HI-TECH CRIME TRENDS 2017

group-ib.ru

HI-TECH CRIME TRENDS 2017

Содержание

Ключевые выводы

Вымогатели

- Как мы и предсказывали в **отчете 2016 года**, вирусы-шифровальщики продолжили свое триумфальное шествие по миру: использование хакерами инструментов из утечек АНБ и функционала самораспространения в корпоративных сетях привело к глобальным эпидемиям. Самые масштабные из них — **WannaCry** и **NotPetya**.
- Программы-вымогатели, шифрующие данные, стали использоваться для маскировки следов атаки и отвлечения внимания от основного инцидента как традиционной киберпреступностью, так и хакерами, финансируемыми государствами.
- Программы-вымогатели для персональных компьютеров и мобильных устройств не претерпели серьезных изменений.

Программы-вымогатели, шифрующие данные, стали использоваться для маскировки следов атаки и отвлечения внимания от основного инцидента

Атаки на критическую инфраструктуру с целью шпионажа или диверсий

- Геополитические разногласия между США и Северной Кореей, Индией и Китаем, Пакистаном и Индией, Россией и Украиной сопровождает повышенная кибершпионская и диверсионная активность. Мы фиксируем, что атак стало не просто больше, но и качественно изменились цели атакующих.
- В некоторых странах банковская система считается объектом критической инфраструктуры. Хакеры, финансируемые государствами, провели несколько успешных атак на банковский сектор как для сбора разведывательных данных, так и для нарушения работоспособности атакуемых банков. Например, на Украине атаки с целью уничтожения данных в банках с начала этого года предпринимались группой **BlackEnergy** дважды. А целью северокорейской группы **Lazarus** являются крупнейшие международные банки, а также Центральные банки в разных странах мира.
- Преступная группа **BlackEnergy** продолжает атаки на финансовые и энергетические компании. Оказавшиеся в их распоряжении инструменты позволяют удаленно управлять Remote terminal unit (RTU), которые отвечают за физическое размыкание/замыкание энергосети. А летом 2017 года были зафиксированы тестовые атаки на энергокомпании Великобритании и Ирландии.

Оказавшиеся в распоряжении у Black Energy инструменты позволяют удаленно управлять Remote terminal unit (RTU), которые отвечают за физическое размыкание/замыкание энергосети.

- Атака **NotPetya**, запущенная в июне 2017 года, привела к нарушению остановки процессов в компаниях нефтегазового, финансового секторов. Временно остановились производства на некоторых предприятиях.
- После победы Дональда Трампа на президентских выборах в США активно обсуждается возможность влияния хакеров на результаты выборных процессов. Атаки на отдельных политиков и государственные

учреждения, шпионаж и сбор секретных или компрометирующих материалов существовали всегда, но теперь эти атаки связывают с возможной попыткой влияния на выборы и другие политические процессы. Эти инциденты подтолкнули специалистов по безопасности к инициированию более тщательных проверок систем и технологий, обеспечивающих чистоту и безопасность проведения выборов.

Целенаправленные атаки на банки и платежные системы

- **Все преступные группы, атаковавшие российские банки, постепенно переключили свое внимание на другие страны и регионы:** США, Европа, Латинская Америка, Азия и Ближний Восток. Впрочем, атаки на финансовые учреждения в России все еще случаются.
- **MoneyTaker**, русскоговорящая преступная группа, специализирующаяся на целевых атаках на финансовые организации по всему миру, сосредоточила свои усилия на небольших северо-американских банках. Один из банков они ограбили дважды.
- Преступная группа **Cobalt** — самая агрессивная и активная группа. Она атакует различные цели — банки, платежные системы, IT-компании, постоянно меняя локации. После серии международных атак они на какое-то время сосредоточились на странах СНГ, но позже опять продолжили свои атаки без явного фокуса на конкретном регионе.
- У преступных групп — **MoneyTaker** и **Cobalt** — в этом году основной целью стали банкоматы и карточный процессинг. В ходе атак взломщики получали доступ к компьютерам, подключенным к SWIFT, но мы не зафиксировали ни одной попытки похитить деньги через систему межбанковского перевода.
- **Одна из преступных групп создала систему автоматизированных хищений через систему межбанковских переводов АРМ КБР (аналог SWIFT), но смогла воспользоваться ей в России всего единожды.**
- Основным инструментом для захвата контроля над корпоративной сетью являются легитимные инструменты для проведения тестов на проникновения: Metasploit и Cobalt Strike.
- Бестелесность и вредоносные скрипты — новый (и теперь уже основной) принцип проведения атак. Хакеры стараются оставаться незамеченными и для этого используют «бестелесные» программы, которые работают только в оперативной памяти и уничтожаются после перезагрузки. Кроме того, скрипты на PowerShell, VBS, PHP помогают им обеспечивать персистентность (закрепление) в системе, а также автоматизировать некоторые этапы атаки.

> Бестелесность и вредоносные скрипты — новый (и теперь уже основной) принцип проведения атак. Это позволяет дольше оставаться незамеченным и помогает автоматизировать некоторые этапы атаки

- Во всех атаках злоумышленники использовали скрытые каналы связи. И зачастую они применяют легитимные средства для установки таких скрытых каналов, например, Plink или AmmyAdmin и т.п.
- **DNS-протокол стали чаще использовать для управления вредоносными программами, а также доставки полезной нагрузки, что позволяет обходить многие средства анализа сетевого трафика.**
- Еще одной новой целью для хакеров, причастных к целенаправленным атакам, стал процессинг производителей терминалов самообслуживания. Злоумышленники получают доступ к процессингам терминалов так же, как и к банкоматам, карточному процессингу, SWIFT , но система отмывания денег используется другая.

- Фокусировка атак на банкоматах и карточном процессинге привела к уменьшению среднего ущерба от одной атаки, однако позволяет атакующим проводить атаки более безопасно для «дропов», обналичивающих украденные деньги. Атакующие находятся в одной стране, их жертва (банк) в другой, а обналичка происходит в третьей.
- Основным вектором первоначального проникновения в сети финансовых учреждений остается почтовый фишинг.
- Несмотря на то, что в некоторых банках используются надежные средства защиты от почтового фишинга, некоторые сотрудники проверяют личную почту на своих рабочих местах. **Личная почта не защищена корпоративными средствами защиты. Этим пользуются злоумышленники. Поэтому для атак на некоторые банки они собирали личные адреса электронной личной почты сотрудников, чтобы в рабочие часы отправлять им письма с вредоносными вложениями.**
- Новым способом уничтожения следов после целенаправленной атаки на банки стало использование программ-вымогателей, шифрующих данные на диске.

Атаки на клиентов банков

- Количество групп и, как следствие, количество атак на юридических лиц в России с целью хищения денег уменьшилось практически в два раза по сравнению с прошлым периодом. Однако средний размер ущерба увеличился, что свидетельствует о том, что хакеры стали более тщательно подбирать своих жертв.
- С рынка ушли трояны **Corebot** и **Vawtrak** (aka Neverquest), причастные к атакам на юридических лиц по всему миру. В случае с **Corebot** автор просто прекратил его поддержку. А в случае с Vawtrak автор был задержан, что привело к остановке его активности.
- **Каждый месяц русскоговорящие хакеры создают 1-2 новую вредоносную программу для хищений денег. Для персональных компьютеров было зафиксировано 6 новых троянов. Самый известный – TrickBot**. Для Android появилось 12 новых банковских троянов, и среди новичков нет явного лидера. Для POS-терминалов появилось 3 новых трояна, и, конечно же, никуда не делись старые, которые усовершенствовали свой функционал и продолжают активно работать.

> Из 22 новых вредоносных программ для хищений денежных средств 20 (91%) созданы и управляются людьми, говорящими на русском языке.

- **В начале года в Германии прошли первые хищения с банковских счетов, когда для обхода двухфакторной аутентификации СМС-код был перехвачен путем атаки на ОКС7 (SS7).**
- В России владельцы банковских бот-сетей, нацеленных на юридических лиц, полностью отказались от атак «Человек-В-Браузере» и используют либо удаленное управление, либо автоматические переводы через системы бухгалтерского учета 1С.
- Некоторые киберпреступники отказываются от веб-инжектов в пользу перенаправления трафика на серверы атакующего с целью перехвата и манипуляции данными в трафике.
- Владельцы трояна **Buhtrap** передали управление своей бот-сетью новым владельцам. После этого тактика атакующих изменилась: основным вектором распространения троянов стал не спам, а взломанные популярные сайты, в том числе, финансовой и юридической тематики.
- **Ущерб от банковских троянов под Android в России вырос на 136% и перекрыл ущерб от троянов для персональных компьютеров на 30%.**

- Банковские Android-трояны по-прежнему атакуют физических лиц. Атаки на юридических лиц не зафиксированы.

> Владельцы Android бот-сетей начали использовать Apple Pay для хищений денег с банковских счетов.

- **Фишинг под банки и платежные системы в России автоматизирован и проходит в реальном времени, что позволяет обходить СМС-подтверждения на списание денег.** Ежедневно жертвами финансового фишинга в России становится более 900 клиентов банков, что в три раза превышает ежедневное количество жертв от вредоносных программ. Однако сумма ущерба от фишинга в десятки раз меньше, чем от вредоносных программ.
- В среднем, 10-15% посетителей финансовых фишинговых сайтов вводят свои данные.
- В 80% случаев фишеры регистрируют почту для сбора скомпрометированных данных в Gmail. На российские поисковики Yandex и Mail.ru приходится лишь 6%.

Атаки на криптовалютные сервисы

- Ажиотаж вокруг криптовалют, блокчейна и ICO, сравнимый с временами золотой лихорадки, вызвал повышенное внимание со стороны киберпреступников. В 2017 году произошла целая серия успешных атак на криптовалютные сервисы и их пользователей.
- **Взломы криптовалютных бирж проводятся по той же схеме, что и целенаправленные атаки на банки — используются схожие, а иногда и идентичные инструменты, а также схожие тактики.**
- Участились случаи, когда мошенники создают фишинговые сайты, копирующие контент сайтов компаний, выходящих на ICO. На таких сайтах пользователи указывают секретный ключ своего кошелька, и деньги автоматически похищают.
- Стартапы, выходящие на ICO, уделяют недостаточно внимания безопасности своих веб-сайтов. В этом случае атакующие, получая доступ к таким сайтам, заменяют адрес кошелька на фейковый и собирают деньги, переводимые в рамках ICO.
- Мы фиксируем рост количества инцидентов, связанных с воровством у пользователей данных криптокошельков с помощью вредоносных программ и вывода денег. Методы идентичны тем, что используются для атак на пользователей банковских приложений.
- Кроме вредоносных программ активно используется компрометация адресов электронной почты, а также получение SIM-карты по поддельным документам для восстановления паролей и получения контроля над счетом в криптовалютных сервисах.
- Трояны-майнеры уже давно используются киберпреступниками. Однако майнинг на взломанных компьютерах или серверах с каждым годом дает все меньший результат из-за крупной эмиссии. Поэтому атакующие начинают использовать их для майнинга новых криптовалют.

> Злоумышленники получают SIM-карты по поддельным документам для восстановления паролей и получения контроля над счетом в криптовалютных сервисах

Развитие хакерского инструментария

- Многие преступные группы и хакеры, финансируемые государствами, пополнили свои

арсеналы благодаря утечкам из спецслужб США. Группа **The Shadow Brokers** публикует (и продает по подписке) инструменты из NSA, а проект WikiLeaks выкладывает секретную информацию из CIA. Опубликованные данные и готовые инструменты сразу применялись во вредоносных программах и встраивались в инструменты для проведения тестов на проникновение во всем мире.

- Многие разработчики вредоносного кода стали более активно выкладывать в открытый доступ исходные коды своих программ. В этот период были выложены исходные коды банковского трояна под персональные компьютеры **TinyNuke**, банковского Android-трояна **Maza-in**, **RATAttack**, использующий защищенный канал мессенджера Telegram, DDoS-трояна **Mirai**, а также различные программы-шифровальщики.

Многие разработчики вредоносного кода стали более активно выкладывать в открытый доступ исходные коды своих программ

- В прошлом году стало очевидно, что атакующих интересуют не только компьютеры и мобильные устройства, но и IoT и роутеры. **В этом году появились трояны под Android, а также ExploitKit, основной целью которых стало получение доступа к роутерам в локальной сети и манипуляция пользовательским трафиком.** Чуть позже выяснилось, что CIA использовала инструмент Cherry Blossom с той же целью.
- Исследование таких Android-троянов, как **CopyCat**, **Gooligan**, **DressCode**, показало, что самые большие бот-сети находятся в Азии и предназначены для показа рекламы.

