSwap вставлял вредоносный скрипт в буфер обмена и имитировал нажатие комбинации клавиш, чтобы открыть консоль разработчика (CTRL+SHIFT+J в Google Chrome, CTRL+SHIFT+K в Mozilla Firefox). Затем он вставлял содержимое буфера (CTRL+V) и «нажимал» ENTER для выполнения содержимого консоли. Чтобы закрыть консоль, он повторял комбинацию клавиш. На это время окно браузера становится невидимым — обычный пользователь, скорее всего, думал, что браузер просто на несколько секунд завис.

JavaScript в адресной строке

В новых вариантах трояна схема была усовершенствована. Вместо взаимодействия с консолью разработчика вредоносный скрипт выполняется напрямую из адресной строки через специальный протокол JavaScript — малоиспользуемую функцию, которую поддерживает большинство браузеров. Программа имитирует нажатие CTRL+L для выбора адресной строки, DELETE — для очистки поля, «вводит» символы на JavaScript через вызов SendMessageA в цикле, после чего вставляет вредоносный скрипт с помощью комбинации CTRL+V. Скрипт выполняется после «нажатия» ENTER. В конце процесса адресная строка очищается, чтобы убрать следы компрометации.

Букмарклет

Троян создает закладку в браузере, но вместо URL-адреса добавляется JavaScript-программа, которая позволяет осуществлять автозамену платежных реквизитов при посещении банковских сайтов. Букмарклеты обычно не возвращают значения и просто выполняются браузером, имея доступ к открытой в нем странице. При этом они могут делать то же самое, что мог бы сделать скрипт, помещенный прямо на странице.

Глобальный ландшафт банковских троянов для ПК

	MnuBot New	BackSwap New	IcedID New	Osiris New	Xbot New	DanaBot New	Quakbot (Qbot)	Gozi (ISFB, Ursnif)	Trickbot	TinyNuke (aka NukeBot)	Gootkit	Dridex	Ramnit	ZeusVM (KINS)	Atmos	Zeus	Retefe	Corebot	UrlZone Banker	Panda Banker	Всего
Австралия						●		●	●		●	●		●	●	●					8
Австрия																	●				1
Аргентина									●											●	2
Бельгия									●				●	●		●					4
Болгария								●							●						2
Бразилия	●																				1
Великобритания			●								●	●	●	●	●	●	●				8
Германия									●				●	●	●	●					5
Испания		●					●		●					●	●	●					6
Италия								●						●	●	●			●		5
Канада			●				●		●				●	●				●		●	7
Колумбия																				●	1
Южная Корея								●													1
Нидерланды							●														1
Норвегия									●												1
Перу									●												1
Польша		●																	●		2
США			●				●	●	●			●	●	●	●	●			●	●	11
Турция															●	●					2
Франция									●	●		●	●		●				●		6
Швейцария																	●				1
Швеция																	●				1
Эквадор																				●	1
Южная Африка														●	●						2
Япония								●									●		●	●	4

АТАКИ С ПОМОЩЬЮ ANDROID-ТРОЯНОВ

После нескольких лет роста рынок Android-троянов в России вышел на плато, однако продолжает активно развиваться на мировой арене. Пять наиболее распространенных схем хищений, описанных нами в отчете за 2016 год, остались прежними:

- Хищение через SMS-банкинг
- Переводы с карты на карту
- Переводы через онлайн-банкинг
- Перехват доступ к мобильному банкингу
- Поддельный мобильный банкинг

Ландшафт банковских Android-троянов

ТРОЯНЫ, АТАКУЮЩИЕ SMS-БАНКИНГ (ТОЛЬКО В РОССИИ)	ТРОЯНЫ, ИСПОЛЬЗУЮЩИЕ ВЕБ-ФЕЙКИ В РОССИИ	ТРОЯНЫ, ИСПОЛЬЗУЮЩИЕ ВЕБ-ФЕЙКИ В МИРЕ
Agent.SX	Limebot (Lipton)	Easy
Flexnet	Asucub	Exobot 2.0
Granzy	Agent.BID	CryEye
Agent.BID	TarkBot	Cannabis
	Банки на ладони	Fmif
		AndyBot
		Loki v2
		Nero banker
		Sagawa
		Agent.cj
		Maza-in
		Loki v2
		Alien-bot
		Rello
		Red Alert v2

В России

Активность владельцев Android-троянов резко снизилась благодаря задержаниям в 2017 году владельцев крупнейших в России Android бот-сетей: **Cron** и **Tiny.z**. Кроме того, владелец другой крупной бот-сети **Honli** просто прекратил использование этого трояна.

Как следствие, **количество проводимых ежедневных хищений снизилось почти в три раза**. Также стоит отметить и снижение среднего размера хищений с использованием Android-троянов. Если в прошлом году он составлял 11 тысяч рублей, то в этом году он опустился до 7 тысяч.

Самой активной в прошедшем году была бот-сеть **Asacub** на базе одноименного приватного трояна. В августе 2017 появилось предложение о продаже форка этой вредоносной программы, но уже в сентябре тема была закрыта. Вторая по активности бот-сеть **Agent.BID** долгое время совсем не использовалась, и лишь с начала 2018 года ее владельцы вернулись к активной работе.

КЕЙС: БАНКИ НА ЛАДОНИ

Дистрибуция Android-трояна через Google Play

Преступникам удалось создать новую крупную бот-сеть с помощью вредоносной программы, замаскированной под финансовое приложение «Банки на ладони», выполняющего роль «агрегатора» систем мобильного банкинга ведущих банков страны. В приложение можно было загрузить все свои банковские карты, просматривать их баланс на основе входящих SMS по транзакциям, переводить деньги с карты на карту, оплачивать онлайн-услуги и покупки в интернет-магазинах. Программа распространялась через спам-рассылки, на форумах и через официальный магазин GooglePlay.

В мае 2018 года один из участников схемы был задержан. Злоумышленник переводил деньги на заранее подготовленные банковские счета суммами от 12 до 30 тысяч рублей за один перевод, вводя SMS-коды подтверждения операций, перехваченные с телефона жертвы.

