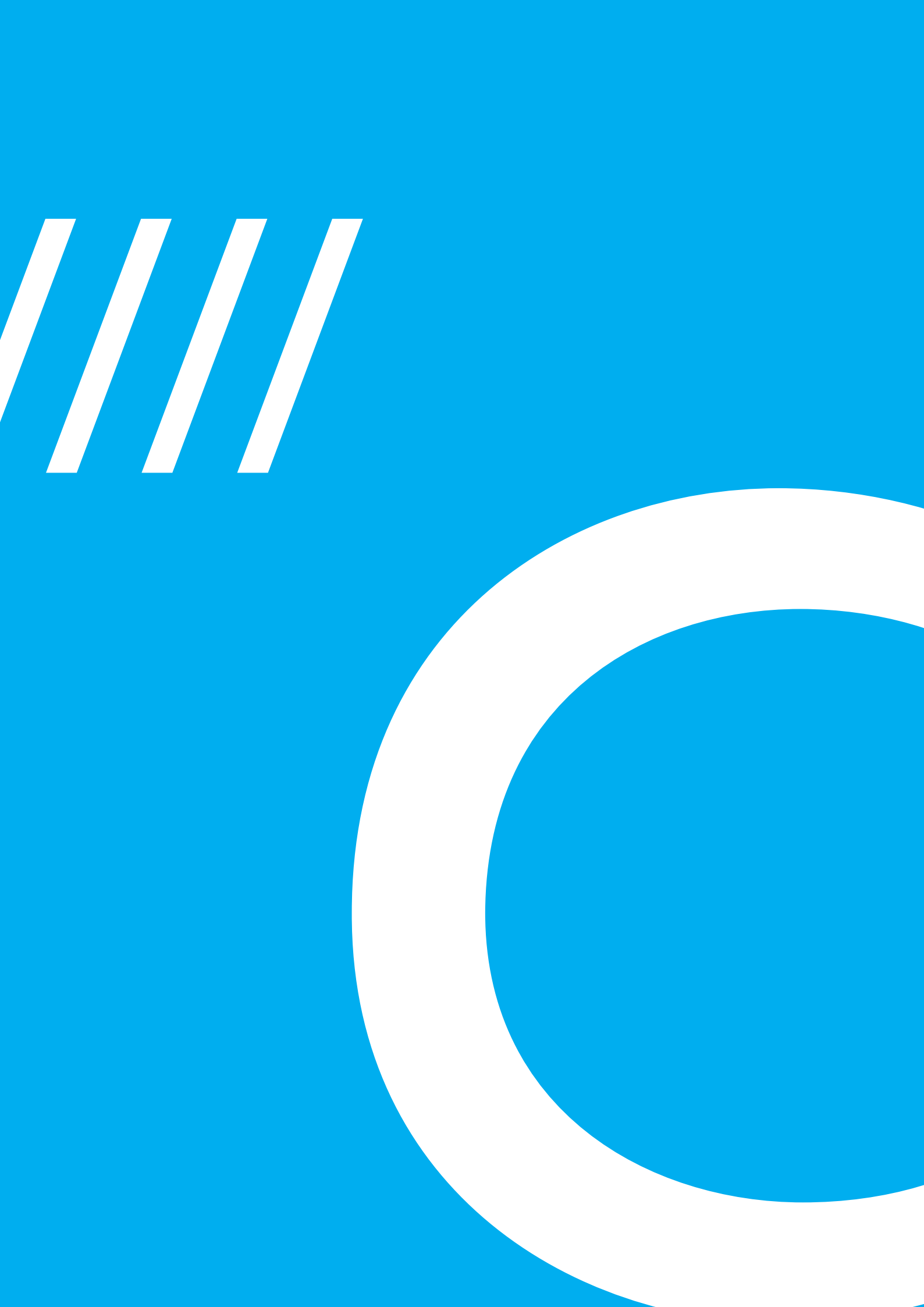
2018

Криптовалютные биржи

Анализ утечек учетных записей пользователей

www.group-ib.ru



Содержание

01

01—
Выводы

ЗА ГОД ЧИСЛО СКОМПРОМЕТИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ КРИПТОБИРЖ ВЫРОСЛО НА 369%

В НАЧАЛЕ 2018 ГОДА ИЗ-ЗА ПОВЫШЕННОГО ИНТЕРЕСА К КРИПТОВАЛЮТАМ И БЛОКЧЕЙН-ИНДУСТРИИ КОЛИЧЕСТВО ИНЦИДЕНТОВ ВЫРОСЛО НА 689% ПО СРАВНЕНИЮ С ПОКАЗАТЕЛЕМ 2017 ГОДА

ВЫВОДЫ

Экспертами международной компании Group-IB, специализирующейся на предотвращении кибератак и разработке продуктов для информационной безопасности, была проанализирована кража 720 учетных записей (логинов и паролей) пользователей 19 бирж на основе данных, полученных от системы Group-IB Threat Intelligence.

***

Ключевые выводы исследования:

- Зафиксирован устойчивый рост числа скомпрометированных учетных записей пользователей криптобирж. За год их количество увеличилось на 369%.

- В начале 2018 года из-за повышенного интереса к криптовалютам и блокчейн-индустрии количество инцидентов выросло на 689% по сравнению со среднемесячным показателем 2017 года.

- Как минимум 5 из 19 рассматриваемых в исследовании бирж стали жертвами целенаправленных кибератак, что привело к большим финансовым потерям (около $80 миллионов).

- Из 19 проанализированных бирж, не было таких, где бы ни один пользователь не пострадал от атак хакеров.

- США, Россия и Китай – три страны, в которых зарегистрированные пользователи чаще других становились жертвами кибератак. Каждый третий пострадавший находится в США.

- Эксперты Group-IB выявили 50 активных ботнетов, задействованных для кибератак на пользователей криптовалютных бирж. Используемая киберпреступниками инфраструктура, в основном, базируется в США (56,1%), Нидерландах (21,5%), Украине (4,3%) и России (3,2%).

- Число используемых злоумышленниками вредоносных программ постоянно увеличивается, а сами инструменты регулярно модифицируются. Среди наиболее часто используемых вредоносных программ — трояны AZORult и Pony Formgrabber, а также бот Qbot.

- Активизация мошенников и повышенное внимание хакерских группировок к криптоиндустрии, модификация вредоносных программ, а также значительные объемы украденных средств, сигнализируют о том, что отрасль еще не готова защищать себя и своих пользователей.