Прогнозы

Инструменты и атаки на критические инфраструктуры

- Атаки **WannaCry** и **NotPetya**, организованные, предположительно, хакерами, финансируемые государствами, показали всему миру, насколько легко сделать эффективный самораспространяемый в корпоративной сети шифровальщик. Ни одна из группировок, ориентированных на кражу денег, еще не проводила атаки таким образом. Масштаб бедствия, скорость заражения и ущерб, нанесенный жертвам, наверняка приведут к появлению подражателей и новым атакам со стороны традиционной киберпреступности — финансово мотивированных хакеров. Изменив вектор первичного попадания в сеть, они могут нанести значительно больший ущерб.
- История с **NotPetya** продемонстрировала, что для захвата контроля над корпоративной сетью достаточно создать шаблон — заскриптовать несколько простых шагов. **В будущем стоит ожидать большого количества заскриптованных атак, а также готовых простых инструментов, которые будут автоматически получать контроль над корпоративным доменом.** Появление таких инструментов в открытом доступе или в продаже среди хакеров может привести к лавинообразному росту самых разных атак на корпоративный сектор. В первую очередь мы ожидаем роста инцидентов с шифровальщиками, кражей конфиденциальной информации и вымогательства за неразглашение, хищений денежных средств, публичных разоблачений, проводимых не финансово мотивированными атакующими.
- Из-за увеличения активности прогосударственных хакеров и повышенного внимания к тематике кибератак уже в ближайшее время появится больше последователей The Shadow Brokers, и инсайдеров, помогающих WikiLeaks

В ближайшее время появится больше последователей The Shadow Brokers, и инсайдеров, помогающих WikiLeaks

- **Мы ожидаем, что авторы вредоносных программ продолжат более активно выкладывать исходные коды своих программ.** Кроме того, утечки, публикуемые The Shadow Brokers и их возможными последователями, также будут немедленно применяться на практике для создания и усовершенствования вредоносных программ. Это даст мощный толчок к развитию индустрии кибернападения.
- Объектами атак вымогателей станут, прежде всего, те страны, где предусмотрены значительные штрафы за утечку конфиденциальной информации.

Целевые атаки на банки

- **Если раньше финансовые учреждения опасались взломщиков-грабителей, то теперь новой и более серьезной для них угрозой могут стать хакеры, финансируемые различными государствами.** Их целью станет слежка за финансовыми потоками, сбор компромата на интересующих их клиентов банков, а также нарушение работоспособности внутренней инфраструктуры. Последнее особенно актуально для стран, выдвигающих взаимные обвинения о нападении в киберпространстве — диверсии могут использоваться как ответная мера.

Главной опасностью для банков станет не воровство денег, а разрушение их ИТ-инфраструктуры как финальный этап целенаправленной хакерской атаки.

- Одним из возможных сценариев диверсии могут быть торги на биржах от имени банка с целью влияния на курсы валют. Это может привести к запуску лавинообразных операций, совершаемых торговыми роботами после резких колебаний валютных курсов.
- У финансово мотивированных хакеров основной целью останется карточный процессинг, поскольку он является наиболее безопасным для атакующих, а схемы обнала достаточно просты.
- Поскольку атаки на карточный процессинг являются безопасными для людей, занимающихся хищением и обналичиванием средств (схемы просты в реализации и не требует от атакующих надежных контактов в сфере отмывания денег, как, например, при атаках на SWIFT), то этот тренд открывает дорогу менее опытным атакующим. Поэтому в следующем году мы можем увидеть атаки, совершенные новыми группами.
- **Особое внимание банкам надо обратить на точки подключения доверенных партнеров, поскольку именно партнеры могут стать новым основным вектором проникновения в банковские инфраструктуры.**
- Автор банковского трояна **Vawtrak** (aka Neverquest), используемого для атак на компании в разных странах, был задержан правоохранительными органами. Однако его высоко профессиональная команда с опытом крупных хищений и доступом к надежным схемам отмывания денег осталась на свободе. Мы ожидаем, что они начнут проводить целенаправленные атаки уже на сами банки, а не только на их клиентов.

Целевые атаки с целью хищений денег

- **Если авторы банковских и POS-троянов для персональных компьютеров добавят функцию самораспространения в корпоративной сети к автоматическому поиску компьютеров, где осуществляется работа с интернет-банкингом, это вызовет значительный рост успешных атак как на корпоративные банковские счета, так и на частные, поскольку пользователи в корпоративных сетях также активно используют интернет-банкинг.**
- В случае широкого распространения мобильного банкинга в корпоративном секторе Android-трояны начнут атаковать пользователей таких приложений. При этом метод распространения троянов останется прежним.
- **Ущерб от хищений с помощью банковских Android-троянов в России уже превысил ущерб от банковских троянов для персональных компьютеров. Мы ожидаем, что аналогичная ситуация будет и в других странах, где высоко проникновение мобильных банковских услуг.**
- С целью снижения своих издержек и повышения эффективности хакеры продолжат отказываться от веб-инжектов в пользу перенаправления трафика на серверы атакующего с целью перехвата и манипуляцией данными в трафике. Это может привести к созданию отдельных сервисов, предоставляющих услуги по автоматизации процессов манипуляции данными в трафике.
- Продажа трафика с роутеров может создать новую услугу, которая позволит значительно увеличить количество фишинговых атак. Пользователей будут просто перенаправлять на фишинговые страницы в определенные периоды времени. При этом особую популярность приобретут те сервисы, которые предложат более качественную аудиторию.

Атаки на криптовалютные сервисы

> Продажа трафика с роутеров может создать новую услугу, которая позволит значительно увеличить количество фишинговых атак.

- **Android-трояны позволят хакерам гораздо эффективнее атаковать пользователей криптовалют.** Методы идентификации владельцев криптокошельков, получения к ним доступа будут идентичны методам, которые используются в атаках на банковские счета. Скорее всего, будут адаптированы текущие банковские Android-трояны.
- Кроме Android-троянов для атак на пользователей криптовалют будут активно использоваться трояны для персональных компьютеров. При этом чаще будут использоваться не специализированные банковские трояны, а трояны общего назначения, в том числе те, что находятся в открытом доступе.
- Фишинг под криптовалютные сервисы станет основной проблемой для их пользователей. Постоянные успешные атаки будут негативно влиять на доверие к отдельно взятым сервисам до тех пор, пока они не повысят свою безопасность и не начнут активную борьбу с фишингом.

> Из-за более простой схемы отмыва денег некоторые группы, специализирующиеся на целенаправленных атаках на банки и платежные системы, переключат свое внимание на биржи криптовалют.

- **Целенаправленные атаки на биржи криптовалют будут проводиться не только традиционной киберпреступностью, но и хакерами, финансируемыми государством.**
- Все, что связано с криптовалютой, станет основной целью хакеров, специализирующихся на веб-атаках. Их основным мотиватором будет продажа трафика с таких сайтов, поскольку на него будет высокий спрос у хакеров, управляющих Android, PC-троянами, а скомпрометированные контакты пользователей будут активно использоваться при проведении целенаправленных атак, фишинге, вишинге и в том числе брутфорсе.
- Финансовый сектор уже давно является целью №1 для проведения атак, сопряженных с вымогательством. Первое время будет расти число попыток получить деньги с владельцев криптовалютных сервисов как за счет хакеров, представляющих реальную угрозу, так и за счет подражателей, которые не способны проводить сложные атаки.
- Скачки курса Bitcoin, ажиотаж вокруг новых криптовалют и ICO значительно повышает интерес к этой теме со стороны населения. Появится все больше желающих инвестировать в криптовалютные сервисы. Это приведет к тому, что многие мошенники вернутся к старым схемам, связанным с «инвестициями», «управлением активами», «гэмблингом» и т.д.

Оценка рынка высотехнологичных преступлений

Рост числа атак и сумм хищений является ярким индикатором финансовой активности киберпреступников, изменения их тактики и целей. Большая часть хакеров следует за деньгами. Если они находят новые, более высокооплачиваемые и безопасные способы заработка, то начинают инвестировать именно туда, создавая новые инструменты, услуги, схемы проведения атак.

Тренд снижения ущерба от хищений у юридических лиц в России сохраняется, а ущерб от банковских троянов под ОС Android продолжает расти. Количество целевых атак на банки и платежные системы растет, но основной доход атакующие получили за пределами России, как мы и предсказывали в прошлом году.

После полной автоматизации фишинговых атак на клиентов банков и платежных систем ущерб от их активности в России стал очень заметным. Ежедневно они атакуют гораздо больше пользователей, чем банковские трояны, но ущерб при этом по-прежнему меньше. Однако из-за простоты схемы ее начинают использовать все большее количество преступников.

Сегмент рынка в России и СНГ	Кол-во групп	Общее число успешных атак в день	Средняя сумма одного хищения	Сколько воруют в день	H2 2016 — H1 2017		H2 2015 — H1 2016		Процент роста к прошлому периоду
					в RUB	в USD	в RUB	в USD	
Хищения в интернет-банкинге у юридических лиц с использование вредоносных программ	3	2	1 250 000 ₽	2 500 000 ₽	622 500 000 ₽	$10 375 000	956 160 000 ₽	16 774 737 $	-35%
Хищения в интернет-банкинге у физических лиц с использование вредоносных программ	1	1	63 000 ₽	63 000 ₽	15 687 000 ₽	$261 450	6 424 200 ₽	112 705 $	144%
Хищения у физических лиц с Andoird-троянами	10	300	11 000 ₽	3 300 000 ₽	821 700 000 ₽	$13 695 000	348 600 000 ₽	6 115 789 $	136%
Целевые атаки на банки	2	—	—	—	1 630 000 000 ₽	$27 166 667	2 500 000 000 ₽	43 859 649 $	-35%
Фишинг	15	950	1 000 ₽	950 000 ₽	236 550 000 ₽	$3 942 500	—	—	—
Обналичивание похищаемых средств	—	—	—	2 638 350 ₽	1 390 449 150 ₽	$23 174 153	1 715 032 890 ₽	30 088 296 $	-19%
Итого				**6 813 000 ₽**	**4 716 886 150 ₽**	**$78 614 769**	**5 526 217 090 ₽**	**96 951 177 $**	**-15%**

Основные тенденции и факты 2016 H2 — 2017 H1

Вымогатели

Вымогатели обзавелись функционалом самораспространения

В прошлом году мы предсказывали, что трояны-шифровальщики получат функции самораспространения в локальной сети и будут использоваться для целевых заражений крупных компаний и для получения выкупа за возможность восстановить доступ к файлам. Это позволило бы злоумышленникам увеличить суммы выкупа и повысить вероятность его получения. Однако на эту возможность обратили внимание не киберпреступники, а хакеры, финансируемые государством.

14 апреля 2017 года хакерской группой **The Shadow Brokers** были опубликованы сведения об уязвимости и исполняемый код эксплойта **EternalBlue**, эксплуатирующий уязвимость в протоколе Server Message Block v1 (SMB).

12 мая 2017 года появился шифровальщик **WannaCry**, а 27 июня 2017 года началось массовое распространение шифровальщика **NotPetya**.

Специалисты связали атаку **WannaCry** с **Lazarus**, группой государственных хакеров из Северной Кореи, а атак **NotPetya** — с **Black Energy**, группой хакеров, финансируемых государством.

Очевидно, что и в первом, и втором случае целью атаки было не получение финансовой выгоды, хотя требование заплатить демонстрировались в обоих случаях.

Ущерб от прогосударственных «вымогателей»

Установить, откуда началось распространение **WannaCry**, не удалось. Учитывая, что атакующими являются хакеры, спонсируемые государством, то, скорее всего, целью атаки были конкретные объекты, чью работоспособность было необходимо нарушить. Все остальные жертвы стали случайными. Пострадали только те компании, у которых необновлённые версии операционных систем были подключены напрямую к интернету.

В случае с **NotPetya** атака была более целенаправленной. Ее объектом стали только компании, использующие программное обеспечение украинского разработчика системы документооборота «M.E.Doc».

В обоих случаях достаточно было изменить вектор начального проникновения, и жертв в нужном сегменте было бы гораздо больше.

Сокрытие следов

Другим прогнозом было использование шифровальщиков для сокрытия целенаправленных атак. В начале 2017 года мы зафиксировали первые случаи использования шифровальщиков для маскировки следов ограбления банка. В ходе атаки на банк с целью его ограбления хакеры получили контроль над доменом. После совершения хищения они запустили модифицированную версию шифровальщика **Petya** от имени администратора домена на всех компьютерах в сети. В результате большая часть компьютеров в сети вышла из строя, что сильно затруднило проведение расследование этой атаки.

Вымогатели под ПК и Android

Хакеры, использующие программы-вымогатели, все больше внимания уделяют именно

корпоративному сектору. Новых методов атак или уникальных инструментов, используемых финансово мотивированными хакерами, не обнаружено. Наиболее активными шифровальщиками стали **Locky** и **Cerber**. Обе вредоносные программы распространяются по партнерской программе русскоговорящими атакующими. Основным вектором распространения остается СПАМ-рассылка, однако некоторые использовали и связки эксплойтов для доставки шифровальщиков на уязвимые компьютеры.

Программы-вымогатели для мобильных устройств заметно снизили свою активность. На русскоговорящих форумах за последний год не появилось ни одного нового предложения о покупке таких программ.

Прогнозы с атаками вымогателей для IoT не оправдались, и пока нет индикаторов, указывающих на то, что хакеры готовятся реализовать это в следующем году. Атаковать корпоративный сектор все еще выгодно, а добавление возможности самораспространения шифровальщиков в локальной сети открывает хорошие перспективы для инвестирования своих сил именно в этом направлении. Вот почему мы считаем, что наибольший ущерб стоит ожидать именно от шифровальщиков с функцией самораспространения. В отличие от атак **WannaCry** и **NotPetya** они будут более точечными.

NotPetya показал, что для захвата контроля над корпоративной сетью достаточно заскриптовать несколько простых шагов. В будущем стоит ожидать большого количества заскриптованных атак, а также готовых простых инструментов, которые будут автоматически получать контроль над корпоративным доменом. Появление таких инструментов в открытом доступе или в продаже среди хакеров может привести к лавинообразному росту самых разных атак на корпоративный сектор. В первую очередь мы ожидаем рост инцидентов с шифровальщиками, кражей конфиденциальной информации и вымогательства за неразглашение. И таких атак стоит ждать, прежде всего, в странах, где предусмотрены высокие штрафы за несоблюдение мер безопасности, утечку данных или нарушение доступности предоставляемых сервисов. Особенно это касается банковского сектора, страховых компаний и медицинских учреждений.