В мире

Новые Android-трояны, предлагаемые на хакерских форумах, ориентированы прежде всего на использование за пределами России: **Easy, Exobot 2.0, Asacub, CryEye, Cannabis, fmif, AndyBot, Loki v2, Nero banker, Sagawa.** Исключением из этого списка является только Asacub.

После публикации исходных кодов трояна **Maza-in** появилось множество его клонов, которые используются до сих пор. В июле 2017 года другой автор банковского трояна под **Android Loki Bot** также выложил исходные коды в открытый доступ.

Троян **Agent.cj** носит чисто локальный характер и атакует пользователей турецких банков.

Обычно банковские трояны под Android распространяются через SMS/MMS рассылки. Однако троян **Exobot 2.0** в начале 2018 года распространялся через приложения, которые ранее были загружены из официального Google Play. В мае 2018, после того как автор полностью продал свой проект, исходные коды Exobot 2.0 были опубликованы в открытом доступе.

Очень активным русскоговорящим разработчиком банковских Android-троянов является хакер под псевдонимом GanjaMan, который разработал всем известные **Gmbot (aka Mazar), Skunk, VBV Grabber**. Его старые разработки более не используются, а сам автор этих вредоносных программ заблокирован на хакерских форумах. Однако до блокировки он успел продать исходные коды своего нового трояна **Cannabis**.

Трояны, которые были активны в прошлом периоде перестали использоваться, вероятно, из-за плохой поддержки их авторами. К таким троянам относятся **Xbot, Abrvall, Vasya, UfoBot, Reich**.

АТАКИ С ПОМОЩЬЮ ВЕБ-ФИШИНГА

В мире

За прошедший период GIB Threat Intelligence обнаружила и проанализировала 2,6 миллиона уникальных фишинговых ссылок на 727 тысячах доменах — на 9% больше, чем в прошлом году. Подавляющее большинство сайтов для хостинга фишинга (46%) использовали зону .com. на зоны .org, .mx, .net приходится по три процента. Как всегда основная масса фишинговых страниц хостилась в США — 63%. При этом большая часть фишинга хостится на легальных, но взломанных веб-сайтах.

В отличии от прошлого периода, первую позицию заняли фишеры, нацеленные на облачные хранилища, а не на финансовый сектор. Неожиданно, самым популярным среди фишеров стал Dropbox, хотя ранее мы видели, что атакующих больше интересуют сервисы Google. 73% всех фишинговых ресурсов попадают в следующие три категории: облачные хранилища (28%), финансы (26%), и онлайн-сервисы (19%).

Как и ожидалось, больше всего финансового фишинга относится к компаниям США. На их долю пришлось 80% всех атак в категории. Второе место занимает Франция, потом Германия. На различные проекты, связанные с криптовалютами, пришлось по 1%.

Фишеры, занимающиеся массовыми атаками, используют специальные фишинг-наборы (phishing kits). **За прошедший период система GIB Threat Intelligence собрала более 18 000 уникальных таких наборов** и проанализировала их конфигурационные файлы. В подавляющем большинстве случаев скомпрометированные данные отправлялись на адрес электронной почты. В 84% случаев фишеры регистрировали почту для сбора скомпрометированных данных на Gmail, на российские Yandex и Mail.ru приходится лишь 4%.

Phishing kit

– готовый фишинговый сайт с конфигурационным файлом, в котором определяется логика его работы и указывается, куда должны быть отправлены скомпрометированные данные.

В России

Веб-фишинг — единственный метод хищений, который показал рост в России в этом году. Количество групп, которые создают фишинговые сайты под российские бренды, выросло с 15 до 26. В России фишинг под банки и платежные системы автоматизирован и проходит в реальном времени, что позволяет обходить SMS подтверждения списания денег. Простота схем и широкий спектр инструментов для хищений привлекает на фишинговый рынок новых игроков.

В этом году с помощью веб-фишинга удалось похитить 251 миллион рублей, что на 6% больше, чем в прошлом году. Средняя сумма одного хищения не изменилась и составляет 1 000 рублей. Общее количество ежедневных успешных атак также выросло, но незначительно — до 1 274. Среднее количество жертв одной группы даже сократилось с 63 до 42. Основным фактором, сдерживающим рост количества атак, является активное выявление фишинговых сайтов и их оперативное закрытие, в том числе благодаря оперативному обмену данными между банками и ФинЦертом (FinCERT) Банка России.

Основными способами привлечения пользователей на фишинговые страницы являются перенаправление посетителей со взломанных сайтов, а также в результате попадания в поисковую выдачу. В России, в отличие от многих других стран, под большую часть фишинговых сайтов регистрируется отдельное доменное имя.

Большую популярность получил фишинг связанный с переводов с карты на карту. В некоторых случаях атакующие брендируют такие фишинговые страницы под конкретный банк, но есть и «небрендированный» фишинг.

КАРДИНГ

Рынок кардеров можно поделить на два основных сегмента: продажа текстовых данных о картах (номер, дата истечения, имя держателя, адрес, CVV) и «дампов» (содержимое магнитных полос карт). Текстовые данные собираются с помощью фишинговых сайтов, банковских троянов для ПК, Android, банкоматов, а также в результате взломов e-commerce сайтов. Дампы получают с помощью скимминговых устройств, а также с помощью троянов для компьютеров с подключенными POS-терминалами.

Большая часть скомпрометированных карт продается на специализированных кард-шопах. Системы GIB Threat Intelligence постоянно фиксируют и анализирует загружаемые на кард-шопы данные. **В среднем каждый месяц на них загружается 686 тысяч текстовых данных карт и 1.1 миллионов дампов.** По нашим данным, 62% продаваемых данных карт относятся к дампам. Это означает, что POS-угрозы являются основным методом компрометации банковских карт.

Кроме количественных показателей, мы фиксируем и стоимость каждого дампа, что позволяет измерять рынок кардинга. **Текстовая информация о банковских картах стоит на кардшопах значительно дешевле:** суммарно текстовые данные продавали всего за $95.6 миллионов, что составляет всего лишь 17% от общего рынка. Например, 19.9 миллионов дампов стоили уже $567.8 миллионов.