02

02–
Предисловие

ИССЛЕДОВАНИЕ ПОСВЯЩЕНО ОЦЕНКЕ КОЛИЧЕСТВА УТЕЧЕК УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ КРИПТОВАЛЮТНЫХ БИРЖ И АНАЛИЗУ ХАРАКТЕРА ИНЦИДЕНТОВ

БЫЛИ ОЦЕНЕНЫ ПРИЧИНЫ УТЕЧЕК И РАЗРАБОТАНЫ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ И БИРЖ

ПРЕДИСЛОВИЕ

Ажиотаж вокруг блокчейна и криптовалют вызвал повышенное внимание к индустрии со стороны киберпреступников. Первые инциденты взломов криптовалютных сервисов, были зафиксированы еще в 2011 году. В 2017 году, одновременно с резким увеличением интереса к криптовалютам, рекордным показателями их капитализации, взлетом курса биткоина, произошли десятки атак на криптовалютные сервисы.

***

В итоге в 2017 году, по данным совместного исследования «EY research: initial coin offerings (ICOs)» аналитиков компаний EY и Group-IB [12], киберпреступникам удалось украсть 10% всех средств, инвестированных в ICO (первичное предложение токенов) через Ethereum, а общий ущерб от атак хакеров на ICO проекты составил почти $400 млн. Например, только в результате взлома биржи Coincheck в январе 2018 года была похищена рекордная сумма в $533 миллиона.

Активизация мошенников и повышенное внимание хакерских группировок к криптоиндустрии, модификация вредоносных программ под криптовалюты, а также значительные объемы украденных средств, – все это сигнализирует о том, что рассматриваемая отрасль еще не готова защищать себя и своих пользователей. Таким образом, предположительно в 2018 году количество инцидентов будет увеличиваться.

Такая ситуация требует оперативной и эффективной реакции всех заинтересованных сторон, включая экспертов из разных областей.

Определить точную сумму ущерба криптоиндустрии от кибератак довольно проблематично, что обусловлено целым рядом причин:

- высокий уровень анонимности и нежелание раскрывать реальную информацию о размерах похищенных средств, опасаясь банкротства;
- отсутствие законодательно утвержденных процедур и обязательств по раскрытию данных об утечках и инцидентах;
- большое количество блокчейнов и валют, действующих субъектов (например, ICO-проекты, кошельки, биржи, майнеры) и отсутствие универсальной методики оценки потерь;
- значительное количество ICO-проектов, которые по своей сути являются мошенническими.

Цель текущего исследования – оценить количество утечек учетных записей пользователей криптовалютных бирж и проанализировать характер этих инцидентов, чтобы определить причины компрометации данных и предложить рекомендации биржам и пользователям по обеспечению безопасности.

03

03—
Результаты исследования

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Для исследования были отобраны 19 крупнейших по капитализации криптовалютных бирж. Проанализировано 720 инцидентов, в ходе которых киберпреступникам удалось получить доступ к паролям и логинам пользователей на сайтах криптобирж.

Скомпрометированные учетные записи относятся к следующим сервисам: Binance, Bit-z, Bitfinex, Bithumb, Bitstamp, Bittrex, BTCC, CEX.io, Coinone, Gate.io, GDAX, Gemini, HitBTC, Huobi, Kraken, KuCoin, OKEx, Poloniex, Wex.nz.

По итогам проведенного исследования получено, что на всех торговых площадках были инциденты взломов персональных кошельков пользователей.

3.1. РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО БИРЖАМ

Исследование показало, что наибольшее число скомпрометированных учетных записей в данной выборке пришлось на биржи Poloniex – 174 учетных записи, Bittrex – 111, CEX.io – 95, HitBTC - 83, Kraken - 61. (Рис. 1).

Такое распределение, вероятнее всего, связано с популярностью данных торговых площадок среди инвесторов и в Интернете, что привлекло внимание мошенников.

3.2.ДИНАМИКА РОСТА УТЕЧЕК

Первые 5 инцидентов кражи учетных записей пользователей криптобирж произошли в 2014 году, что зафиксировала система кибербразведки Group-IB Threat Intelligence (см. приложение 2):

- по сравнению с 2016 годом количество скомпрометированных учетных записей в 2017 году увеличилось на 369%;
- среднемесячное количество утечек в 2017 г. составило 30,75;
- только в январе 2018 года биржи столкнулись с 212 утечками логинов и паролей;
- в январе 2018 года количество инцидентов взлетело на 689%, по сравнению с показателем 2017 года.

К концу 2016 года было обнаружено уже 139 утечек (Рис. 2).

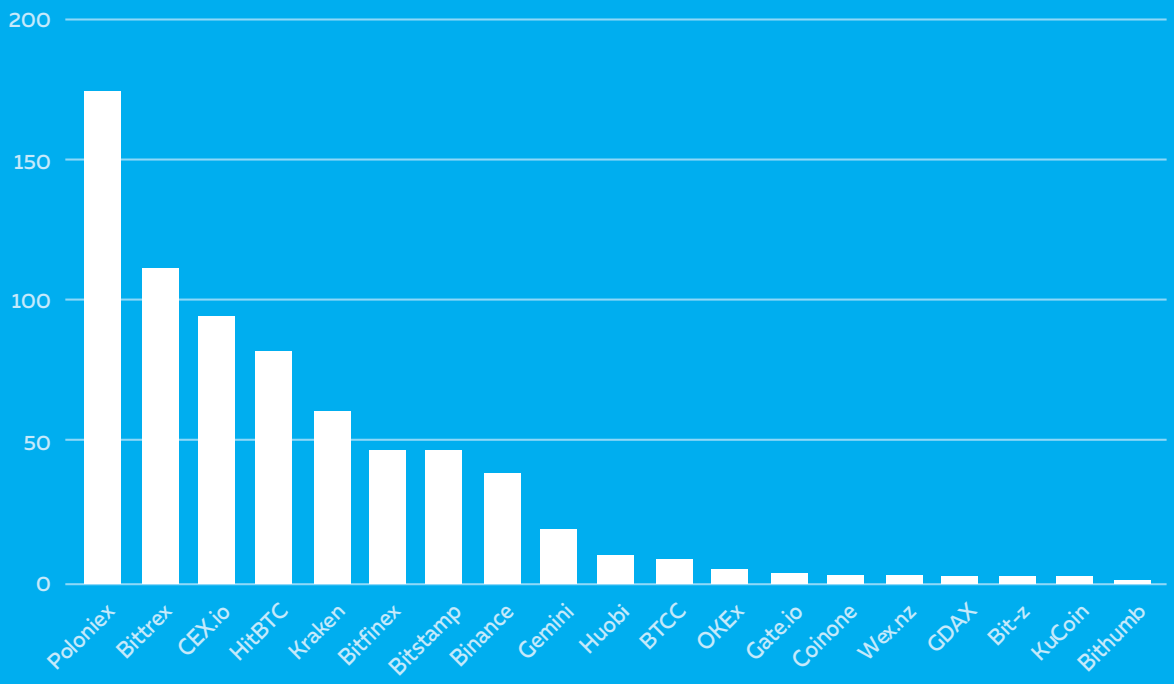


Рисунок 1: Распределение скомпрометированных учетных записей по биржам
Источник: Group-IB, 2018