Атаки на объекты критической инфраструктуры

Развитие

Новости об атаках на промышленные предприятия, обнаружении уязвимостей и получение удаленного доступа к различным терминалам управления Industrial Control Systems (ICS) в последнее время появляются все чаще. Но для проведения успешной атаки, которая может привести к реальным сбоям в работе ICS, необходимо больше, чем просто удаленный доступ и пароли некоторых пользователей. Нужно понимать, как работают физические процессы в ICS, чтобы иметь возможность влиять на них и, что самое главное, закладывать логику работы для влияния на эти физические процессы в инструменты атакующего.

Первой вредоносной программой, которая реально смогла повлиять на физические процессы и привести к выводу из строя оборудования, был вирус **Stuxnet**, используемый Equation Group (Five Eyes/Tilded Team). Основная особенность **Stuxnet** — это возможность разрушительного влияния на оборудование Siemens, которое использовалось для управления скоростью вращения центрифуг для обогащения урана на заводе в Иране. Атаковав оборудование Siemens, **Stuxnet** незаметно изменял скорость центрифуг, что и привело к их уничтожению. Это было в 2010 году, и от этого времени принято вести отсчет новой эры использования кибероружия. После этой атаки несколько лет наблюдалось затишье. Оказалось, что все это время хакеры искали возможность влиять на ICS и выводить их из строя, когда это будет необходимо. Дальше других в этом направлении продви-

нулась группа **Black Energy**, также известная как **Sandworm**.

Много шума было вокруг выявленной в 2014 году кампании Energetic Bear (Dragonfly/ Crouching Yeti) по воздействию на энергетические компании с помощью инструмента Havex, который, предположительно, был установлен более чем в 2 000 сетях. Но Havex не мог влиять на физические процессы. Это был этап разведки. Его основной целью был сбор информации об используемом оборудовании в этих энергетических компаниях, и для сбора этой информации он «прослушивал» OPC-протокол (Open Platform Communications), используемый для управления объектами автоматизации и технологическими процессами. Или, проще говоря, анализировал взаимодействие SCADA с «железом» и понимал, какое оборудование стоит в конкретной локации. Это важнейший процесс для будущих атак.

Еще одним важным этапом в подготовке было получение доступа к SCADA Human machine interfaces (HMIs). Вредоносная программа Black Energy 2, используемая одноименной группой (или Sandworm) была нацелена на HMI трех вендров: General Electric's Cimplicity HMI, Siemens' SIMATIC WinCC и BroadWin's WebAccess. Используя уязвимости в этих продуктах, Black Energy 2 устанавливался на их серверы.

В декабре 2015 года случилось вторая после Stuxnet атака на объект критической инфраструктуры, в результате которой был нанесен реальный ущерб. Для атаки использовалась вредоносная программа Black Energy 3. С ее помощью в трех энергетических компаниях Украины атакующие вызвали перегрузку сети, заменили на подстанциях прошивку некоторых Serial-to-Ethernet устройств, что сделало их неработоспособными. Затем, используя удаленный доступ, атакующие отключили источники бесперебойного питания и, используя простую утилиту KillDisk, вывели из строя компьютеры под управлением Windows в сети энергетической компании, в том числе компьютеры с HMI.

Результат эволюции

В декабре 2016 года была совершена атака на одну из украинских подстанций, которая привела к отключению электроэнергии на 75 минут. Эта малозаметная тестовая атака показала, на что способен новый набор инструментов группы **Black Energy**, который получил название Industroyer, или CRASHOVERRIDE, описанный компанией Eset.

Industroyer — это полноценный фреймворк для атак на ICS. Используя накопленный опыт и инвестиции в разработку, атакующие автоматизировали многие процессы.

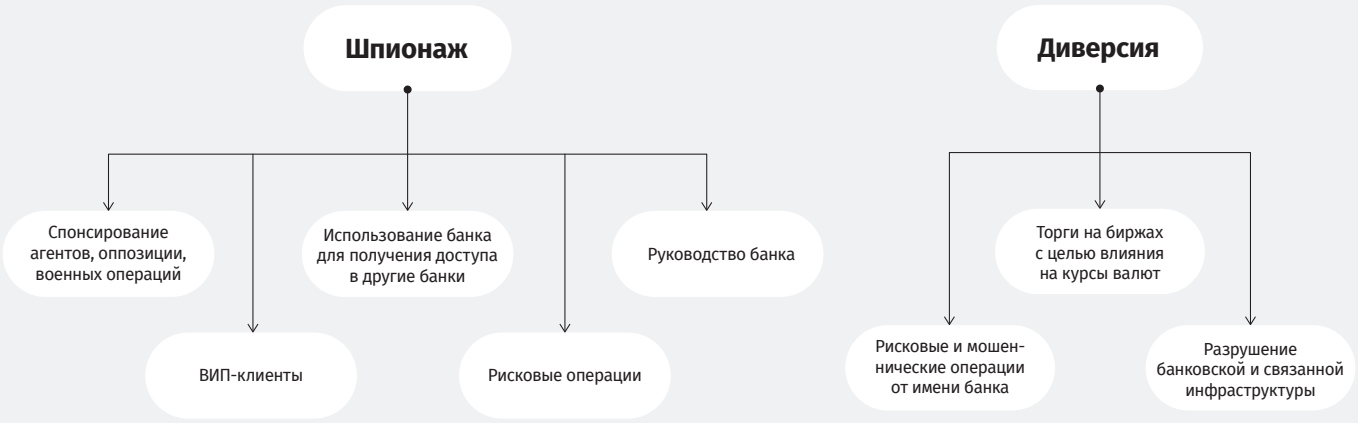
Как и в Havex, они используют OPC-протокол для построения карты сети индустриальных устройств.

Как и в Black Energy 2, они атаковали библиотеки и конфигурационные файлы HMI, чтобы лучше понимать окружение и иметь возможность подключаться к другим локациям энергетической сети.

Как и в случае атаки с помощью Black Energy 3, они научились вызывать перегрузку энергетической сети и выводить некоторые элементы из строя, чтобы усложнить процедуру реагирования и восстановления электроэнергии.

Но кроме этого, у них появились новые модули для работы с протоколами IEC 60870-5-101, IEC 60870-5-104, IEC 61850. Эти протоколы используются для удаленного управления Remote terminal unit (RTU), которые отвечают за физическое размыкание/замыкание сети. Примечательно, что такие элементы используются не только в энергетических компаниях, но и в других сферах городского хозяйства — водоснабжении, газовых сетях.

Еще одно дополнение — модуль для эксплуатации старой уязвимости CVE-2015-5374 в оборудовании Siemens SIPROTEC, которая вызывает отказ в обслуживании и делает устройство недоступным.



Что еще нового у Black Energy

Black Energy известна своими атаками на энергетические компании. Однако начиная с этого года группа была замечена в атаках на банковскую инфраструктуру.

Кроме основной вредоносной программы Black Energy они применяют новый бэкдор, использующий защищенный протокол Telegram. При этом существует две реализации, одна на языке Rust, другая на Python.

Ранее они использовали уникальную утилиту KillDisk, теперь для уничтожения написали своего шифровальщика файлов на компьютерах и серверах в сети банка. Шифровальщик определяется как «Win32/Filecoder.NKH» и шифрует файлы с помощью алгоритма RSA-1024 и AES, добавляя к файлам расширение .xcrypted.

В июне они запустили атаку с помощью **NotPetya**. И уникальный шифровальщик, и **NotPetya** использовались для вывода из строя локальной сети коммерческих организаций.

Целенаправленные атаки на банки и платежные системы

Хакеры, финансируемые государством, — новая угроза для банков.

В некоторых странах банковская система признана объектом критической инфраструктуры. Хакеры, стоящие на службе или финансируемые государствами, провели несколько успешных атак на банковский сектор как с целью сбора разведывательных данных, так и с целью нарушения работоспособности атакуемых банков.

Equation Group (США)

15 апреля хакеры из **The Shadow Brokers** выложили новый дамп из набора инструментов хакеров из **Equation Group**, предположительно работающих на АНБ. Согласно выложенным документам, они атаковали два SWIFT Service Bureaus, чтобы получить доступ к данным о банковских операциях ряда финансовых институтов Ближнего Востока и Латинской Америки.

SWIFT Service Bureaus — это сторонние сервис-провайдеры, организующие и размещающие соединения со SWIFTNet финансовых организаций, которые хотят иметь возможность подключения к этой сети, но предпочитают отдавать такие операции на аутсорсинг. По свидетельству SWIFT, подобный пакет услуг включает разделение, размещение и эксплуатацию компонентов для связи со SWIFT, а также обеспечение механизмов входа в систему, управление сеансами связи и гарантирование безопасности пользователям SWIFT.

Архивы, связанные со SWIFT, именуются JEEPFLEA и содержат учетные данные и детали архитектуры EastNets, крупнейшего сервисного бюро SWIFT на Ближнем Востоке.

Вторым сервисным бюро, предположительно, является Business Computer Group (BCG) в Панаме.

Поскольку банковские транзакции заносятся в базу данных Oracle, использующую софт SWIFT, в опубликованных архивах содержатся описания инструментов, которые помогали АНБ получать данные из этой базы, в том числе список пользователей и запросы в форме SWIFT-сообщений.

Архивные документы, добытые и опубликованные **Shadow Brokers**, содержат идентификаторы, информацию об учетных записях и данные административных аккаунтов.

Lazarus (Северная Корея)

В феврале 2016 года стало известно о попытке хищения $1 миллиарда из Центрального Банка Бангладеш. Анализируя код вредоносных программ, специалисты по безопасности нашли схожие фрагменты кода, которые ранее уже встречался в других атаках. На основании схожести кода и аналогичной схемы развертки систем на зараженных компьютерах специалисты сошлись во мнении, что за этой атакой стоит группа **Lazarus**.

Уже в феврале 2017 года стало известно о компрометации нескольких банков в Польше. Расследование показало, каким образом злоумышленники попали в сеть банков и какие вредоносные программы использовали, а также были выявлены некоторые другие регионы, веб-ресурсы которых стали объектом атаки. Анализируя код вредоносных программ, специалисты снова связали эти атаки с группой **Lazarus**. Целью группы **Lazarus** являются крупнейшие международные банки, а также Центральные Банки в разных странах мира. Но только в отличие от инцидента в Бангладеше целью атакующих были не деньги.

Лаборатория Касперского выпустила отчет о реагировании на инцидент, к которому причастна группа **Lazarus**. В ходе реагирования они нашли инструменты для работы со SWIFT. Одной из основных задач этих инструментов был сбор данных о транзакциях: Sender and Receiver, Account and Statement Numbers as well as some other data.

Кроме того, анализ активности этой группы показал, что они имели доступ в сети некоторых банков в течение нескольких месяцев, но ни один из этих банков не стал жертвой хищений.

BlackEnergy

Основной задачей группы **BlackEnergy** всегда являлось нарушение работоспособности атакуемых ими объектов, в том числе банков. Например, на Украине атаки с целью уничтожения данных в банках с начала этого года предпринимались дважды.

В конце 2016 года были зафиксированы целевые атаки на финансовые организации на Украине. На компьютер жертвы с помощью загрузчика, написанного на RUST, загружался бэкдор **TeleBot**, написанный на Python. **В период январь-февраль 2017 года преступной группе удалось скомпрометировать сеть крупного украинского IT-интегратора. Через него злоумышленникам удалось получить доступ к четырем украинским банкам и загрузить туда троян, схожий с TeleBot, однако написанный на языке Rust.**

После получения доступа они загружали Telegram бэкдор и самописный RAT. Затем они использовали **Mimikatz** для получения логина и пароля администратора, для доступа к другим машинам в сети. После получения доступа уровня администратора контроллера домена они использовали программу шифровальщик для зашифровки файлов на компьютерах и серверах в сети банка. Шифровальщик определяется как «Win32/Filecoder.NKH» и шифрует файлы с помощью алгоритма RSA-1024 и AES, добавляя к файлам расширение .xcrypted. Он шифрует все файлы, кроме директории «C:\Windows». После окончания шифрования Троян создает файл под названием «!readme.txt» со следующим содержанием «Please contact us: openy0urm1nd@protonmail.ch».

27 июня 2017 года мир узнал о массовой атаке с помощью программы-шифровальщика **NotPetya**. Жертвой этой атаки стали компаниии, использовавшие программное обеспечение для отчетности и документооборота украинского разработчика M.E.Doc.

Атакующие получили доступ к исходному коду M.E.Doc и серверу обновлений, который они использовали для распространения зараженного обновления с автоматической установкой. После запуска NotPetya происходило шифрование файлов, а троян начинал распространяться дальше по корпоративной сети с помощью Eternalblue-подобного эксплойта и легитимного инструмента удаленного управления PsExec.

Для получения полного контроля над корпоративной сетью часто и государственные, и финансово мотивированные хакеры действовали по простому сценарию, который мы описывали в прошлом отчете. Его можно разбить на **следующие этапы:**

1. Получение доступа к любому компьютеру в сети.
2. Получение логинов и паролей с первого зараженного компьютера.
3. Подключение с полученными логинами и паролями к соседним компьютерам и получение паролей с них, до тех пор, пока не найдут пароль администратора домена.