Оценка рынка кардшопов

H2 2017 – H1 2018, данные Group-IB

	Текстовые данные	Дампы	Всего
Общее количество	10 218 489	16 927 777	27 146 266
Размер рынка	$95 590 424	$567 791 443	$663 381 867
Минимальная цена	$0.75	$0.5	
Максимальная цена	$99.99	$295	
Средняя цена	$9.35	$33.54	
Медиана	$8	$25	

POS-угрозы

Основным методом получения дампов банковских карт является использование POS-троянов, которыми заражают компьютеры с подключенными POS-терминалами. Принцип работы всех POS-троянов остался неизменным: они собирают данные карт из оперативной памяти в тот момент, когда карты считывают через POS-терминал.

Атакующие по-прежнему делятся на две категории:

- массово и случайно атакующие всех подряд в поисках возможности установить POS-троян;
- целенаправленно атакующие вендоров POS-терминалов или крупные сетевые организации, доступ в сети которых открывает возможность заражения сразу множества устройств.

Самый серьезный удар по индустрии кардинга был нанесен в начале 2018 года, когда Министерство юстиции США сообщило об аресте и предъявлении обвинений трем гражданам Украины, которые входили в состав группы **FIN7 (aka Navigator)**. Согласно данным из обвинительных заключений Дмитрий Федоров (Hotdima), Федор Гладырь (Das или AronaXus) и Андрей Копаков (Santisimo) были задержаны в январе и марте 2018. Официальное заявление Министерства юстиции гласит, что с 2015 года группа FIN7 атаковала более 100 компаний и организаций на территории США, взломав тысячи различных систем. Сообщается, что только в США хакеры похитили свыше 15 миллионов платежных карт, скомпрометировав более 6 500 POS-терминалов.

Рынок POS-угроз достаточно динамичный. Отслеживая андеграундные форумы и участвуя в реагировании на инциденты, **специалисты Group-IB регулярно наблюдают появление новых троянов, а также продажу и публикацию в открытом доступе исходных кодов** уже зарекомендовавших в реальных атаках инструментов.

Продажа и публикация исходных кодов POS-троянов

05 октября 2017 На андеграундном форуме было опубликовано объявление о продаже исходного кода банковского бота **Dented**. Данный троян обладает функциями по сбору TRACK1 и TRACK2 банковской карты. Продажа осуществляется трем клиентам по цене $3000 с оплатой в Bitcoin.

2017

01.06.2017
Обнаружение POS-трояна LockPos

10.07.2017
Атаки на бразильские компании с помощью LockPos

10.09.2017
Продажа Sisyphus POS
Атакующий — refreshers
Форум — exploit.in

01.10.2017
Группа Lazarus использует в Южной Корее RatankbaPOS

05.10.2017
Продажа банковского трояна Dented Banking Bot с POS-граббером
Атакующий — refreshers
Форум —exploit.in

10.11.2017
Обнаружен троян GratefulPOS

15.11.2017
Атака на пабы и рестораны с помощью Alina POS

01.12.2017
Продажа исходного кода NCR Radiant (RPOS)
Атакующий — iscorb
Forum — exploit.in

01.12.2017
Идентифицирован троян PinkKite

2018

08.02.2018
Продажа исходного кода POS-сниффера
Атакующий — ftp_admin
Форум — exploit.in

15.02.2018
Обнаружен троян UDPoS

13.04.2018
Утечка исходного кода трояна Treasure Hunter
Атакующий — crossair
Форум — exploit.in

08.05.2018
Утечка исходного кода POS-трояна
Атакующий — unsigned
Форум — exploit.in

08.06.2018
Продажа исходного кода MagicPos
Атакующий — cocofresh
Форум — exploit.in

04.07.2018
Поиск Remote Desktop Protocol с доступом к POS
Атакующий — beau
Форум — exploit.in

8 февраля 2018 Пользователь ftp_admin выставил на продажу исходные коды своего трояна **POS Sniffer** за $5000. Троян, продававшийся с марта 2016 года, реализован в виде драйверов к системе и работает под Windows x32.

08 июня 2018 Пользователь cocofresh опубликовал тему с продажей исходных кодов POS-трояна **MagicPos** с административной панелью за $350.

08 мая 2018 Пользователь Unsigned char опубликовал ссылку на скачивание исходных кодов POS-трояна для сбора Track1 и Track2.

06 апреля 2018 Пользователем crossair опубликовал на андеграундном форуме архив, содержащий исходные коды POS-трояна **Treasure Hunter**. Впервые информация об этом трояне появилась еще в 2014 году. Архив trhutt34C.rar содержит внутри себя два файла: adminPanel.rar и cSources.rar — исходные коды административной панели и самой вредоносной программы.

Новые трояны

Июнь 2017 Зафиксирована серия атак на бразильские компании с новым POS трояном **LockPos**, который связывают с группой, ранее использовавшей **FlokiBot**.

Сентябрь 2017 Пользователь Refreshers опубликовал тему по продаже нового трояна для POS-систем **SisyphusPOS**.

Октябрь 2017 Специалисты из Proofpoint обнаружили, что группа Lazarus использует новый POS-троян **RatankbaPOS** для атак на компании в Южной Корее.

Ноябрь 2017 Специалистами RSA был выявлен новый POS-троян **GratefulPOS**, код которого состоит из фрагментов кодов вредоносных семейств FrameworkPOS, TRINITY, BlackPOS и BrickPOS. По аналогии с FrameworkPOS, вредонос извлекает данные платежных карт из оперативной памяти терминала и отправляет их на управляющий сервер в виде зашифрованных DNS-запросов.

Декабрь 2017 Исследователи из компании Kroll Cyber Security идентифицировали еще один POS-троян **PinkKite**. PinkKite весит всего 6 КБ и содержит модули считывания памяти и проверки данных. Особенностью этой кампании является ручная пересылка данных карт через отдельный сеанс RDP на один из трех центров обмена информацией PinkKite.

Февраль 2018 Исследователи из компании Forcepoint обнаружили троян с именем **UDPoS**, маскирующийся под легитимное средство удаленного управления LogMeIn и передающий данные кредитных карт с помощью DNS-запросов.