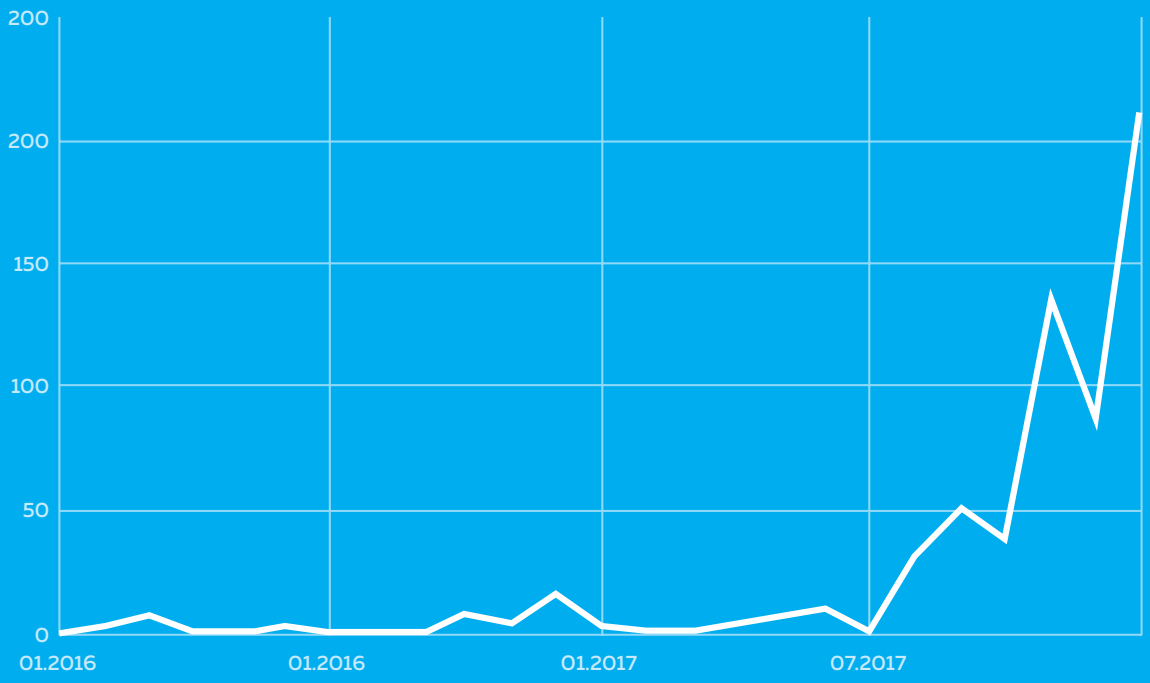


Рисунок 2: Количество утечек учетных записей по месяцам с января 2016 по январь 2018 гг.
Источник: Group-IB, 2018

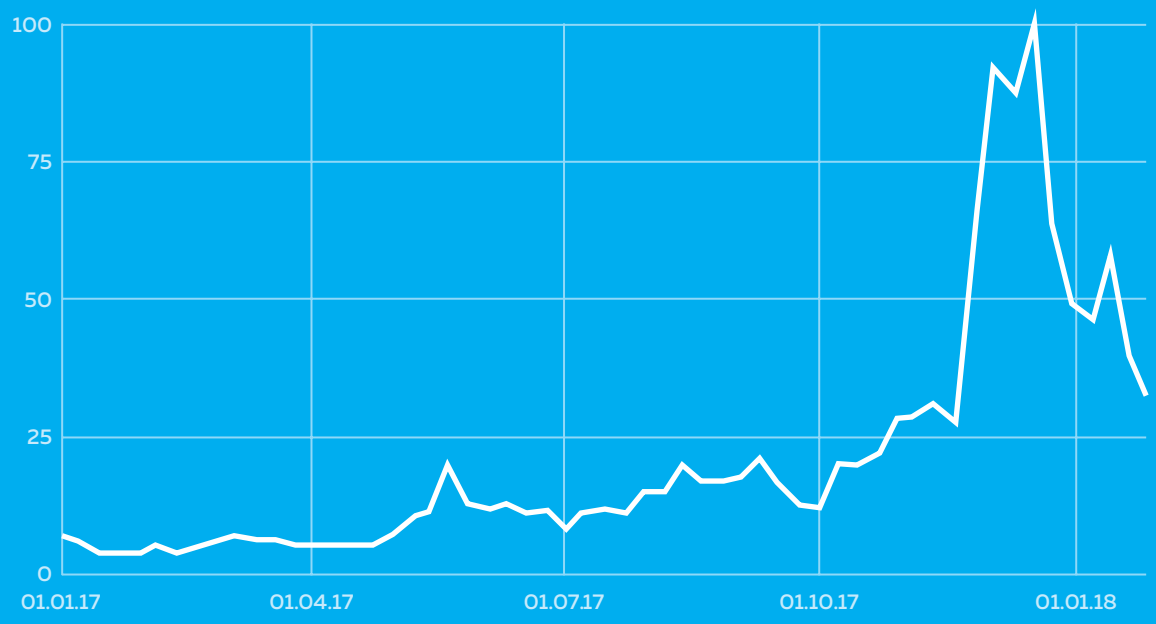


Рисунок 3: Динамика поисковых запросов слова «биткоин»
Источник: Google Trends [1]