В атаке NotPetya хакеры просто заскриптовали эти три простых шага, и это привело к тому, что атака прошла успешно не только на компании, которые использовали M.E.Doc, но и на другие компании, подключенные к зараженным. Именно этот подход и открывает ящик Пандоры. В будущем стоит ожидать большого количества автоматизированных атак, а также готовых простых инструментов, которые будут автоматически получать контроль над корпоративным доменом. Появление таких инструментов в открытом доступе или в продаже среди хакеров может привести к лавинообразному росту самых разных атак на корпоративный сектор. В первую очередь мы ожидаем роста инцидентов с шифровальщиками, кражей конфиденциальной информации и вымогательства за неразглашение, хищений денежных средств, публичных разоблачений, проводимых не финансово мотивированными атакующими.

Финансово мотивированные хакеры

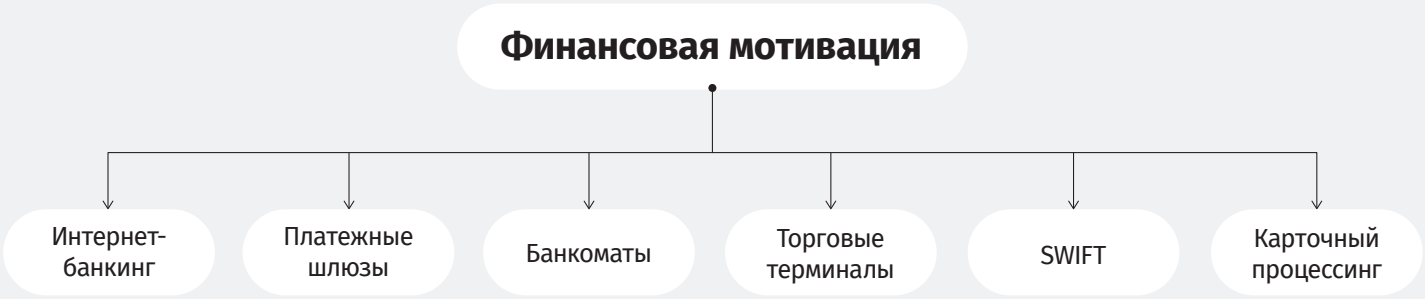
Финансово мотивированные хакеры, как и ожидалось, стали еще более активно атаковать финансовые учреждения в разных концах света. Независимо от атакуемого региона самым основным методом проникновения в сети банков остается фишинг.

Атакующие осознают, что в банках используются надежные средства защиты от почтового фишинга, но некоторые сотрудники все-таки проверяют на своих рабочих местах личную почту, которая не защищена корпоративными средствами защиты. Поэтому для атак на банки атакующие собирали личные адреса электронной почты сотрудников банков, чтобы отправлять им письма с вредоносными вложениями в рабочие часы.

Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и OffensiveWare Multi Exploit Builder (OMEB).

Группа **MoneyTaker** сосредоточила свои усилия на небольших северо-американских банках, один из банков они грабили дважды. Кроме Северной Америки группа активно атаковала банки и в других регионах, например, в России. Стоит отметить, что часть атак MoneyTaker на банки связывают с Anunak (aka Carbanak, FIN7 Navigator, Teleport Crew, Digital Plagiarist), но мы рассматриваем их как отдельную группу, тесно связанную с участниками группы **Anunak**.

Группа **Cobalt** атакует всех подряд, экспериментируя с разными регионами. На какое-то время они сосредоточились на странах СНГ, но позже опять продолжили свои атаки



без явного фокуса. Работая с ограбленными банками, а также с банками, на которые готовится атака с целью ограбления, мы сталкиваемся с тем, что основное внимание они уделяют безопасности SWIFT и банкоматов, поскольку об этих успешных атаках чаще сообщают СМИ. Но атакующих интересует более широкий спектр банковских систем, которые можно атаковать. Кроме банкоматов и SWIFT мы фиксировали атаки на карточный процессинг, платежные шлюзы и терминалы, терминалы для торговли на биржах. Только системы интернет-банкинга пока остались без внимания, хотя в прошлом их также часто атаковали и успешно похищали деньги.

Бестелесность и скрипты

Бестелесность и скрипты — новый, теперь основной принцип проведения атак. Хакеры стараются оставаться как можно незаметнее и для этого используют «бестелесные» программы, которые работают только в оперативной памяти и уничтожаются после перезагрузки. Кроме того, скрипты на PowerShell, VBS, PHP помогают им обеспечивать персистентность в системе, а также автоматизировать некоторые этапы атаки.

Бестелесность дает два основных преимущества:

- Их сложно обнаружить стандартными средствами антивирусной защиты.
- Отсутствие файлов на диске оставляет меньше следов вредоносной активности и очень сильно усложняет процесс реагирования на инцидент и проведения криминалистических исследований, что необходимо для будущего расследования. Если нет файла, вы не можете восстановить его атрибуты, понять, когда он появился в системе, что его запустило, какой у него функционал и т.п.

Скрипты также дают ряд преимуществ:

- Вредоносные скрипты также тяжело обнаружить средствами антивирусной защиты. Написать сигнатуру на скрипт без ложно положительных срабатываний гораздо сложнее, чем на бинарный файл.
- Скрипты легко модифицировать, что облегчает труд атакующих.
- Легко обеспечить персистентность (закрепление в системе). Обычно такие скрипты сохраняются в реестре или вызываются при наступлении определенных событий через Windows Management Instrumentation (WMI), Group Policy Objects (GPOs), Scheduled task. Такие скрипты очень просты, обычно их основная задача — загрузить основную программу из внешнего или локального источника и запустить ее.

Представьте ситуацию, что банк ограбили. И в ходе атаки на одном из компьютеров в Scheduled task осталась задача на выполнение скрипта, который просто загружает файл из легитимного облачного хранилища и запускает его. Найти такую задачу без правильного реагирования крайне сложно, поэтому мы даже сталкивались с ситуацией, когда один банк грабили дважды.

Цель — банкоматы

В июле 2016 года злоумышленники провели серию успешных атак на банкоматы банка Тайваня (First Bank). Атака прошла в нескольких городах, и в результате атакующим удалось похитить 2,18 млн. долларов. Были задержаны люди, занимавшиеся снятием денег, но не было установлено, кто стоял за этой атакой.

В декабре 2016 года специалисты Group-IB нашли вредоносную программу, которая использовалась для атаки Тайваньского банка. Это была программа, очень похожая на ATMSpitter, — разработанная и используемая группой Cobalt в других инцидентах. Именно эта группа ответственна за большинство атак с заражением банкоматов в России, СНГ и множестве других стран. Тактика и инструменты, используемые этой группой для атак на банкоматы, подробно описаны в отдельном отчете http://www.group-ib.ru/cobalt.html

В атаке против европейских банков использовалась реализация ATMSpitter со стандартной библиотекой MSXFS.dll. В Тайване злоумышленники применяли реализацию со стандартной библиотекой CSCWCNG.dll. Дальнейшее расследование полностью подтвердило, что эту атаку провела именно группа **Cobalt**. На тот момент ее интересовали преимущественно сегменты сети по управлению банкоматами и последующая инициация банкоматом выдачи денег через диспенсер. Только потом они переключились на другие цели в банках.

Обе программы представляют собой практически одну функцию main, исполняющуюся последовательно, без создания отдельных потоков. Происходит последовательный вызов необходимых функции из финансовых библиотек, и дается команда выдать деньги из диспенсера. **Кроме этого, есть следующие совпадения:**

- Большинство вредоносных программ для атак на банкоматы имеют продвинутые системы защиты. Например, защиту в виде сессионных паролей для усложнения реверс-инжиниринга со стороны других злоумышленников используют коммерческие протекторы; для сокрытия своего присутствия в системе применяют очистку логов, отключение сети на время своей работы, запись в альтернативные NTFS-потоки, шифрование своих служебных файлов и логов. В обеих реализациях ATMSpitter ничего из этого нет.
- В нем используется только одно средство защиты — проверка месяца запуска. Если текущая дата не совпадает с июлем 2016 (Тайвань) или с сентябрем 2016 (Европа), то программы выдадут особенное сообщение об ошибке. Оно выглядит так, словно невозможно подключиться к устройству.

Сообщение об ошибке:

Европа: WFSOpen failed with error: WFS_ERR_INTERNAL_ERROR

Тайвань: CscCngOpen/CscCdmOpen failed with error: System Failure

Таким образом, сообщение об ошибке не раскрывает реальную причину незапуска программы, и только автор программы знает о ней (см. строку 1 в Таблице 1).

В обеих реализациях имеется идентичный кусок кода, где создается незашифрованный txt файл с результатами выдачи наличных (disp.txt в Европе, и displog.txt в Тайване) – строка 2 в Таблице 1.

В обеих реализациях «ATMSpitter» отсутствует пользовательский интерфейс, управление происходит через командную строку. В качестве аргументов передаются значения: сколько купюр и из какой кассеты банкомата необходимо выдать. Если указано неправильное количество аргументов, ATMSpitter выведет сообщение об ошибке и необходимом синтаксисе (см. строку 3 в Таблице 1).

При этом в обеих реализациях используются аналогичные параметры «Cassette number» (номер кассеты) и «Banknotes Count» (счетчик банкнот).

	Параметр	Европа реализация ATMSpitter с использованием стандартной библиотеки MSXFS.dll	Тайвань реализация ATMSpitter с использованием стандартной библиотеки CSCWCNG.dll	Комментарий аналитика Group-IB
1	Средство защиты	Проверка месяца запуска. Если текущая дата не совпадает с сентябрем 2016, то программа выдаст сообщение об ошибке. Оно выглядит так, словно невозможно подключиться к устройству. WFSOpen failed with error: WFS_ERR_INTERNAL_ERROR Это соответствует месяцу, когда был инцидент в европейском банке – сентябрь 2016.	Проверка месяца запуска. Если текущая дата не совпадает с июлем 2016, то программа выдаст сообщение об ошибке. Оно выглядит так, словно невозможно подключиться к устройству. Error message: CscCngOpen/CscCdmOpen failed with error: System Failure Это соответствует месяцу, когда был инциденты в Тайване – июль 2016.	Соответствует датам инцидентов (в Европе – сентябрь 2016, в Тайване – июль 2016). При этом человек, запускающий программу, не будет видеть реальную причину незапуска, она известна только разработчику.

2	Идентичные куски кода	int v1; // eax@1
		CHAR *v2; // ebx@1
		HANDLE v3; // esi@1
		int v4; // eax@1
		DWORD NumberOfBytesWritten; // [esp+2Ch] [ebp-Ch]@1
		va_list va; // [esp+44h] [ebp+Ch]@1
		
		va_start(va, a1);
		NumberOfBytesWritten = 0;
		v1 = lstrlenA(a1);
		v2 = (CHAR *)malloc(v1 + 10240);
		wvsprintfA(v2, a1, va);
		v3 = CreateFileA(«disp.txt», 0x120116u, 3u, 0, 4u, 0, 0);
		SetFilePointer(v3, 0, 0, 2u);
		v4 = lstrlenA(v2);
		WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);
		CloseHandle(v3);
		free(v2);
			int v1; // eax@1
			CHAR *v2; // esi@1
			HANDLE v3; // edi@1
			int v4; // eax@1
			DWORD NumberOfBytesWritten; // [esp+Ch] [ebp-4h]@1
			va_list va; // [esp+1Ch] [ebp+Ch]@1
			
			va_start(va, lpString);
			NumberOfBytesWritten = 0;
			v1 = lstrlenA(lpString);
			v2 = (CHAR *)malloc(v1 + 10240);
			wvsprintfA(v2, lpString, va);
			v3 = CreateFileA(«displog.txt», 0x120116u, 3u, 0, 4u, 0, 0);
			SetFilePointer(v3, 0, 0, 2u);
			v4 = lstrlenA(v2);
			WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);
			CloseHandle(v3);
			free(v2);
				В обеих реализациях имеется идентичный кусок кода, где создается незашифрованный txt файл с результатами выдачи наличных (disp.txt в Европе, и displog.txt в Тайване)

3	Сообщения об ошибке при некорректной передаче аргументов	Если какие-либо аргументы выходят за пределы возможного диапазона, будет выведено сообщение об ошибке: Error! Banknotes Count should be from 1 to 60 Error! Cassette number should be from 1 to 15 Error! Cassettes count should be from 1 to 15 Error! Dispenses Count should be from 1 to 500	Если какие-либо аргументы выходят за пределы возможного диапазона, будет выведено сообщение об ошибке: Invalid parameter: Cassette slot number. Must be a digit from 1 to 9 Invalid parameter: Banknotes Count. Must be a digit from 1 to 60	Аналогичные сообщения об ошибке, связанные с «Cassette number» (номером кассеты)и «Banknotes Count» (счетчиком банкнот).

Таблица 1. Сравнительная таблица вредоносных программ, используемых в Европе и Тайване

Цель — платежные шлюзы

Атаки на платежные шлюзы — явление довольно редкое, но они случаются каждый год. Первыми такие атаки провели члены преступной группы Anunak, потом аналогичные атаки проводили независимые хакеры, а также преступная группа Cobalt. Пока подобные атаки мы фиксируем только в России. Но, как показывает практика, мошеннические схемы и атаки, отработанные в России, впоследствии применяются в других странах. Целью являются не только банки, но и компании, управляющие платежными терминалами.

Тактика атакующих отличается лишь на последнем этапе:

- После получения удаленного доступа в сеть банка атакующие ищут платежные шлюзы.
- На шлюзах он ищут скрипты и файлы журналов, чтобы понять типичный формат передачи сообщений для осуществления транзакций. Это необходимо для того, чтобы позже формировать такие же сообщения.
- Запускают SOCKS-прокси на внутренних хостах для обеспечения связи с платежными шлюзами или используют другие средства удаленного доступа.