ATM-угрозы

Некоторые группы не способны взломать сеть банка и заразить банкоматную сеть, но **могут заразить отдельные банкоматы при наличии физического доступа.** В прошедшем периоде для банковского сектора активными были две угрозы: **Cutlet** и **Ploutus-D**.

Общая схема атаки «Jackpotting» включает 3 уровня злоумышленников:

- организатор / заказчик;
- разработчик ПО;
- дропы.

Главным в атаке является организатор, чаще всего он и заказывает разработку вредоносной программы.

Основной целью организатора является получение денег с минимальными рисками. Для начала работы ему нужен полный набор инструментов. Есть два пути для их получения: заказать у разработчиков или перекупить у других злоумышленников. Далее организатор находит команду дропов (не менее 2-х человек) — людей, которым необходимо получить физический доступ к внутренней системе банкомата. Чтобы дропы не обманули организатора и не начали самостоятельную работу, в наборе вредоносных программ имеется специальный генератор ключей. Когда вредоносное ПО загружается в банкомат, оно требует ключ активации для дальнейшей работы. Такой ключ можно получить только из генератора ключей, который находится у организатора.

Для вскрытия банкомата злоумышленники высверливают, прорезают или прожигают отверстия на лицевой панели клавиатуры банкомата. Средний размер отверстия составляет 5 сантиметров. После этого они получают прямой доступ к шлейфу проводов.

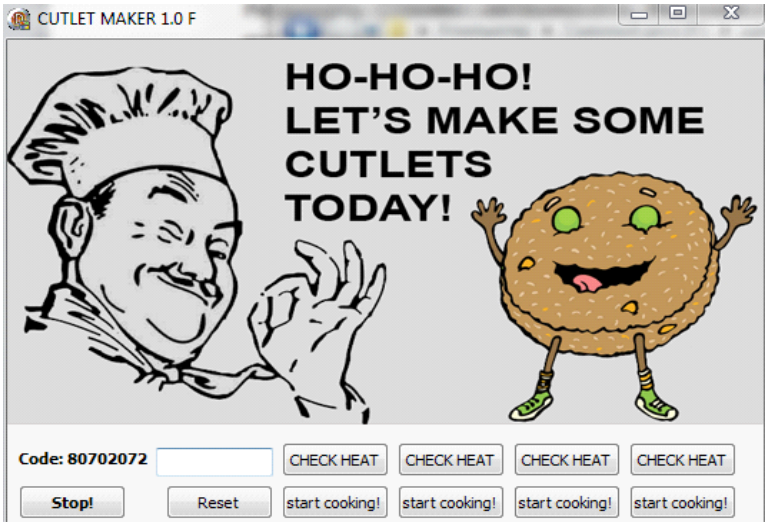
Злоумышленники отсоединяют диспенсер от USB-хаба или COM-порта (в зависимости от банкомата) и устанавливают на его место специальную заглушку, которая имитирует работу диспенсера. Затем они подключают к USB/COM порту диспенсера микрокомпьютер с низким энергопотреблением.

В этот момент дропы используют телефоны для взаимодействия с организатором и получения ключа активации.

Средняя продолжительность действий злоумышленников, требуемых для хищения денежных средств, составляет около 8 минут. После получения наличности преступники заклеивали отверстие в банкомате с помощью наклейки.

Cutlet

В середине 2017 года появился **новый комплект для атак на банкоматы, в том числе с новой вредоносной программой, которую назвали cutlet**. Теперь вместе с набором инструментов шла максимально подробная инструкция по использованию с советами, как избежать проблем при работе. Впоследствии cutlet получила собственное приложение под Android, что позволяло злоумышленнику не использовать ноутбук, а обходится смартфоном.



Набор «Cutlet» до сих пор остаётся актуальным. Мы наблюдаем большое количество активных тем о продаже на хакерских форумах.

06 декабря 2017 Пользователь под ником cutlet master опубликовал предложение о продаже полного набора софта **Cutlet Maker** на форуме crdclub.ws. Стоимость полного набора составила 1 000$. в набор входят 3 программы:

- Stimulator22 — предназначена для проверки баланса в кассетах банкомата;
- c0decalc — предназначена для генерации кода активации программы Cutlet Maker;
- Cutlet Maker 1.0 F — предназначена для вывода денег из банкомата.

15 декабря 2017 Пользователь под ником md5 опубликовал предложение о продаже полного набора софта Cutlet Maker на форуме ifud.ws. Стоимость полного набора составила уже $800, однако через неделю цена была снижена до $500. Отметим, что самый первый комплект «cutlet» продавался за $5 000.

17 января 2018 Пользователь под ником «she0» опубликовал предложение о продаже полного набора софта «Cutlet Maker» на форуме moneymaker.hk. Стоимость полного набора составила 50 000 рублей.

20 декабря 2017 На самом популярном русскоязычном андеграундном форуме exploit.in была устроена бесплатная раздача полного набора ПО. Пользователь под ником Onions пообещал раздать софт первым 3 отписавшимся старожилам форума.

20 декабря 2017 На форуме migalki.pw пользователь под ником vulns опубликовал ссылку для скачивания cutlet. Архив содержал два файла: cm17F (Cutlet Maker 1.7 F), Stimulator22.

28 мая 2018 Пользователь с псевдонимом sl111 опубликовал объявление о продаже нового ATM трояна **Котлета v2**. Объявление было размещено на форуме exploit.in. Котлета v2 представляет собой вредоносную программу для банкоматов Wincor. Исходя из текста объявления, Котлета v2 обладает практически теми же функциональными возможностями, что и Cutlet Maker. Отличием трояна от своего предшественника является отсутствие необходимости в генерации паролей активации (генерация происходила с помощью утилиты c0decalc.exe). Автор объявления, судя по сообщению являющийся разработчиком этого вредоносного ПО, предложил троян вместе с исходными кодами. Троян написан на C/C++. Цена Котлеты v2 составляет $5 000. В комплекте с трояном идут исходные коды, документация и инструкция по его применению.