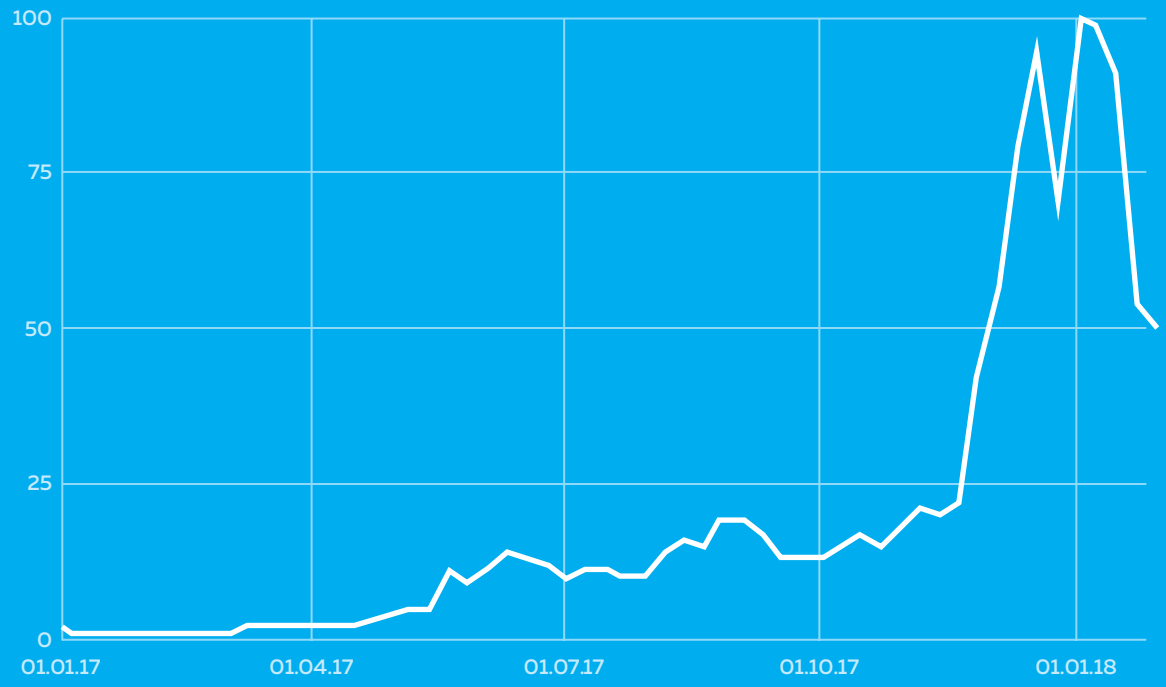


Рисунок 4: Динамика поисковых запросов слова «криптовалюта»
Источник: Google Trends [2]

3.3. ФАКТОРЫ, ПОВЛИЯВШИЕ НА РОСТ УТЕЧЕК

В первую очередь количество скомпрометированных учетных записей обусловлено ростом интереса к криптовалютам и блокчейн-индустрии. По данным Google Trends, интерес к криптовалютам достиг максимального значения в конце 2017 года.

По данным Google, поисковый запрос «биткоин» занял второе место среди самых популярных тем в международных новостях. В 2017 году эта тема стала популярнее ключевых геополитических и экологических проблем. Запрос “Как купить биткоин” попал в тройку популярнейших запросов в 2017 году [6].

***

В конце 2017 года были достигнуты рекордные показатели капитализации глобального рынка криптовалют. Таким образом, 3 января 2018 года общая стоимость мирового рынка криптовалют составила более $700 миллиардов, а 7 января 2018 года впервые в истории превысила $800 миллиардов. Такой показатель лишь немного меньше капитализации компании Apple на 8 января 2018 года, составившей $885 миллиардов.

В течение первой недели января капитализация криптовалют увеличилась примерно на $250 миллиардов (на 44%). В декабре 2017 года биткоин установил новый рекорд: его стоимость пробила потолок в $20 тысяч, тем самым в два раза превысив показатель, зафиксированный в конце ноября того же года ($10 тысяч).

TOP SEARCH QUERIES IN 2017

1. Hurricane Irma
2. Bitcoin
3. Las Vegas Shooting
4. North Korea
5. Solar Eclipse

Рисунок 5: Самые популярные поисковые запросы в 2017 г. Источник: Google Trends Global, 2017 [3]

Рост интереса со стороны широкой общественности привел к массовой регистрации на криптобиржах. В один момент количество пользователей криптовалютных бирж стало расти на более чем 100 000 заявок в день [7]. В середине декабря 2017 года биржа Kraken, в своем блоге сообщила об увеличении количества заявок от новых пользователей на 50 000 в день, а число новых заявок на техподдержку выросло на 10 000 в день [8].

Биржи отреагировали на подобную ситуацию введением ограничительных мер на количество пользователей, поскольку испытывали немалые трудности, пытаясь обеспечить ликвидность активов на бирже и ее техническое функционирование. В конце декабря 2017 года, по крайней мере, три биржи криптовалют – Bittrex, Bitfinex и CEX.io – запретили регистрацию новых пользователей [9]. В январе 2018 года биржа Binance была вынуждена прекратить регистрацию новых аккаунтов, так как всего за один час количество ее пользователей увеличилось на 240 000 человек [10]. Чжао Чанпэн, учредитель и генеральный директор Binance, сообщил в своем Твиттере о «слишком большом спросе» [11].

Некоторые биржи вводят суточный/недельный/месячный лимит на покупку и продажу: Bittrex (лимит на вывод – 100 биткоинов), HitBTC (суточный лимит на вклад и вывод – $10 тысяч), CEX.io (суточный лимит на вклад и вывод – $10 тысяч), Poloniex (лимит – $25 тысяч) и GDAX (суточный лимит на ввод и вывод – $10 тысяч).