- Создают и запускают в локальной сети скрипт, который автоматически формирует тысячи транзакций на маленькие суммы пополнения карт и балансов телефонов атакующих.
- Другой скрипт переводит деньги с телефонов на карты, и далее запускается стандартная процедура отмыва денег.

  Основная сложность в этой схеме — это процедура обналичивания. Но, в отличие от атак на банкоматы, ущерб от одной атаки значительно больше $1-4 млн.

  У этой схемы есть и преимущество: ежедневно через такие шлюзы проходит огромное количество мелких транзакций, и мошеннические транзакции теряются в общем объеме. Из-за этого сложно установить счета получателей и своевременно остановить вывод денег с них.

Цель SWIFT и АРМ КБР

SWIFT — это система, позволяющая финансовым и нефинансовым организациям передавать транзакции посредством «финансовых сообщений». Аналогом этой системы в России является АРМ КБР. Логика работы обоих систем — отправка сообщений, которые бывают входящими и исходящими. Атакующие поняли, что, чтобы похищать деньги, необходимо иметь возможность манипулировать этими сообщениями, что они успешно сделали в некоторых банках.

- **Май 2016 года** — атака на банк в Гонконге.
- **Июнь 2016 года** — атака на SWIFT на Украине. Похищено $10 млн. Данные об атаке попали в прессу.
- **Ноябрь 2016 года** — атака на АРМ КБР.
- **Декабрь 2016 года** — атака на SWIFT в Турции. Данные об атаке стали известны средствам массовой информации. В результате было похищено $4 миллиона.
- **Январь 2017 года** — атака на банк в Латинской Америке.

Логика атаки простая:

- Обнаружение серверов в атакуемом банке, где стоит SWIFT или АРМ КБР.
- Отслеживание исходящих сообщений.
- Замена в исходящих сообщениях платежных деталей.
- Транзакции подтверждаются входящими сообщениям, поэтому их тоже надо перехватывать и заменять в них мошеннические реквизиты на оригинальные, которые были указаны оператором системы.

  Руками провернуть такую схему практически невозможно, и для реализации необходимо специальное программное обеспечение, которое будет делать это автоматически.

  Приведем примеры инструментов, используемых атакующими для атак в банке Гонконга и России.

Комплект для работы с АРМ КБР состоит из следующих компонент:

Main module — запускает другие модули с параметрами, указанными в основном файле конфигурации.

AutoReplacer (XmlBin) — заменяет платежные реквизиты в отправляемых финансовых сообщениях. Результаты замены записываются в Xml-Resultfile. Поле SUM не меняется, чтобы избежать обнаружения.

Hiding (EdBin) — проверяет входящие / подтверждающие сообщения. Он проверяет поле «PayeePersonalAcc» и сравнивает его с «HackAcc» в файле Xml-Resultfile. Если значения совпадают, то скрытый модуль восстанавливает исходное поле PayeePersonalAcc.

Полный набор инструментария в Гонконге восстановить не удалось. Один из его компонентов выполнял **следующие действия:**

- Ищет в директории D:\WIN32APP\SWIFT\ ALLIANCE\SERVER\Batch\Outgoing\HK\ HKAcksBak\ файлы исходящих сообщений.
- Если файл больше 102400 байт, то допишет в файл C:\\Temp\\Msg\\log.txt «Too big file

<имя файла> : <размер файла> > 102400\r\n», иначе откроет его на чтение и будет искать подстроки «OTTC605384», «OTTC605385», «OTTC601386», «OTTC601387», «OTTC605381», «OTTC605382».

- OTTC означает «Outward Telegraphic Transfer Comm & Charges».
- Если файл содержит эту подстроку, то в лог C:\\Temp\\Msg\\log.txt вставит строчку «Found file: %s with required token: <найденная подстрока>\r\n» и скопирует этот файл в директорию «C:\\Temp\\Msg\\»
- Перейдет в режим ожидания на 2,5 секунды, после чего повторит процесс поиска подстроки.

Цель атаки — карточный процессинг

Карточный процессинг стал основной целью киберпреступников в этом году, поскольку позволяет сравнительно легко и безопасно похищать крупные суммы. Этот метод был испытан в России, а затем многократно повторен в странах СНГ и США всеми крупными преступными группами. Получение доступа к карточному процессингу ничем не отличается от получения доступа к любой другой финансовой системе банка.

Схема очень проста:

- После получения контроля над банковской сетью атакующие проверяли, есть ли возможность подключаться к системе управления карточным процессингом.
- Легально открывали или покупали доступные на рынке карты банка, в который они получили доступ. Обычно для хищения использовалось около 30 карт.
- Мулы — преступники, специализирующиеся на обналичке денег, — с открытыми заранее картами уезжали в другую страну, где ждали сигнала к началу операции.
- Атакующие, используя доступ к карточному процессингу, убирали или увеличивали лимиты на снятие наличных для карт, с которыми уехали мулы.
- Убирали овердрафт лимиты, что позволяло уходить в минус даже по дебетовым картам.
- Мулы, используя эти карты, снимали наличные в одном банкомате, потом переходили к другому и так далее. Средний ущерб от одной такой атаки составлял $0.5 млн.

Преимущества, из-за которых эта схема стала такой популярной:

- Система карточного процессинга защищена не так хорошо, как SWIFT, поэтому атакующие достаточно легко вносили изменения в лимиты и оставались незамеченными. При этом атака может проходить без использования специальных программ, например, тех, что применяют преступные группы Lazarus или MoneyTaker в атаках на SWIFT.
- Не требуется сложная схема обналичивания и отмыва украденных денег. Атакующие сразу снимали чистый кэш.
- Для того, чтобы обеспечить обнал, достаточно оформить или купить несколько карт.
- Снимая деньги в другой стране, хакеры выигрывали время, поскольку служба безопасности банка не могла оперативно связаться с полицией, получить записи с камер видеонаблюдения и задержать преступников. Для сравнения: когда в ходе логической атаки на банкоматы хищение проходило в той же стране, где находился и атакованный банк, это приводило к тому, что людей, снимавших наличность в банкоматах, часто задерживали.

Цель атаки — брокеры и торговые терминалы

В России существовали как минимум три преступные группы, имеющие возможности атаковать брокеров: **Anunak, Corkow, Lurk**. Были выявлены успешные случаи атак с использованием **Corkow**, а во вредонос-

ных программах **Corkow** и **Lurk** обнаружены функции, позволяющие совершать подобные атаки.

Один из громких инцидентов произошел в феврале 2015 года, когда в результате использования вредоносной программы Corkow и несанкционированного доступа к терминалу торговой системы злоумышленник совершил 7 сделок на покупку и продажу долларов США на сумму более $500 млн.

13 октября 2016 организация «Securities and Futures Commission» (SFC) сообщила о 16 хакерских инцидентах, за год затронувших семь брокеров. В результате инцидентов были совершены несанкционированные сделки на сумму свыше $100 млн. долл. Идет следствие.

Уничтожение следов атаки

После успешных атак на банки атакующие всегда стремились уничтожить следы своего присутствия, чтобы усложнить проведение расследования и как можно дольше оставаться незамеченными для исследователей. Для уничтожения следов они использовали такие инструменты, как SDelete, MBRKiller, самописные утилиты для затирания данных. Было очевидно, что использование шифровальщиков для сокрытия следов атаки — лишь вопрос времени.

В начале 2017 года мы зафиксировали первые случаи использования шифровальщиков для сокрытия следов ограбления банка. В ходе атаки на банк с целью его ограбления хакеры получили контроль над доменом. После совершения хищения они запустили модифицированную версию шифровальщика **Petya — PetrWrap** от имени администратора домена на всех компьютерах в сети.

PetrWrap написан на языке C, скомпилирован в MS Visual Studio. Он содержит программу-вымогатель **Petya** (версия 3), которая используется для заражения машины жертвы. Кроме того, **PetrWrap** оснащен собственными криптографическими алгоритмами и в процессе работы изменяет код **Petya**, что позволяет преступникам скрыть факт использования **Petya** в процессе заражения.

После завершения процесса шифрования появляется сообщение о том, что было произведено шифрование, с требованием связаться со злоумышленником по email razlokyou@tutanota.com для получения дальнейших инструкций. Стоит отметить, что в этом инциденте шифровалась только MFT (файловая таблица NTFS) таблица, что позволило восстановить данные. Однако большая часть компьютеров в сети банка вышли из строя, что сильно усложнило реагирование на инцидент.

Атаки на клиентов банков

Трояны для персональных компьютеров

В России

В России, начиная с середины 2012 года, мы наблюдаем постоянное снижение ущерба от банковских троянов для персональных компьютеров. За последний год не появилось ни одного нового банковского трояна, атакующего пользователей в России.

После 2012 года владельцы банковских бот-сетей начали отказываться от эксплойтов и использовать для распространения СПАМ. Напомним, что в прошлом периоде это был основной метод доставки банковских троянов в России. Сейчас мы видим, что ситуация в очередной раз меняется и они заново начинают использовать метод Driveby – взлом легитимных сайтов и перенаправление пользователей на сервер с эксплойтами.

Атаки на компании

Количество групп и, как следствие, количество атак на юридических лиц в России с целью хищения денег уменьшилось практически в два раза по сравнению с прошлым

периодом. В этом году им удалось похитить только 622 миллиона рублей, а в прошлом 956 миллионов. Однако снижение составило лишь -35%, поскольку средний размер ущерба увеличился до 1.25 миллионов рублей. Это свидетельствует о том, что атакующие стали более тщательно подбирать жертв.

Осталось только 3 преступных группы в России, которые похищают деньги у юридических лиц: Ranbyus, RTM, Buhtrap2. Стоит отметить, что бот-сеть Buhtrap сейчас используется другой группой. И в настоящий момент они самые активные. После передачи управления другим людям, спустя некоторое время тактика действия изменилась, и основным вектором распространения стал не СПАМ, а взломанные легитимные сайты, в том числе финансовой тематики. Примечательно, что взломанными финансовыми сайтами оказались те же сайты, что и 5 лет назад, когда распространялся Carberp.

В России владельцы банковских бот-сетей под юридических лиц полностью отказались от атак «Человек-В-Браузере» и используют либо удаленное управление, либо автоматические переводы через системы бухгалтерского учета 1С. При этом модуль автозалива через 1С начали использовать все три группы.

Атаки на пользователей

Физических лиц с помощью банковских троянов для персональных компьютеров атакует только одна преступная группа — Proxy. В этом году им удалось похитить 15.7 миллиона рублей (по сравнению с 6.4 миллионами в прошлом году). Ущерб незначительный, но вырос он благодаря тому, что большую часть прошлого года преступная группа была неактивна.

В январе этого года Proxy начала атаковать клиентов банков Казахстана, продолжая атаки на клиентов некоторых банков России. Но с апреля этого года они полностью прекратили атаки на территории РФ.

На мировой арене

Ситуация с банковскими троянами на мировой арене претерпела серьезные изменения.

С рынка ушли трояны Corebot и Vawtrak (aka Neverquest), разработанные русскоговорящими авторами, причастные к атакам на юридических лиц по всему миру. В случае с Corebot автор просто прекратил его поддержку. А в случае с Vawtrak автор был задержан, что привело к остановке его активности.

Но им на замену пришли новые: Trickbot, Sphinx 2, TinyNuke, Portal, GNAEUS, Plan2016. Вместе с новыми троянами по-прежнему оставались активными Dridex, Qadars, Gootkit, Panda, Jupiter, GozNym, Quakbot, Ramnit, Retefe, Atmos, Tinba, KINS, Citadel, Zeus, Sphinx, Shifu.

Из 22 новых вредоносных программ для хищений денежных средств 20 (91%) создано и управляются людьми, говорящими на русском языке.

Самым заметным игроком этого года стал троян Trickbot, которого называют приемником трояна Dyre. Напомним, что владельцев бот-сети Dyre задержали в конце 2015.

Некоторые атакующие отказываются от веб-инжектов в пользу перенаправления трафика на серверы атакующего с целью перехвата и манипуляцией данными в трафике. К таким троянам относятся Trickbot, GNAEUS, Portal, Quakbot, Dridex, Retefe. Это очень старый метод, но на какое-то время он не пользовался популярностью среди атакующих. Сейчас он заново набирает популярность.

В отличие от России, в других регионах основным методом распространения по-прежнему остается СПАМ. Некоторое время методом Driveby распространялись GozNym, Gootkit, Vawtrak, Ramnit, все остальные использовали электронную почту.

TinyNuke — один из ярких примеров нового тренда. Разработчики вредоносного кода стали более активно и по собственному желанию выкладывать исходные коды своих программ. Рабочий исходный код банковско-

	Trickbot New	Sphinx 2 (zbot.ACB) New	TinyNuke New	Portal New	GNAEUS New	Plan2016 New	Dridex	Qadars	Gootkit	Panda	Jupiter (Midas, Bolek)	GozNym	Quakbot (Qbot)	Ramnit	Retefe (ProxyAdder)	Atmos	Tinba	KINS	Citadel	Zeus	Sphinx	Shifu	Количество
Австралия	●	●					●	●						●	●	●	●	●		●	●		11
Австрия								●							●		●				●		4
Бельгия								●															1
Болгария																				●			1
Бразилия									●												●		2
Великобритания	●						●	●	●	●		●		●	●	●	●	●		●	●	●	14
Германия	●							●	●	●		●		●		●	●	●	●	●	●		12
Испания							●	●	●							●	●	●		●			7
Италия								●	●	●						●	●	●		●		●	8
Казахстан															●								1
Канада	●	●						●	●	●		●	●	●		●	●	●	●	●	●		14
Колумбия																					●		1
Нидерланды									●	●			●			●	●						5
Новая Зеландия	●																●				●		3
ОАЭ																				●	●		2
Португалия																●							1
Польша							●	●		●	●	●							●				6
Россия															●					●			2
Румыния							●																1
США		●	●		●	●	●	●	●	●		●	●	●		●	●	●	●				15
Турция																				●			1
Украина											●												1
Франция		●	●				●		●							●		●		●			7
Швейцария									●						●								2
Швеция									●														1
Япония																	●				●	●	3

го трояна и системы управления был выложен автором в открытый доступ.