Ploutus-D

25 января 2018 компания Diebold Nixdorf опубликовала отчёт «Potential Jackpotting US». В нём сообщается, что власти США предупреждают компанию о том, что на территории США впервые зафиксирована атака типа «Jackpotting» на банкоматы, произведенные их компанией. Ранее, в октябре 2017 года подобная атака была зафиксирована на территории Мексики. Также в СМИ появилась информация, что атаке могли подвернуться банкоматы компании NCR Corp.

Предположительно, злоумышленники для атаки использовали вредоносное ПО Ploutus-D.

Ploutus-D – новая модификация более старой версии Ploutus. Эта программа впервые была замечена в Мексике в 2013 году. Тогда она распространялась при помощи CD-ROM. Первые упоминания Ploutus-D на андеграундных форумах датируются началом 2017 года. Однако ни одного положительного отзыва о работе или хотя бы проверке данного ПО нет, а все вендоры, которые создавали топики о его продаже, имеют плохую репутацию. Активных продаж программы на андеграундных форумах не замечено.

Ploutus не уникальная разработка, в мире существует несколько различных реализаций примерно одной и той же схемы атаки. Различия между ними минимальны и сводятся к специализации на определённом виде банкоматов, наиболее распространённых в регионе использования программы.

6. УГРОЗЫ ДЛЯ КРИПТОВАЛЮТНОГО РЫНКА И БЛОКЧЕЙН-ПРОЕКТОВ

Трояны для хищения приватных ключей, массовые фишинговые атаки, майнеры, перебор паролей, дефейс сайта, угон доменов и различного рода мошенничества с криптовалютами уже стали обыденностью. Вместе с тем, ландшафт угроз для криптовалютного рынка непрерывно меняется, и в этом году мы видим появление новых схем для кражи криптовалют и взломов торговых площадок, а также адаптацию схем, характерных для взломов в финансовом секторе.

АТАКИ НА БЛОКЧЕЙН-ПРОЕКТЫ

В 2018 году мы наблюдали различные типы атак на блокчейн-проекты, среди которых можно выделить следующие:

Атака на блокчейн (Blockchain attack)
Эксплуатирование особенностей конкретных аспектов самой технологии блокчейн, как в «атаке 51%» или атаке повторного вывода средств.

Повторное использование учетных данных (Credentials reuse)
Использование злоумышленниками известных им идентификаторов пользователя в других сервисах для получения доступа к кошельку (при условии их совпадения).

Взлом домена (Domain hijacking)
Изменение данных регистрации домена. Например, хакеры изменяют A-записи и перенаправляют трафик веб-сайта на вредоносный сервер для сбора данных (логинов и паролей) или перевода средств.

Мошенничество изнутри проекта (Insider work)
Использование доступа к информационным системам для кражи криптовалюты членом команды проекта или аутсорсным специалистом.

Вредоносное ПО (Malware)
Атаки с использованием специально разработанного вредоносного программного обеспечения. Вредоносные программы используются не только для кражи приватных ключей или паролей пользователей, но и для доступа к машинам системных администраторов, а также создания бэкдоров в инфраструктуре биржи.

Фишинг (Phishing)
Использование полной копии или имитации оригинального веб-сайта проекта, поддельных писем или сообщений от имени проекта для кражи конфиденциальной информации или загрузки вредоносного ПО на компьютеры жертв.

Уязвимость в исходном коде (Source code vulnerability exploitation)
Использование логических ошибок или других уязвимостей в программном обеспечении, используемом на проекте.

МАНИПУЛЯЦИИ КУРСАМИ КРИПТОВАЛЮТ

Существует множество различных схем манипуляций криптовалютным рынком. Например, схемы **Pump&Dump (P&D)**. В таком случае трейдеры объединяются в группы в Telegram или Discord, число членов которых достигает нескольких тысяч человек. Затем они выбирают определенную криптовалюту, не имеющую особой ценности и перспектив (такие криптовалюты называют «shitcoin») и начинают одновременно скупать ее, тем самым искусственно взвинчивая курс. Этот этап называется «пампом», а следующий за ним этап, когда участники схемы продают свои позиции, – «дампом».

Большинство мошеннических схем и инструментов атак, используемых для хищения криптовалют, аналогичны тем, что используются на традиционных рынках для хищения сведений о банковских картах и других пользовательских данных. Еще в 2016 году мы выпустили отчет о том, как хакерская группа Corkow взломала банк и, используя его брокерские счета, повлияла на обменный курс рубля. Аналогичное мошенничество, но с криптовалютой совершили неустановленные хакеры в начале 2018 года. Подготовка к атаке заняла более двух месяцев.

Тактика действия атакующих на криптовалютном рынке была следующей:

1. В январе 2018 года неизвестная группа хакеров зарегистрировала домен, созвучный с брендом крупнейшей китайской криптобиржи Binance.
2. Ссылки на фишинговый ресурс начали рассылать трейдерам этой криптобиржи с целью получения их логинов и паролей.
3. Получив логины и пароли, атакующие смогли создать API-ключи, которые позволяют автоматизировать работу с биржей.
4. 7 марта 2018 года в течение двух минут атакующие автоматически, используя созданные ранее API-ключи скомпрометированных трейдеров, разместили множество заявок на покупку малоизвестной криптовалюты Viacoin.
5. Заявки на покупку привели к тому, что через 30 минут курс Viacoin подскочил на 143% с $2.80 до $6.79, по данным coinmarketcap.com.
6. После того как курс Viacoin вырос, атакующие начали продавать их за bitcoin с 31-го заранее подготовленного аккаунта.
7. После окончания торгов были отправлены запросы на вывод средств.

АТАКИ НА ICO

В 2018 году количество проектов, выходящих на ICO снизилось, а их качество и уровень подготовки к кибератакам стали значительно выше. При этом объемы средств, которые вкладывают инвесторы, стали значительно больше, что привлекает внимание злоумышленников, за 2017 год «заработавших» на ICO более $400 миллионов. Только за первое полугодие 2018 года ICO-проекты собрали почти $14 млрд — в два раза больше, чем за весь 2017 год ($5,5 млрд).

В 2018 году атакам подверглись проекты, проводящие закрытый раунд ICO. Например, проект TON (Telegram Open Network), основанный Павлом Дуровым, подвергся фишинговой атаке, в результате чего злоумышленникам удалось украсть около $35,000 в Ethereum.