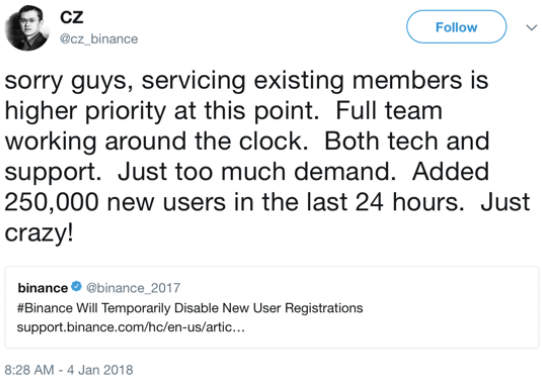


Рисунок 8: Пост Чжао Чанпэна, основателя Binance в Twitter

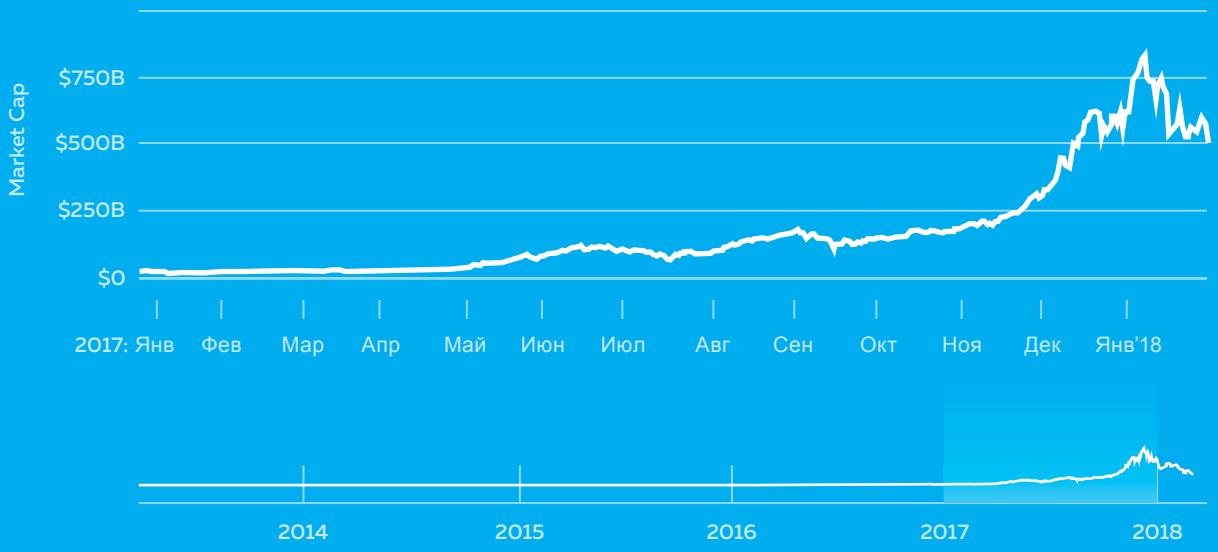


Рисунок 6: Общая капитализация криптовалютного рынка
Источник: coinmarketcap.com [4]

Рисунок 7: Стоимость биткоина (в долларах США)
Источник: coindesk.com [5]

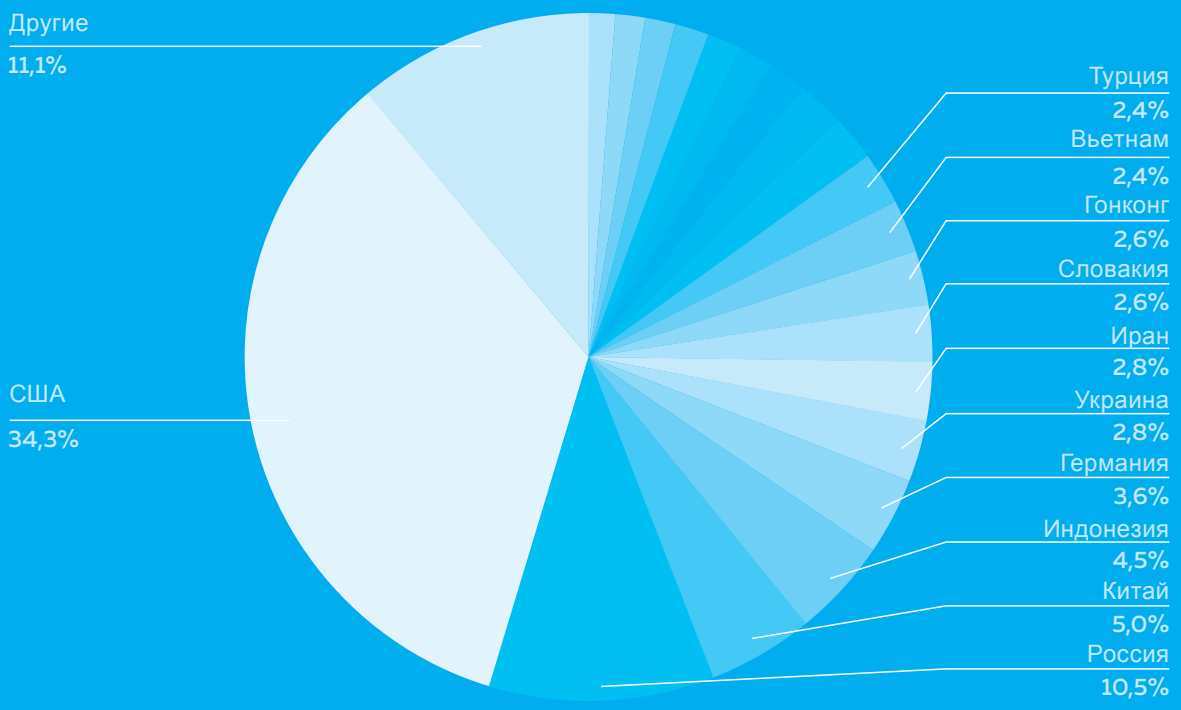


Рисунок 9: Распределение жертв по странам
Источник: Group-IB, 2018

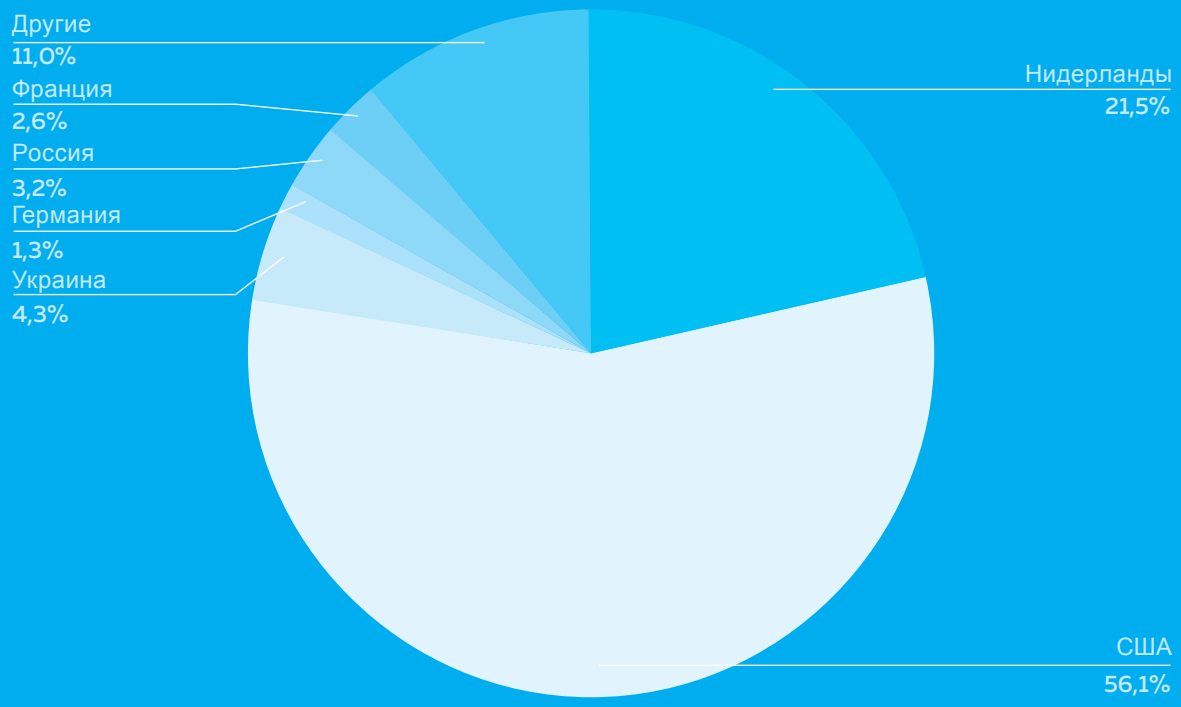


Рисунок 10: Страны, где располагаются C&C-серверы киберпреступников
Источник: Group-IB, 2018

3.4. РАСПРЕДЕЛЕНИЕ ЖЕРТВ ПО СТРАНАМ

Скомпрометированные учетные записи в нашей выборке принадлежат пользователям из всех стран мира. При этом выделяются три страны, которые пострадали больше всего, – это США, Россия и Китай, причем в США живет каждый третий пострадавший пользователь.