В начале года в Германии прошли первые хищения с банковских счетов, когда для обхода двухфакторной аутентификации СМС-код был перехвачен путем атаки на ОКС7 (SS7).

Трояны под Android

Как и ожидалось, рынок банковских Android-троянов оказался самым динамичным и быстро растущим. Ущерб от банковских троянов под Android в России вырос на 136% и перекрыл ущерб от троянов для персональных компьютеров на 30%.

Мы по-прежнему не фиксируем атак на юридических лиц, однако все необходимое для них у киберпреступников уже есть, и мы ожидаем, что атаки могут начаться в ближайшее время.

Атакующим удалось повысить средний ущерб от одной атаки благодаря тому, что новые группы больше ориентированы на получение

данных банковских карт, а не на СМС-банкинг, как это было раньше.

Основным каналом распространения по-прежнему остается СМС. И на текущий момент его используют следующим образом:

1. Массово рассылают СМС с вредоносной ссылкой.
2. Сканируют доски объявлений и на оставленные номера телефона присылают СМС с вредоносной ссылкой - якобы как отклик на оставленное объявление.
3. Вредоносные программы под Android рассылают по контактам СМС с вредоносной ссылкой.

Менее популярным каналом является распространение зараженных приложений на неофициальных репозиториях. Как правило, такое распространение подразумевает вовлечение нескольких людей, которых чаще всего находят на специализированных форумах.

Менее популярным, но самым целевым методом является контекстная реклама в поисковых системах.

6 схем хищений, описанных нами в прошлом отчете, остались прежними:

- Хищение через СМС-банкинг
- Переводы с карты на карту
- Переводы через онлайн-банкинг
- Перехват доступа к мобильному банкингу
- Поддельный мобильный банкинг
- Покупки с помощью Apple Pay

Стоит отметить сокращение активности, связанной именно с СМС-банкингом. Основная причина — задержания, проведенные правоохранительными органами в России. Были арестованы организаторы наиболее активных бот-сетей, использующих схему хищений через СМС-банкинг. Это две группы, использующие троян Cron, и группа, использующая троян Opfake.

Хищение с помощью СМС-банкинга мы по-прежнему фиксируем только в России. Однако для всех остальных стран актуальны все остальные схемы.

Каждый месяц мы фиксируем появление нового банковского трояна под Android. За последний год появились следующие вредоносные программы: Limebot (и позже его новая версия Lipton), Easy, UfoBot, Rello, Loki, Red Alert, Vasya Bot, ExoBot (и позже его новая версия ExoBot 2.0), Instant VBV Grabber, Alien-bot, maza-in, Catelites Android Bot. Авторами всех банковских Android троянов являются русскоговорящие хакеры.

В конце прошлого года авторы трояна Catelites Android Bot сообщили, что сделали универсальный веб-фейк для 2249 банковских приложений из Google Play. Как утверждает автор, 2249 приложений взяты из Google Play методом парсинга по ключевым словам «bank» и «money». Троян ищет на телефоне жертвы одно из этих приложений и выводит универсальное окно, в которое подставляет иконку и название банка, взятое из Google Play.

Важным событием этого года стала публикация автором в открытом доступе банковского трояна Maza-in. Сразу после этого начало появляться множество инсталляций этой вредоносной программы с небольшими модификациями.

Автоматические хищения с помощью Android-троянов очень сильно шагнули вперед. Атакующие используют два сценария автоматического хищения:

Полностью автоматизированное. После попадания на систему троян проверяет состояние банковского счета и автоматически совершает денежные переводы, которые подтверждает перехваченными СМС-кодами. Полное автоматизированное хищение мы фиксируем пока только с СМС-банкингом.

По нажатию одной кнопки. Троян также определяет балансы и предварительно собирает данные банковской карты, либо логин и пароль от интернет-банкинга и автоматически проверяет их корректность. Далее атакующие выбирают, для каких устройств нужно сделать перевод, нажимают кнопку в системе управления бот-сетью, и вредоносная программа по сценарию совершает переводы с карты на карту, либо перевод в интернет-банкинге и автоматически подтверждает транзакции СМС-кодом, который перехватывает на зараженном устройстве.

Apple Pay

Технологии мобильных платежей Samsung Pay и Apple Pay пришли в Россию 29 сентября и 4 октября 2016 года. В начале 2017 года банки начали активно внедрять эти технологии, и хакеры не оставили это без внимания.

Преступная схема следующая:

1. Мошенники заражали Android-устройство и получали из него данные банковской карты либо логин/пароль от интернет-банкинга, а также информацию о текущем балансе.
2. Если баланс пользователя представляет интерес, то мошенники привязывали на своем iPhone банковский счет жертвы к Apple Pay. Для этого им нужны данные карты или логин/пароль, которые они получали на первом шаге, а также СМС-подтверждения, которые успешно перехватывает Android-троян. Теперь они могут совершать покупки без наличия физической карты.
3. Apple Pay дает два основных преимущества: не надо физически носить карту, нет лимитов на транзакции. Считается, что если во время оплаты пользователь подтверждает платеж своим отпечатком пальца, значит, транзакция должна быть исполнена, поэтому остановить такое мошенничество сложно.
4. При этом для совершения покупки на большую сумму платежный терминал может запросить ПИН-код. Но у некоторых банков есть список доверенных точек, в которых ПИН-код даже при больших покупках не требуется. Поэтому мошенники вынуждены осуществлять покупки в определенных точках.

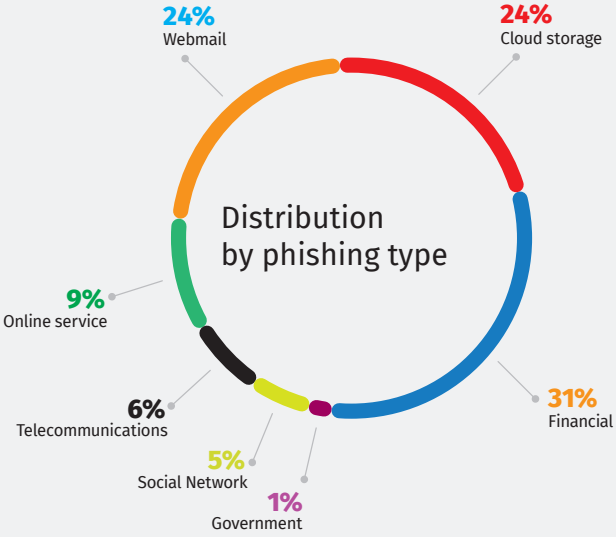
Ландшафт банковских Android-троянов для описываемого периода выглядел следующим образом:

Трояны, атакующие СМС-банкинг (только в России)	Трояны, использующие веб-фейки в России	Трояны, использующие веб-фейки в мире
Agent.SX Fakeinst.FB Opfake.A Flexnet Granzy Cron Agent.BID	Limebot Tiny.z Honli Asucub Cron Agent.BID ApiMaps	Catelites Android Bot Maza-in Alien-bot Instant VBV Grabber Reich Marcher Easy UfoBot Rello Loki Red Alert Vasya Bot ExoBot Skunk Abrvall Xbot GMbot Spy.agent.SI

Фишинг

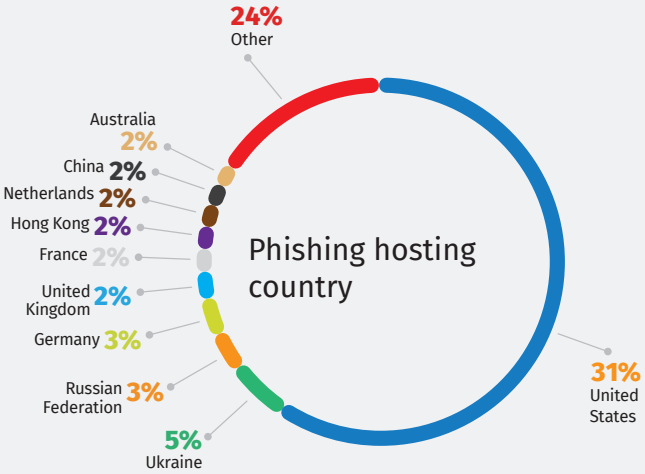
Нами было обнаружено и проанализировано 1,4 миллиона уникальных фишинговых ссылок на 657 тысячах доменах. 5% из этих ссылок использовали HTTPS.

Традиционно основной целью мошенников являются финансовые учреждения. Почти 80% всех фишинговых ресурсов попадают в следующие три категории: финансовый (31%), облачные хранилища (24%) и почтовые сервисы (24%).



Большая часть фишинговых ресурсов хостилось на взломанных легитимных сайтах. В основном атакующие использовали хорошо известные уязвимости под системы управления контентом Joomla и WordPress.

В России ситуация немного иная. Взломанные сайты используются как источник жертв. При посещении взломанного сайта при определенных условиях жертву перенаправляли на фишинговый сайт, который хостится на арендованных атакующими серверах, либо бесплатных хостингах. 60% всех фишинговых сайтов хостилось в США, на втором месте Украина (5%), а третью и четвертую позицию делят Россия и Германия (по 3%).



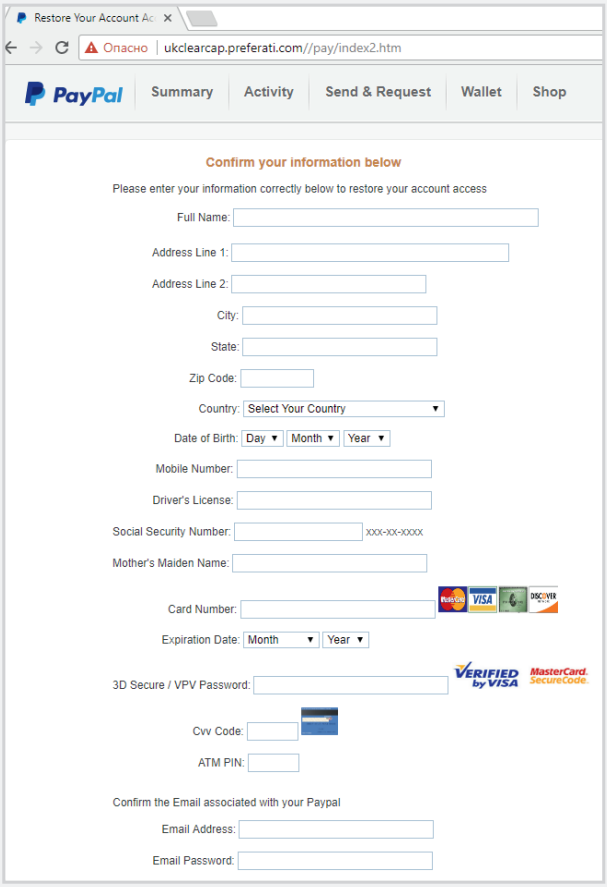
Фишинг под банки и платежные системы в России автоматизирован и проходит в реальном времени, что позволяет обходить СМС-подтверждения на списание денег. Ежедневно жертвами финансового фишинга в России становятся более 900 клиентов разных банков, что в три раза превышает ежедневное количество жертв от вредоносных программ. Однако сумма ущерба от фишинга в десятки раз меньше, чем от вредоносных программ. В прошлом году мы предупреждали, что автоматизация фишинга и простота его использования станет основной причиной роста фишинговых атак и нанесенного ущерба.

Всего в России действует 15 групп, занимающихся фишингом под финансовые учреждения. Суммы ущербов всегда небольшие, но количество жертв, которых они заманивают на свои сайты, ежедневно исчисляется тысячами. Около 10-15% посетителей финансовых фишинговых сайтов вводят свои данные. За год им удалось похитить 236.6 миллионов рублей.

В других регионах мы наблюдаем много оффлайн-фишинга. То есть на фишинговом сайте осуществляется сбор данных, они сохраняются локально или отправляются мошеннику, который уже позже проверяет их корректность и пытается воспользоваться спустя какое-то время.