Все самое плохое, как правило, происходит именно в день старта продаж токенов в рамках проведения ICO. Шквал DDoS-атак одновременно с наплывом пользователей, лавина сообщений в в каналы Telegram и Slack, спам по списку рассылок.

Фишинг

Около 56% всех средств, украденных в ходе ICO, были похищены с помощью фишинговых атак. В разгар «криптовалютной лихорадки» все стремятся как можно быстрее купить токены (зачастую они продаются с большой скидкой) и не обращают внимания на такие мелочи, как подмененные домены. При этом фишинговая атака на ICO не требует серьезной подготовки и высокой квалификации.

Схема атакующих осталась неизменной с 2016 года:

- Злоумышленники отслеживают новые проекты, выходящие на ICO.
- Создают фишинговую страницу на доменном имени схожим с оригинальным. Основным отличием страницы является запрос секретного ключа или требование перевести криптовалюту на адрес мошеннического кошелька или смарт-контракта.
- На оригинальный сайт проекта начинается DDoS-атака, чтобы сделать его недоступным и спровоцировать инвесторов переходить на фишинговый ресурс.
- Одновременно с DDoS-атакой начинается SPAM-рассылка со ссылкой на фишинговый сайт.
- Кроме того, злоумышленники покупают контекстную рекламу в поисковых сетях, организовывают лавину сообщений в мессенджерах и любыми способами стараются нагнать трафик на фишинговый сайт, чтобы поднять его в топ поисковой выдачи.

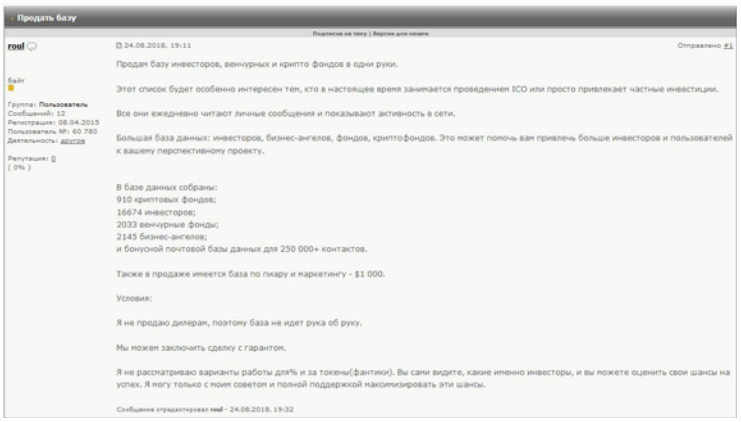
Если основной сайт проекта, выходящего на ICO, уязвим, то тактика меняется. Вместо создания фишингового ресурса **непосредственно перед стартом ICO на оригинальном сайте заменяется адрес кошелька** или смарт-контракта на мошеннические.

Кража проекта

Одна из особенностей проектов, выходящих на ICO, — полная открытость и прозрачность. Большая часть разработок и исходных кодов публикуется в открытом доступе. В первую очередь команда публикует White Paper, что открывает возможности для мошенничества.

- Злоумышленники находят новый не сильно раскрученный проект, но с хорошо проработанным описанием.
- Описание проекта полностью копируется и переводится на разные языки.
- Создается лендинг под новым брендом и с новой командой, но с ворованным описанием.
- Проект под новым брендом раскручивается в сети. Появляется контекстная реклама, ведутся обсуждения на специализированных площадках, чтобы привлечь внимание инвесторов.

Фишинговые атаки на ICO-проекты не всегда проводятся с целью хищения средств. В этом году зафиксировано несколько случаев кражи баз данных инвесторов, участвующих в ICO. Такая информация затем может продаваться на андерграундных форумах или использоваться для шантажа.



ЦЕЛЕВОЙ ВЗЛОМ КРИПТОБИРЖ

В прошлом отчете мы уже писали, что **у хакеров которые могут профессионально провести целенаправленную атаку и похитить миллионы долларов появилась новая цель – криптобиржи.** От их рук в 2016 году пострадали Bitfinex, Shapeshit, Gatecoin, Bitcurex.

В 2017 и 2018 годах внимание хакеров к криптобиржам только возросло. Всего за 2017 год и первые 9 месяцев 2018 года было взломано 13 криптовалютных бирж, как минимум 5 из них были атакованы северокорейскими хакерами из группы Lazarus, чьи жертвы преимущественно находятся в Южной Корее. Биржа YouBit (бывшая Yapizon) после второй атаки потеряла 17% своих активов и обанкротилась.

Суммарно за 2017 и первые 9 месяцев 2018 года в результате взломов криптовалютных бирж было похищено $877 миллионов в криптовалюте. 60% от общей суммы было похищено у японской биржи Coincheck.

Основным вектором проникновения в корпоративные сети криптобирж стал целевой фишинг. Злоумышленники отправляют вредоносные вложения, например, с темой «Engineering Manager for CryptoCurrency job», «Investment Proposal.doc», маскируясь под юридические компании и другие криптобирж. В случае запуска вредоносных файлов на компьютеры жертв устанавливается RAT, разработанный и постоянно обновляемый хакерской группой Lazarus. Далее злоумышленники исследуют локальную сеть и находят рабочие места или серверы, на которых осуществляется взаимодействие с приватными кошельками криптобирж.

Дата*	Название проекта	Страна	Преступная группа	Похищено в криптовалюте	Похищено в USD
Фев 2017	Bithumb	Южная Корея	Unknown	-	$7 mln
Апр 2017	YouBit	Южная Корея	Unknown	-	$5.6 mln
Апр 2017	Yapizon (YouBit)	Южная Корея	Lazarus	3,816 BTC	$5.3 mln
Авг 2017	Ether Delta	-	Unknown	-	$266 k
Авг 2017	OKEx	Гонконг	Unknown	-	$3 mln
Сен 2017	Coinis	Южная Корея	Lazarus	-	-
Дек 2017	YouBit	Южная Корея	Lazarus	17% активов	-
Янв 2018	Coincheck	Япония	Lazarus	523,000,000 NEM	$534 mln
Фев 2018	Bitgrail	Италия	Uknown	17,000,000 NANO	$170 mln
Июн 2018	Bithumb	Южная Корея	Lazarus	-	$32 mln
Июн 2018	Coinrail	Южная Корея	Uknown	11 разных криптовалют	$37 mln
Июн 2018	Bancor	-	Uknown	-	$23 mln
Сен 2018	Zaif	Япония	Uknown	-	$60 mln
				Всего	**$877 mln**

* Итоговые данные в таблице были изменены 22 октября 2018 года.