На Рис. 9 показаны страны, демонструющие наибольшую активность в индустрии криптовалют: большинство ICO-проектов в 2017 году было запущено в США и России [12].

***

При анализе географии хостов мы предположили, что киберпреступники использовали, так называемый, «bulletproof» хостинг – услугу, предлагаемую некоторыми хостинговыми компаниями и обеспечивающую клиентам весьма существенную свободу в отношении тех типов материалов, которые они могут загружать в сеть такого хостинга и распространять по ней.

Мы предполагаем, что в 3/4 случаев преступники используют инфраструктуру в США и Нидерландах по следующим причинам: местные хостинг-услуги относительно дешевы (как на легальном, так и на черном рынках), кроме того, эти страны представляют собой крупные инфраструктурные узлы, гарантирующие высокую скорость и надежность работы.

3.5. ИНФРАСТРУКТУРА КИБЕРПРЕСТУПНИКОВ

Мы выявили по меньшей мере 50 активных ботнетов, стоящих за атаками на пользователей криптовалютных бирж. Зараженные устройства управляются с различных IP-адресов (C&C), разбросанных по всему миру.

Географически инфраструктура киберпреступников, причастных к утечкам, распределена следующим образом:

- большинство хостов сконцентрировано в США (56,1%);
- второе место по популярности занимают Нидерланды (21,5%), затем идут Украина (4,93%) и Российская Федерация (3,2%).

Ряд IP-адресов в нашей выборке связан с прокси-сервисами, предназначенными для того, чтобы замаскировать истинное расположение C&C-сервера (например, Cloudflare, Blazingfast).

3.6. ВРЕДОНОСНЫЕ ПРОГРАММЫ

Ниже приведено несколько примеров вредоносных программ, которые использовались киберпреступниками для кражи учетных записей

3.6.1. AZORult

AZORult stealer известен с 2016 года, когда он впервые появился на черном рынке. При помощи этого вредоносного ПО преступники крадут пароли из известных браузеров и .dat файлов популярных криптокошельков.

Первые объявления о продаже AZORult были обнаружены на теневых форумах весной 2016 г. В 2017 г. была выпущена новая версия – "AZORult2".

Кроме того, в течение 2017 г. вышел ряд обновлений AZORult. Текущая версия обладает следующим функционалом.

- Кража паролей из браузеров, почтовых клиентов, FTP-клиентов, IM-клиентов.
- Кража cookie-файлов, данных из форм автозаполнения в браузерах.
- Кража данных банковских карт из браузеров типа Google Chrome.
- Получение .dat файлов из популярных криптокошельков; кража файлов из Skype и с рабочего стола жертвы
- Сбор информации о системе жертвы.

3.6.2. Pony Formgrabber

Pony Formgrabber используется киберпреступниками с 2012 г. Это вредоносное ПО предназначено для получения данных пользователей, использующихся при авторизации.

Сбор данной информации производится из файлов конфигурации, баз данных, тайных хранилищ более 70 программ на компьютерах жертв. После запуска вредоносное ПО начинает собирать информацию об операционной системе и ее основном языке, крадет логины и пароли пользователя и передает эти данные на соответствующий C&C-сервер.

К источникам информации могут относиться FTP-клиенты, веб-браузеры, пароли электронной почты (POP3, IMAP, SMTP), сертификаты электронной цифровой подписи, пароли для подключения к удаленному рабочему столу (RDP), dat-файлы (биткоин-ключи).

3.6.3. Qbot aka Quakbot

Qbot (также известный как Quakbot) – это сетевой червь с функциями бэкдора, в первую очередь, предназначенный для сбора логинов и паролей.

Данная программа может загружать файлы, удалять себя, заражать всю сеть, прерывать процессы в ОС. После заражения системы Qbot проникает в explorer.exe и браузер. Все украденные данные собираются и отправляются на FTP-серверы. Это довольно старая угроза, описанная специалистами Symantec в 2009 г.

В декабре 2015 г. исследователи сообщили, что сайты, на которых размещается набор эксплойтов Rig Exploit Kit, обслуживают обновленную версию Qbot. В январе 2016 г. Qbot заразил более 500 устройств в крупной государственной организации.