Хакеры используют готовые фишинг-наборы (Phishing kits) — это уже готовый фишинго-

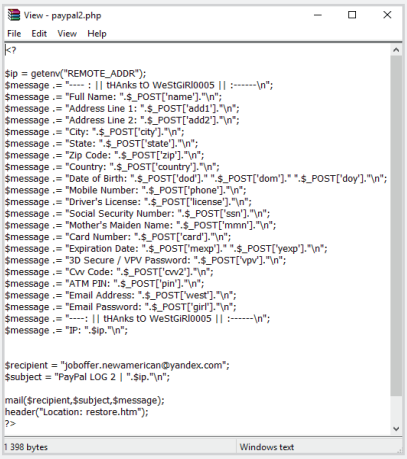
Фишинговая страница

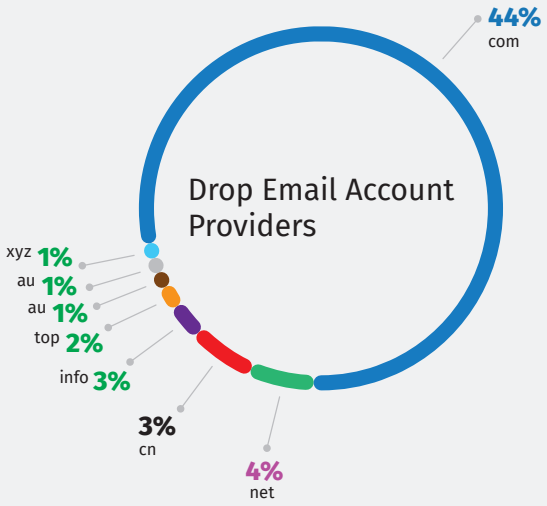


Фишинг кит

your_email_here.php	2 KB	PHP File
true.php	29 KB	PHP File
Thank_You.php	22 KB	PHP File
secure.php	23 KB	PHP File
robots.txt	61 bytes	Plain Text
lib	--	Folder
info.php	540 bytes	PHP File
index.php	11 KB	PHP File
includes	--	Folder
identity.php	52 KB	PHP File
html	--	Folder
Email3.php	1 KB	PHP File
Email2.php	2 KB	PHP File
Email.php	2 KB	PHP File
card.php	33 KB	PHP File
bank.php	26 KB	PHP File
auth	--	Folder
account.php	79 KB	PHP File

Конфигурационный файл





вый сайт с конфигурационным файлом, в котором определяется логика работы фишингового сайта и то, куда должны быть отправлены скомпрометированные данные. Мы собрали более 12 тысяч уникальных фишинговых наборов и проанализировали их конфигурационные файлы. В подавляющем большинстве случаев скомпрометированные данные отправлялись на адрес электронной почты. В 80% случаев фишеры регистрируют почту для сбора скомпрометированных данных в Gmail, на российские Yandex и Mail.ru приходится лишь 6%.

Коллективная работа

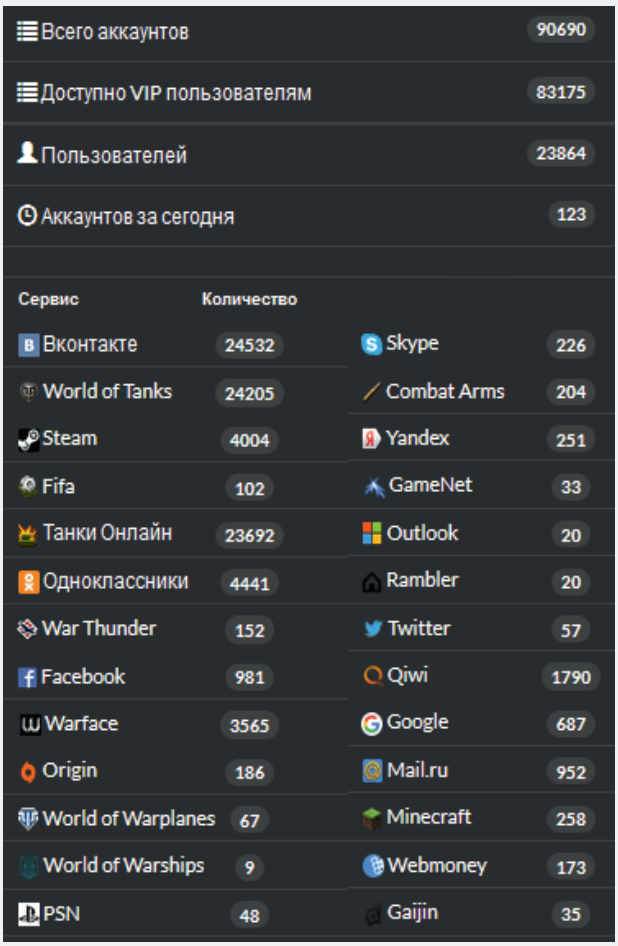
Русскоговорящие киберпреступники очень часто создают и используют партнерские программы, например, по распространению вредоносных программ, спама, телефонному мошенничеству и т.п. Коллективная работа над одной задачей позволяет организаторам быстрее добиваться своих целей и масштабировать свой криминальный бизнес. Разумеется, при этом им необходимо выплачивать небольшой процент своим партнерам.

В случае с фишингом ситуация похожа. В конце прошлого года один из злоумышленников создал 26 фишинговых сайтов под

социальные сети, игровые ресурсы, почтовые сервисы, электронные кошельки. Дополнительно он создал сайт, где публиковал ссылки на свои фишинговые ресурсы и предлагал каждому желающему, кто хочет кого-то атаковать, пользоваться этими фишинговыми ресурсами.

Это означало, что каждый, кто не может создать фишинговый сайт своими силами, может воспользоваться уже готовыми фишинговыми ресурсами. За такое бесплатное пользование собранные данные были доступны всем VIP-пользователям. Пользователи с VIP-доступом получали доступ не только к чужим данным, но и гарантии, что все собранные ими с помощью фишинга данные не будут доступны другим пользователям. VIP-доступ на 30 дней стоил 200 рублей.

Таким образом участниками этой схемы в



течение нескольких дней были скомпрометированы более 90 000 логинов и паролей.

Это наглядный пример эффективной коллективной работы, позволяющий даже людям без необходимого опыта начать проводить простые атаки.

POS-трояны

Анализируя данные на кард-шопах, можно сделать однозначный вывод, что самым ходовым товаром являются не полные данные карт, которые можно получить с помощью троянов, фишинга, взлома e-commers сайтов, а именно данные магнитной полосы. Основным источником таких данных являются POS-трояны.

Атакующие по-прежнему делятся на две категории:

1. Массово и случайно атакующие всех подряд в поисках возможности установить POS-троян.
2. Целенаправленно атакующие вендоров POS-терминалов или крупные сетевые организации, доступ в сети которых тоже открывает возможность заражения сразу множество устройств.

Как и в случае с банковскими троянами, за отчетный период были выявлены новые POS-трояны: **LockPoS**, **MajikPOS**, **FlokiBot**, **ScanPOS**, **FastPOS**.

Ничего особенного новые трояны не привнесли. Они по-прежнему работают как RAM-scrapers и, анализируя оперативную память, извлекают из нее данные банковских карт — как с магнитной полосой, так и с чипом.

Но никуда не делись и старые трояны (**PoSeidon**, **AbaddonPOS**, **Alina** и т.п.), которые также зарекомендовали себя достаточно эффективными инструментами для сбора данных банковских карт.

Обычно тактика действий атакующих следующая:

1. Используя сканеры сети, осуществляется поиск открытых портов, через которые можно получить доступ к удаленному управлению устройством (среди которых RDP и VNC).
2. Используя различные брутеры и небольшие словари, атакующие начинают подбор паролей к таким устройствам. Словари содержат характерные имена пользователей и паролей для POS-терминалов, например, различные комбинации со словами pos, cash, payment и т.п.
3. В случае успешного подбора пароля мошенник проверяет, к чему он получил доступ и представляет ли для него это устройство интерес. Например, это сеть ресторана.
4. На устройство загружается инструмент восстановления паролей Mimikatz, Fgdump, VNCPassView.
5. На некоторые компьютеры и терминалы устанавливают бэкдоры, которые обычно являются публичными RAT (Remcos, Netwire и д.р.), а также легитимные средства удаленного доступа – такие, как Ammyy Admin, TeamViewer.
6. Используя удаленный доступ, руками устанавливают POS-троян.

Группы, которые проводят целенаправленные атаки, делают это гораздо интереснее, но и

ущерб в их прибыли значительно выше.

	Пострадавшая компания	Описание
Июль 2017	**B&B Theatres**	Компания, которая владеет и управляет крупнейшей театральной сетью в Америке. Была взломана в октябре 2015 году и данные карт утекали в сети вплоть до апреля 2017.
Июнь 2017	**The Buckle Inc.**	Компания управляет более чем 450 магазинами. Была взломана в октябре 2016 и данные карт утекали в сети вплоть до апреля 2017.
Май 2017	**Kmart**	Крупнейший ритейлер в США в очередной раз был скомпрометирован. В 2014 году он уже был взломан. В обоих случаях целью были POS-терминалы.
Май 2017	**Sabre Corp.**	Был получен доступ к системе SynXis Central Reservations system, используемой многими отелями и содержащей платежные данные.
Апрель 2017	**Shoney's**	Компания владеющая более 150 ресторанами. Была взломана в декабре 2016 и данные карт утекали в сети вплоть до марта 2017.
Март 2017	**24×7 Hospitality Technology**	POS-вендор который обрабатывает операции с кредитными и дебетовыми картами для тысяч отелей и ресторанов. Данные карт собирали с помощью трояна PoSeidon.
Март 2017	**Verifone**	Verifone крупнейший производитель платежных терминалов. Был взломан в середине 2016 . Предположительно, использовался троян MalumPOS.
Февраль 2017	**Arby's**	Компания владеет более 1000 ресторанами, часть из которых были заражены. Данные карт утекали в сети с октября 206 по январь 2017.
Декабрь 2016	**InterContinental Hotels Group**	Головная компания для более чем 5000 отелей по всему миру, включая Holiday Inn. Данные утекали в сеть с сентября 2016 по декабрь 2016, более чем с тысячи точек.
Август 2016	**Eddie Bauer**	Сеть более чем 350 магазинов была взломана. Во всех магазинах на кассы был установлен троян и данные карт утекали с января по июль 2016.
Август 2016	**Oracle**	MICROS – подразделение Oracle продают POS-системы, которые используются более чем в 330 тысячах мест.
Июль 2016	**Kimpton Hotels**	Сеть из 62 бутиковых отелей была взломана и в период с февраля по июль 2016 данные карт утекали в сеть.

Атаки на криптовалютные сервисы

Криптовалюты и связанные с ними сервисы — крайне динамичный и высокодоходный рынок. При такой скорости развития и притока денег вопросы безопасности часто становятся для стартапов второстепенными. Хакеры успешно этим пользуются. Чем успешнее финтех-проект, чем масштабнее ICO, тем он более привлекателен для атак.

Количество угроз для криптовалютных и блокчейн-проектов, фиксируемых нашей системой **Threat Intelligence**, взлетело вместе с курсом биткоина. Уже успешно использованы уязвимости в исходном коде смарт-контрактов. Получены доступы к секретным кошелькам криптобирж. Произошли утечки баз данных пользователей, угоны доменных имен. Владельцы бот-сетей отслеживают обращения зараженных устройств к веб- и мобильным приложениям кошельков, бирж, фондов. Создание и продвижение фишинговых сайтов-клонов для перехвата доступов к клиентским счетам уже ставится на поток.

Так, по данным Chainalysis , хакерам удалось украсть 10% всех средств, инвестированных в ICO-проекты в 2017 году в Ethereum. Общий ущерб в долларовом эквиваленте составил $225 миллионов, 30 000 инвесторов лишились в среднем по $7500. Подобный размах мы наблюдали на заре развития онлайн-банкинга — хакеры всегда следуют за деньгами.

Уязвимости в исходных кодах

Уязвимость в исходных кодах — это ночной кошмар для разработчиков сервисов.

17 июня 2016 года произошла, пожалуй, самая масштабная атака за всю историю криптоиндустрии — из-за ошибки в коде перспективный и очень популярный в то время проект The DAO лишился более $60 миллионов.

Хищение было совершено из-за уязвимости под названием «рекурсивный вызов» — она позволяла бесконечно снимать средства The DAO и переводить их в дочернее ДАО посредством многократного разделения ДАО, повторно собирая ETH в рамках одной транзакции.

Однако окно для создания дочернего ДАО составляло ровно 27 дней, и средства с кошелька все это время нельзя было вывести. Сообщество начало искать пути «восстановления справедливости» и в конце концов остановилось на Хардфорк Ethereum. Таким образом, все токены DAO, вне зависимости от того, находятся они в «белой» или «черной», дочерней или основной ДАО, теперь заморожены и отправлены на новый адрес контракта. С этого адреса держатели токенов смогут вывести принадлежащую им долю. Экстра-баланс будет отправлен на адрес с мультиподписью, контролируемый кураторами The DAO. Последние вернут дополнительные токены, потраченные во время этапа создания, законным владельцам.

19 июля 2017 года из-за уязвимости в коде смарт-контракта Multisig кошелька Parity (1.5 и более поздний) хакер смог вывести 153 000 ETH, то есть порядка $30 000 000 по курсу на тот момент времени.

Атака была практически сразу замечена разработчиками. Почти сразу группа энтузиастов, называющих себя The White Hat Group, воспользовалась тем же эксплоитом, чтобы спасти деньги пользователей, переведя их на неподверженный багу кошелек.

Разработчики Parity сообщили, что суммарно насчитывалось 596 уязвимых кошельков, и основной удар злоумышленников пришелся на три из них — **кошельки ICO:**

- Edgeless Casino
- Swarm City
- æternity blockchain

В кошелек The White Hat Group было выведено почти 40% всего инвестиционного портфеля криптовалютного фонда satoshi.fund — более $7 миллионов.

Позже The White Hat Group вернули все средства.

Целенаправленные атаки

Самым ценным для любого криптовалютного сервиса являются секретные ключи, которые используются для подтверждения транзакций. Компрометация ключа означает потерю контроля над счетом и, как следствие, всех средств.

А вот возможность получения таких ключей не сильно отличается от того, чтобы получить контроль над критичной системой внутри банка, а в некоторых случаях гораздо проще. И тут основной проблемой является получение доступа в локальную сеть компании, для чего используются точно такие же методы, что и при атаках на банки.

2 августа 2016 года третья в мире по популярности гонконгская криптовалютная биржа Bitfinex была скомпрометирована и в результате лишилась почти 120 000 биткоинов (порядка $72 млн по курсу), спровоцировав заметное колебание курса криптовалюты. Аккаунты клиентов биржи были защищены технологией мультиподписи — два из трех ключей хранились самой биржей (один в холодном хранилище), а третий — BitGo. Успешный вывод средств свидетельствует о получении контроля над корпоративной инфраструктурой Bitfinex.