КРИПТОДЖЕКИНГ

Криптоджекинг – относительно новое направление, получившее наибольшее развитие в 2017-2018 гг. После загрузки специализированного вредоносного программного обеспечения вычислительные ресурсы компьютера используются злоумышленниками для добычи криптовалюты без ведома владельца. Программы для скрытого майнинга распространяются на тысячи компьютеров, образующих ботнет.

Количество криптовалюты, получаемой в результате майнинга, напрямую зависит от совокупной производительности ботнета, поэтому вычислительные мощности в корпоративных сетях представляют для злоумышленников больший интерес, чем персональные компьютеры. Для массового распространения может использоваться, например, EternalBlue Exploit (CVE-2017-0144). Подобная уязвимость была использована при распространении шифровальщиков WannaCry в мае 2017 года и Petya в июне 2017 года. Так, операторы бот-сети намайнили при помощи трояна **Smominru**, распространявщегося с помощью EternalBlue Exploit, приблизительно 8 900 Monero ($2.8-$3.6 миллионов). Каждый день ботнет добывал примерно 24 Monero, что на тот момент в среднем составляло $8500.

Одной из первых успешных попыток разработки программного обеспечения для майнинга в браузере является решение **Coinhive**, заявившее о себе в сентябре 2017 года. Вслед за ним появились **CryptoLoot, JSEcoin, Minr, CoinImp, ProjectPoi (PPoi), AFMiner**, **Papoto**. Эти проекты предоставляли API, позволяющий владельцам веб-сайтов использовать вычислительные мощности компьютеров своих пользователей для майнинга криптовалюты. Такая модель сразу же привлекла внимание многих хакеров, которые обладают знаниями о том, как работать с нелегальным веб-трафиком.

Можно выделить следующие векторы компрометации с целью встраивания вредоносных скриптов для майнинга:

Взлом веб-сайтов

Взломы могут осуществляться разными способами: подбор паролей, эксплуатация уязвимостей в CMS или другом программном обеспечении, перехват паролей с помощью вредоносных программ или фишинговых сайтов. Поскольку майнинг осуществляется на компьютере посетителя и только в момент просмотра веб-сайта, залогом успеха является не количество взломанных сайтов, а их аудитория. Поэтому, как это было и с распространением обычных троянов методом Drive-by download, сайты с высоким количество посетителей ломаются целенаправленно.

Расширения для браузеров

В 2017 году появилось расширение для Google Chrome под названием Active Poster. По некоторым оценкам, в скрытом майнинге участвовало более 100 тысяч пользователей. После нескольких жалоб в службу поддержки расширение было удалено. Аналогичные расширения были найдены и в браузере Mozilla Firefox.

Уязвимость третьей стороны (Third party services)

Многие сайты используют сторонние JavaScript-библиотеки на своих страницах. Обычно это рекламные сети, аналитические или трекинговые сервисы. Операторы таких решений могут вставлять в свои скрипты майнинговый функционал специально или в результате компрометации со стороны хакеров, как это было со скриптами Coinhive на YouTube.

Атаки Man-in-the-Middle

Пользовательский трафик перенаправляется через промежуточные звенья, у которых зачастую есть доступ к контенту. Например, злоумышленники могут перехватывать незащищенный трафик, проходящий через точки доступа в публичный Wi-Fi, и вставлять в него к криптоджекинг-скрипты. Такие атаки уже были применены к сети Starbucks в Аргентине.

Незаменимым инструментом для проведения таких атак становятся бот-сети из домашних роутеров, например, Mirai и его аналоги. Заразив домашний роутер, можно манипулировать трафиком всех пользователей, которые его используют. В одном из последних случаев атакующему удалось найти 0-day уязвимость в маршрутизаторе MikroTik. С ее помощью он смог заразить около 200 000 устройств, которые встраивали в отображаемые страницы скрипт для майнинга от Coinhive.

АТАКА 51%

Как следует из названия, эта атака подразумевает установления контроля над 51% мощности системы. В роли атакующих может выступать как один майнер с крупным сосредоточением вычислительной техники, так и группа — пул. Однако получение контроля над 51% мощности не обязательно считать атакой, по крайне мере, до тех пор, пока владелец этой мощности не начнет целенаправленно использовать свое преимущество.

Владея 51% мощности сети, атакующий может:

- заморозить работу системы;
- остановить подтверждение транзакций;
- приостановить майнинг;
- лишить других майнеров возможности подтверждать транзакции;
- списывать средства повторно.

Наибольшей опасностью для системы считается повторное списание средств (double spending). Так, атакующий может создать скрытый альтернативный блокчейн и использовать его для подтверждения собственных транзакций. Двойное списание средств возможно и при меньшем контроле мощностей, но именно сосредоточение 51% предоставляет 100% гарантию, что верным блоком будет признан блок злоумышленника.

О самой «атаке 51%» известно уже давно. Например, в 2016 году проекты Krypton и Shift подверглись атаке этого типа. В том же году известный в криптосообществе китайский предприниматель Чандлер Го заявил, что намерен при поддержке других майнеров осуществить «атаке 51%» на проект Ethereum Classic.