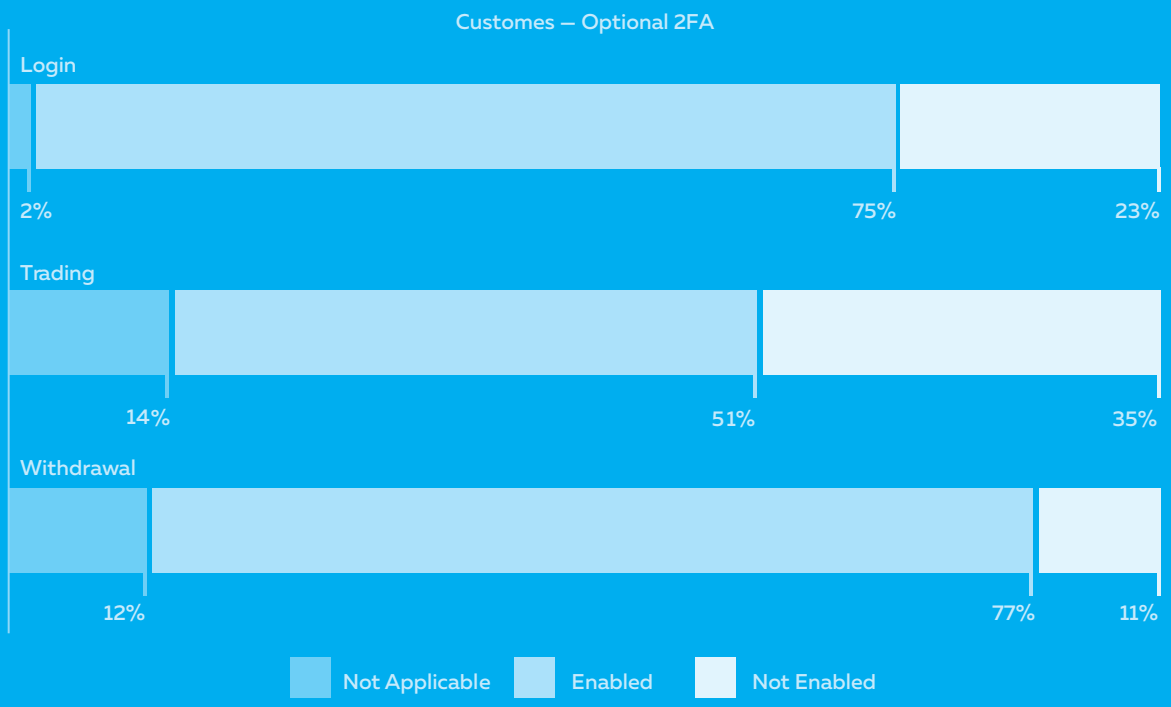


Рисунок 11: Биржи и их политика в отношении опциональной 2ФА
Источник: Кембриджский центр альтернативного финансирования, 2017

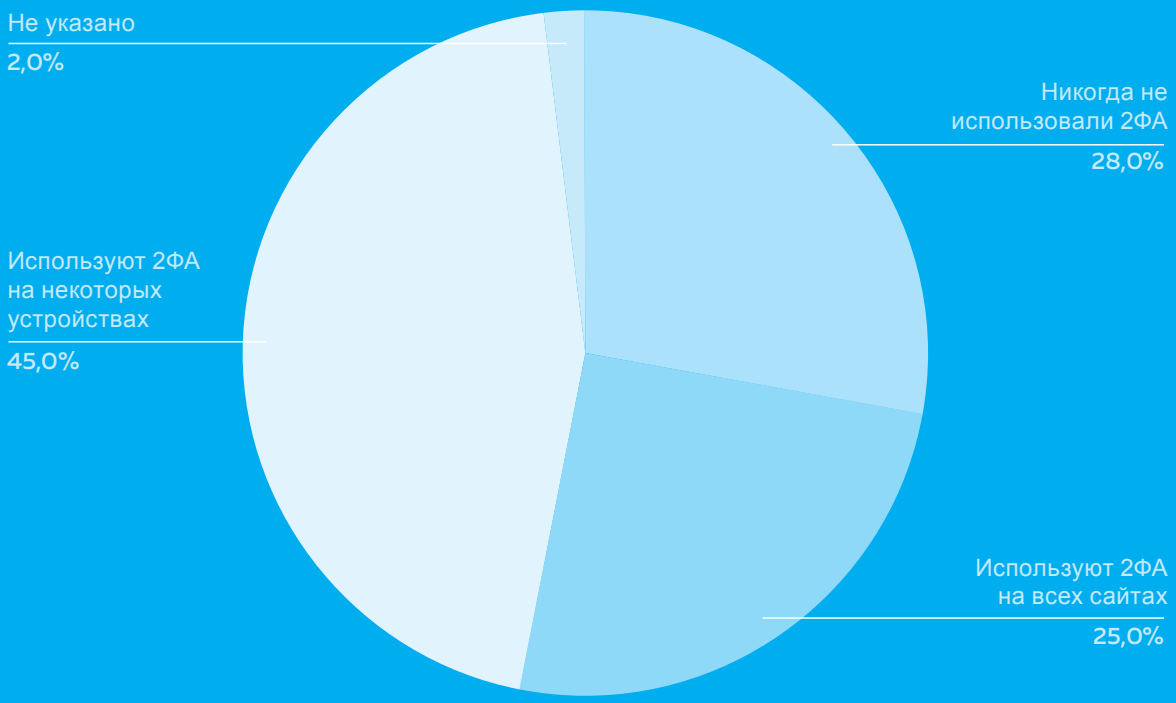


Рисунок 12: Использование 2ФА
Источник: Университет Мэриленда и Университет Джона Хопкинса, 2016 [14]

3.7. ПРИЧИНЫ УСПЕХА КРАЖИ

3.7.1. Отсутствие двухфакторной аутентификации (2ФА)

Утечка аутентификационных данных может привести к краже криптовалюты злоумышленниками. Одна из мер, позволяющих избежать финансовых потерь, – это использование второго фактора для подтверждения операции.

Согласно исследованию, проведенному Кембриджским центром альтернативного финансирования, 75% бирж предоставляют опциональную 2ФА для входа пользователей в свои аккаунты и лишь 23% считают ее обязательной. Только у 35% сервисов для проведения всех торговых операций обязательным условием является использование 2ФА и 11% обязуют своих пользователей использовать ее для вывода средств. Таким образом, меньше половины бирж считают активацию 2ФА обязательной минимальной мерой для предотвращения несанкционированного доступа к функциональным возможностям аккаунта, и большая часть предоставляет ее лишь в опциональном формате.

При этом существует зависимость между объемом торгов на бирже и необходимостью прохождения пользователями 2ФА при регистрации: функцию 2ФА предоставляет 80% крупных бирж и только 32% небольших [13]. Важно отметить, что 2ФА представляет собой опциональный элемент защиты, который большинство бирж предлагает своим клиентам, но при этом не требует от пользователей его обязательной активации.

3.7.2. В тех случаях, когда 2ФА доступна, пользователи, как правило, ее не используют

Согласно совместному исследованию Университета Мэриленда и Университета Джона Хопкинса [14], примерно 28% людей никогда не использовали 2ФА. При этом 64% из числа опрошенных впервые слышат об этом способе защиты и им никогда не предлагали ее использовать. Лишь 25% использовали 2ФА на всех устройствах и сервисах, где предлагалось, в то время как 45% опрошенных активировали эту функцию только для некоторых сервисов (Рис. 12). Такая статистика коррелирует с докладом Duo Labs [15], согласно которому лишь 28% людей используют 2ФА, а 56% респондентов никогда не слышали об этой функции.

В докладе, сделанном на конференции по безопасности USENIX Enigma 2018 в Калифорнии, инженер-программист из компании Google Гжегож Милка сообщил, что в настоящее время менее 10% активных аккаунтов в Google используют 2ФА для защиты своих сервисов [16].