13 октября 2016 года с одного из биткоин-адресов Польской криптовалютной биржи Bitcurex несколькими транзакциями было переведено около 2300 биткоинов, что составило около $1,5 млн. В тот же день администрация объявила о проблемах на сервере, возникших в связи с обновлением биткоин-клиента. Через неделю после этого команда биржи сделала новое заявление, в котором говорилось о текущих работах по обновлению сети и повышению мер безопасности. 27 октября на сайте биржи появилось еще одно сообщение администрации, в котором она признала факт хакерской атаки и потерю части средств. 30 ноября 2016 года биржа возобновила деятельность, но в начале 2017 года сайт вновь ушел в оффлайн, и более не появлялось никаких сообщений и разъяснений, биржа просто прекратила работу.

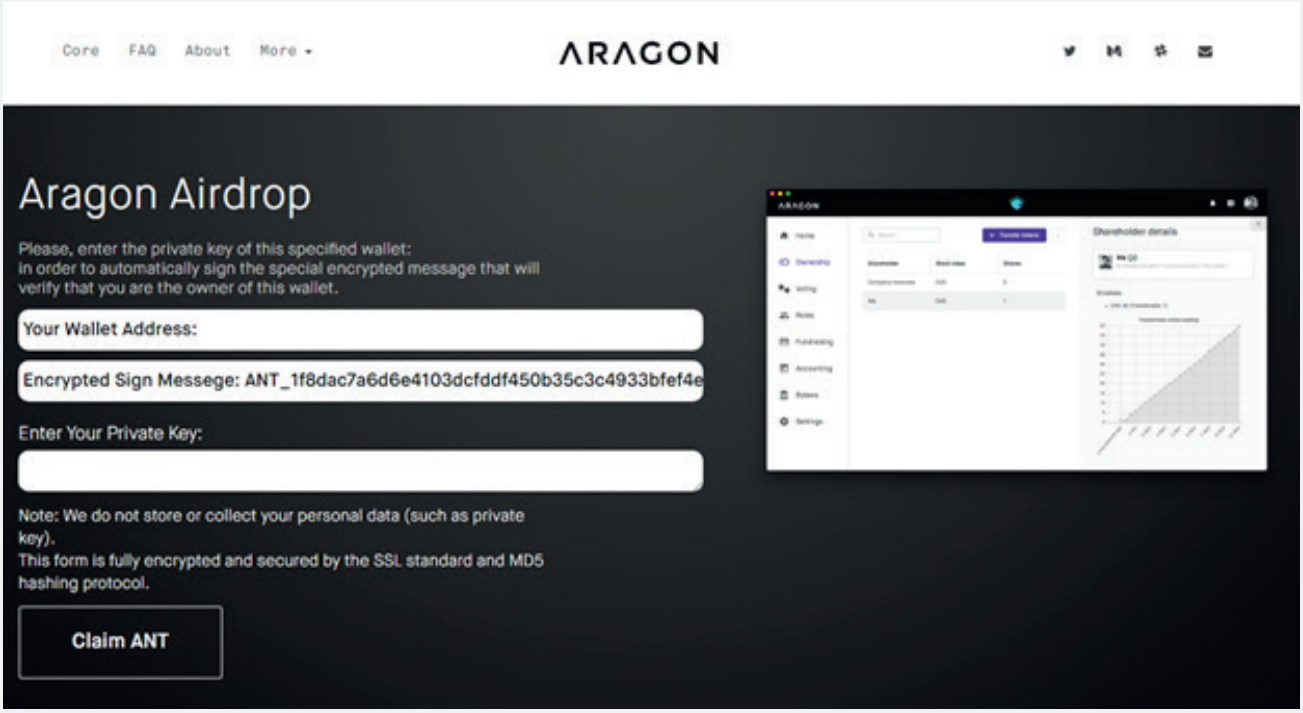
16 июля 2017 года израильский стартрап CoinDash запустил процедуру ICO (Initial Coin Offering, первичного размещения токенов). Через три минуты после размещения токенов неизвестные злоумышленники взломали сайт CoinDash и подменили адрес официального Ethereum-кошелька на свой собственный. За первые пять минут после взлома на кошелек хакеров перевели более $6 млн. В настоящее время злоумышленники получили уже 43 488 ETH, что по курсу на тот момент соответствовало $8,3 млн.

29 июня 2017 года Южнокорейская криптовалютная биржа Bithumb, являющаяся четвертой по величине в мире, сообщила о взломе. Атакующие сумели скомпрометировать компьютер одного из сотрудников биржи, после чего получили доступ к информации о 31 800 пользователях ресурса (порядка 3% от всей пользовательской базы).

Domain hijacking

12 октября 2016 года администрация Blockchain.info, одного из наиболее популярных веб-кошельков в интернете, предупредила о DNS-hijacking атаке — данные DNS были изменены: CloudFlare подменили хостинг-провайдером из Талсы, США. Посетители сайта попали на совершенно другие серверы, где могли подвергнуться атакам.

30 июня 2017 года неизвестные злоумышленники сумели перехватить контроль над доменом Classic Ether Wallet — кошелька для криптовалюты Ethereum Classic (ETC). После перехвата управления доменом хакер изменил настройки сайта так, чтобы поль-



зователи перенаправлялись на его сервер. Вредоносная версия сайта «копировала закрытый ключ, вводимый пользователем, и пересылала его хакерам». В результате было похищено около $300 000.

Фишинг под ICO

Этот тип атак становится очень популярным среди атакующих из-за своей простоты и эффективности.

Тактика атакующих следующая:

- Они отслеживают новые проекты, выходящие на ICO
- Создают фишинговую страницу, основным отличием которой является запрос секретного ключа
- Все секретные ключи автоматически подключатся к электронным кошелькам мошенников, и денежные средства автоматически выводятся на заданные мошенником счета.

Отслеживая такие кошельки, мы видим, что одна группа может зарабатывать до $1.5 миллионов долларов в месяц.

https://etherscan.io/address/0x68b0e0db7918c0211ea1fb78292a879839137dd0

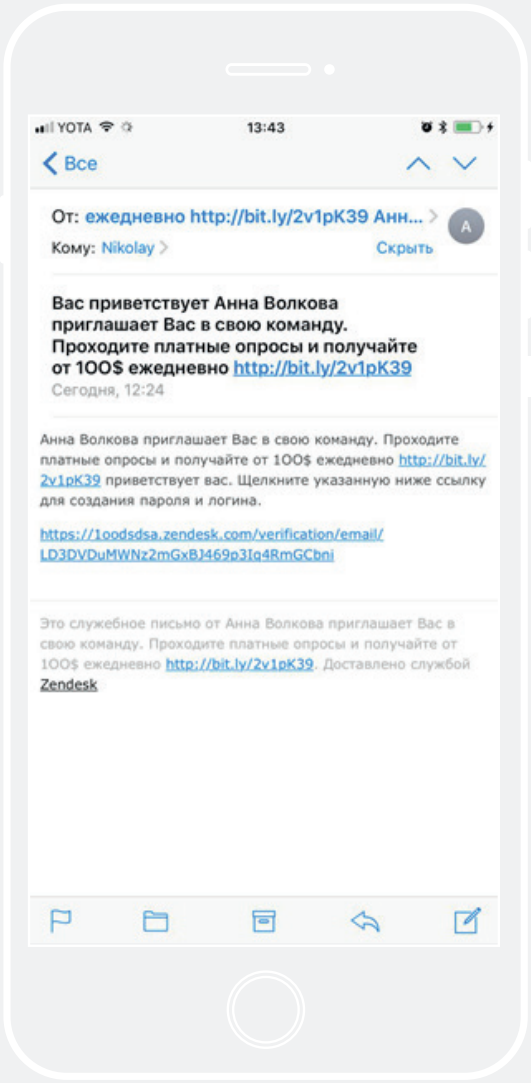
https://etherscan.io/address/0x0a5650aba6473c48898f3d9366b52c21a4eec37b

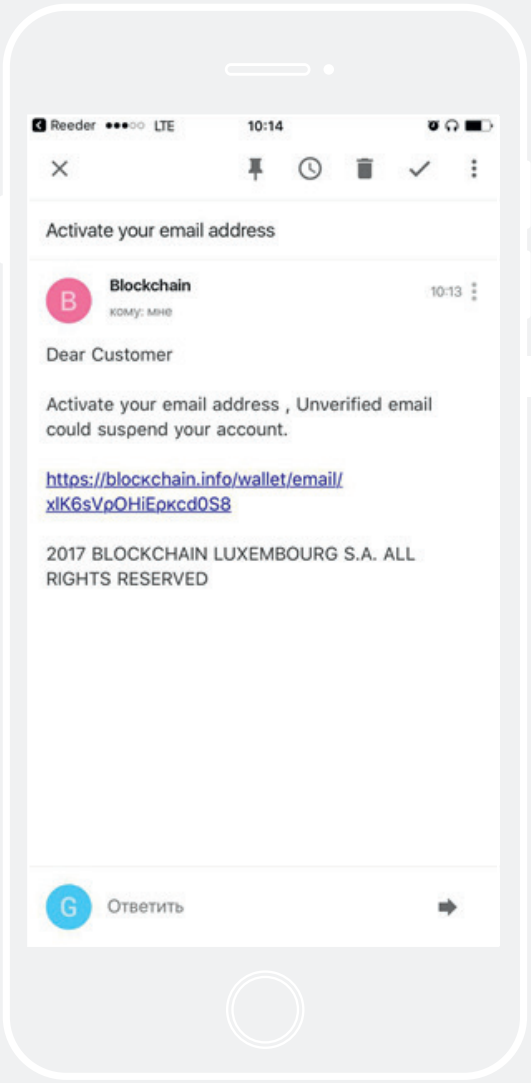
https://etherscan.io/address/0x1e80dad60d19fb8159af3f440a8ceaa0e5581847

https://etherscan.io/address/0x3681828DA105fC3C44E212f6c3Dc51a0a5A6F5C6

https://etherscan.io/address/0x4a0d27a1044dd871a93275de5109e5f5efc4d46e

https://etherscan.io/address/0x89C98CC6D9917B615257e5704e83906402f0f91f





Фишинг

Для получения доступа к кошелькам не обязательно создавать фишинговую страницу под каждую отдельную биржу. Для восстановления доступа может быть достаточно восстановления пароля на адрес электронной почты или номер мобильного телефона.

Для доступа к электронной почте используются фишинговые страницы под популярные почтовые сервис-провайдеры (Gmail, Yahoo, Outlook и т.п.).

Ограничения применения

Настоящим Group-IB информирует о том, что:

- Настоящий отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
- Оценка рынка высокотехнологичных преступлений 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 компании

Group-IB – одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий.

С 2003 года мы работаем в сфере компьютерной криминалистики, консалтинга и аудита систем информационной безопасности, обеспечивая защиту крупнейших российских и зарубежных компаний от финансовых и репутационных потерь.

- Крупнейшая и самая опытная Лаборатория компьютерной криминалистики в Восточной Европе
- Круглосуточный Центр реагирования на инциденты информационной безопасности CERT-GIB
- Система раннего предупреждения киберугроз – линейка продуктов для проактивной защиты

EUROPOL INTERPOL

Официальный партнёр EUROPOL и INTERPOL

OSCE

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

WORLD ECONOMIC FORUM

Постоянный член Всемирного экономического форума

IDC Gartner Forrester

В числе лучших мировых поставщиков Threat Intelligence по версии международных агентств

УНИКАЛЬНАЯ РЕСУРСНАЯ БАЗА, НАКОПЛЕННАЯ ЗА 14 ЛЕТ РАБОТЫ

Высокотехнологичная инфраструктура сбора данных об угрозах в ключевых регионах происхождения: Россия и Восточная Европа, Юго-Восточная Азия, Ближний Восток

ИНФРАСТРУКТУРА МОНИТОРИНГА

Распределенная сеть мониторинга и HoneyNet-ловушек

Аналитика бот-сетей

Трекеры сетевых атак

Мониторинг хакерских форумов и закрытых сетевых сообществ

Данные сенсоров TDS

Система поведенческого анализа

ОПЫТ ЭКСПЕРТОВ

Результаты криминалистических экспертиз Лаборатории Group-IB

Материалы расследований

Мониторинг и анализ вредоносных программ

База обращений и практика реагирования на инциденты CERT-GIB

Целевая аналитика Group-IB на 7 языках

ОБМЕН ДАННЫМИ

Команды реагирования CERT

Регистраторы и хостинг-провайдеры

Производители средств защиты

Организации и объединения по противодействию киберугрозам

Europol, Interpol и правоохранительные органы

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ПОД УПРАВЛЕНИЕМ ОПЫТНЫХ СПЕЦИАЛИСТОВ

Собственные решения для извлечения данных из закрытых источников, поиска по хакерским площадкам, проведения криминалистических исследований, анализа и моделирования угроз, в том числе:

Выявление неизвестных угроз с помощью алгоритмов поведенческого анализа и технологий машинного обучения

Система детектирования фишинга, извлечения phishing kits и оперативное блокирование опасных ресурсов с помощью глобально признанного CERT

Масштабная база преступных групп и индивидов с автоматическим построением связей между преступниками и анализом социальных графов

Предотвращаем и расследуем киберпреступления с 2003 года.

www.group-ib.ru
blog.group-ib.ru
info@group-ib.ru
+7 495 984 33 64
twitter.com/groupib
facebook.com/group-ib