И если в 2017 успешных атак этого типа не было, то **в первой половине 2018 рынок столкнулся сразу с пятью случаями успешных атак**:

- **4 апреля** Сеть криптовалюты Verge подверглась «атаке 51%», которая стала возможной из-за бага в коде. Атака продлилась примерно три часа и, по оценкам одного из участников дискуссий, атакующий мог добыть криптовалюту на сумму более $1 миллион.
- **18 мая** Директор по коммуникациям Bitcoin Gold Эдвард Искра впервые предупредил об атаке и указал, что майнер захватил по меньшей мере 51% хешрейта сети. Так, начиная с 16 мая на BTG-адрес атакующего поступило более 388 тысяч монет Bitcoin Gold. Таким образом, злоумышленник мог «заработать» около $18 миллионов.
- **22 мая** Майнинговый пул SuprNova сообщил, что блокчейн криптовалюты Verge подвергся атаке 51% и все корректные блоки отвергаются. По их информации, проблема затронула все пулы и всех майнеров, поскольку злоумышленник на тот момент контролировал все блоки. Представители самого проекта ранее сообщили о вероятной DDoS-атаке на пулы и задержках с валидацией блоков.
- **3 июня** Блокчейн ZenCash подвергся «атаке 51%», в результате которой неизвестные злоумышленники похитили более $550000 в эквиваленте криптовалюты ZEN. Злоумышленникам удалось реорганизовать 38 блоков, а сама атака продлилась менее четырех часов. по данным сайта Crypto51, который оценивает затраты на «атаки 51%», операция обошлась злоумышленникам в $30000.
- **6 июня** Сеть недавно появившейся криптовалюты Litecoin Cash (LCC), которая является форком более известной криптовалюты Litcoin (LTC), также столкнулась с атакой 51%.

ОГРАНИЧЕНИЕ ПРИМЕНЕНИЯ

Настоящим Group-IB информирует о том, что:

- Настоящий отчет подготовлен специалистами Group-IB без какого-либо финансирования третьми лицами.

- Оценка рынка высокотехнологичных хищений проводилась на основании собственной методики Group-IB.

- Описание технических деталей угроз в настоящем отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованные в настоящем отчете технические детали угроз ни в коем случае не являются пропагандой мошенничеств и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.

- Все упоминания компаний и торговых марок в настоящем отчете сделаны на основании полученных от таких компаний разрешений и/или на основании уже опубликованных в средствах массовой информации сведениях.

- Сведения, опубликованные в настоящем отчете, могут быть использованы заинтересованными лицами по своему усмотрению при условии указания ссылки на Group-IB.

О GROUP-IB

15 ЛЕТ
практического опыта

55 000+
часов реагирования

1 000+
расследований по всему миру

Group-IB — один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

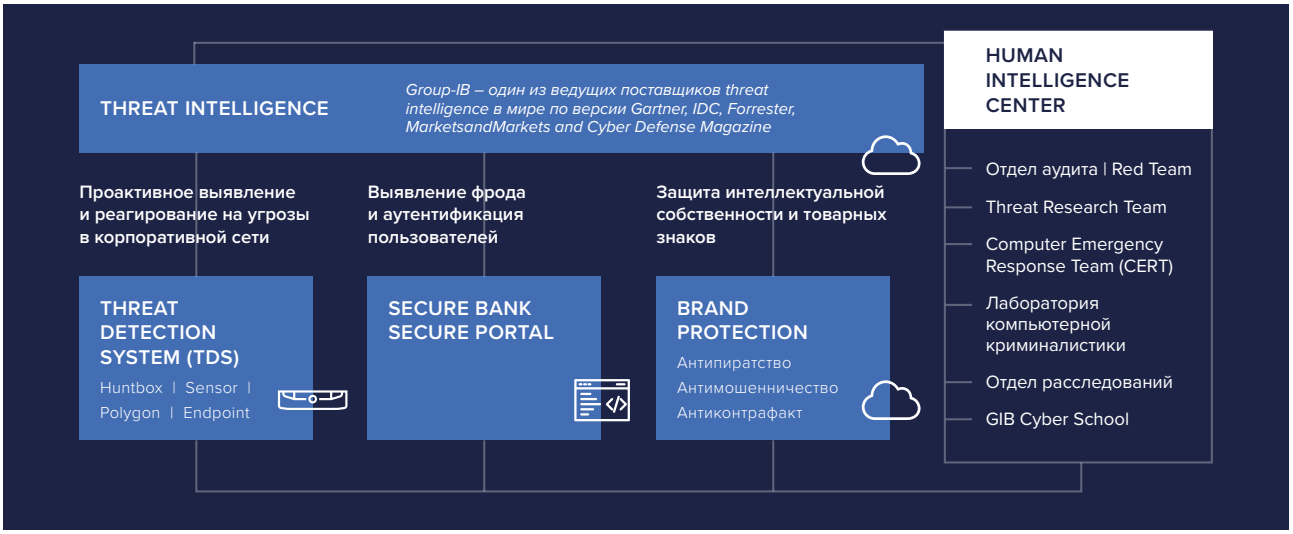
- Партнер Interpol и Europol
- Поставщик решений в сфере кибербезопасности, рекомендованный SWIFT и ОБСЕ

Технологии, созданные опытными кибердетективами

Стек уникальных технологий, нацеленных на автоматизированный трекинг атак и вредоносной активности, извлечение и анализ данных об угрозах, отслеживание инфраструктуры атакующих и обогащение их профайлов.

Высокопрофессиональная команда

Эксперты Group-IB, постоянно участвующие в реагировании и расследовании сложных кибератак, непрерывно обогащают наши решения актуальными сведениями о самых современных тактиках и инструментах злоумышленников.



Фокус на атакующих

Анализируя угрозы более 15 лет, мы аккумулировали уникальную экспертизу и разработали специализированные технологии для распознавания паттернов, характерных для атакующих.

Наши решения позволяют не только выявить атаку на ранней стадии, но и помогают понять цели и методы злоумышленников, отслеживать изменения в их тактике и инфраструктуре.

Уникальная экспертиза

Эксперты Group-IB проводили тренинги профессионального развития для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд безопасности и преподавателей университетов в Великобритании, Германии, Нидерландах, Бельгии, Франции, Тайланде, Бахрейне и Ливане.

Усильте экспертизу своей команды с GIB Cyber School
group-ib.ru/cyberschool

Узнайте больше о Group-IB

group-ib.ru

Свяжитесь с нами

+7 (495) 984 33 64

info@group-ib.ru

Будьте в курсе новостей

facebook.com/GroupIB

twitter.com/GroupIB

youtube.com/GroupIB

instagram.com/Group_IB