3.7.3. Пользователи не используют надежные длинные пароли

Согласно докладу о расследованиях утечек, подготовленному специалистами компании Verizon, в 81% случаев хакеры получали доступ к данным, используя либо взломанные, либо ненадежные и легко угадываемые пароли[17]. По исследованию компании Dashlane, проведенному на основании протоколов паролей 35 ведущих криптовалютных бирж, было обнаружено, что более 70% площадок позволяют пользователям защищать свои учетные записи слабыми паролями. В исследовании указывалось, что тестеры смогли открыть торговые счета с паролями типа «12345», «пароль» или просто повторяющаяся буква. В выборке, состоящей из 720 учетных записей пользователей, анализ выборки показывает, что многие пользователи использовали пароли короче 8 символов (Рис. 13). Также было обнаружено, что нередко один и тот же пароль использовался для доступа к аккаунтам на различных биржах, что категорически не рекомендуется и несет прямую угрозу безопасности пользователя.

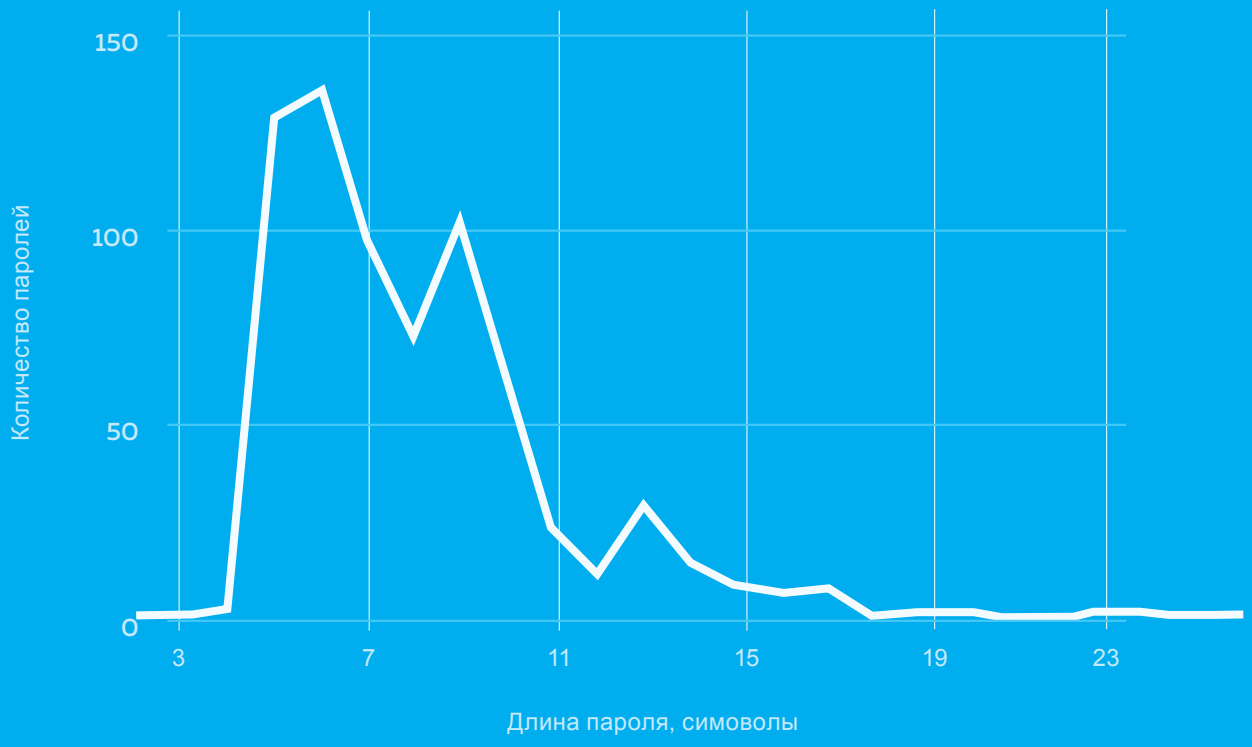


Рисунок 13: Длина украденных паролей
Источник: Group-IB, 2018

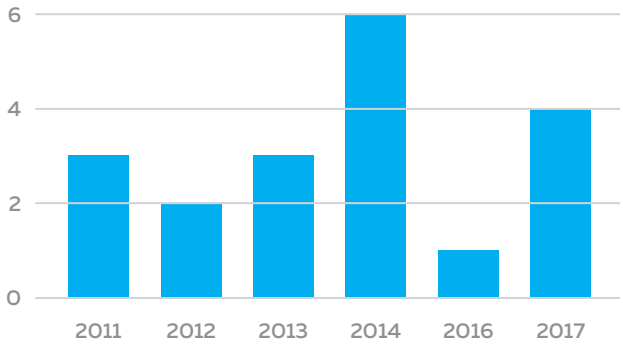


Рисунок 14: Распределение бирж по годам основания
Источник: Group-IB, 2018

3.8. Пострадавшие биржи и связанные с ними утечки данных

Сейчас нет такой площадки, которая бы обеспечила своим пользователям абсолютную безопасность. Пусть это крупная биржа с большой командой высокооплачиваемых инженеров и программистов или новичок на рынке. Как минимум пять из рассматриваемых в исследовании бирж криптовалют стали жертвами целенаправленных кибератак, широко освещаемых СМИ.

BITSTAMP
Дата: 4 января 2015
Ущерб: 19,000 BTC ($5,1 million)
Эта биржа, основанная в 2011 г. как альтернатива бирже Mt.Gox, тоже оказалась не самой безопасной. В январе 2015 года некоторые из "горячих" кошельков Bitstamp были взломаны, что привело к потере примерно 19000 BTC, эквивалентных $5,1 млн. Как показало расследование, за несколько недель до инцидента многие сотрудники Bitstamp стали жертвами фишинговой атаки. Файлы с вредоносным ПО были умело замаскированы под личные электронные письма и сообщения в Skype.

POLONIEX
Дата: 4 марта 2014
Ущерб: 12,3% от всех BTC (97 BTC)
Poloniex, одна из самых активных бирж, занимающихся торговлей биткоинами и альткоинами, была взломана летом 2014 г. Для кражи хакеры воспользовались ошибкой в исходном коде, которая позволила им вывести средства. Вскоре после взлома торги были приостановлены, а оператор объявил, что счета всех пользователей будут сокращены на 12,3%. Таким образом Poloniex распределила убытки, избежав панического вывода средств, в результате которого часть трейдеров могла полностью лишиться своих монет. [22].

HITBTC
Дата: в начале 2015
Биржа HitBTC была взломана примерно тогда же, когда BTER и Excoin. При этом руководство сервиса ничего не сообщило об объемах кражи и заявило, что средства пользователей она не затронула [21].

HUOBI
Дата: в конце 2015
По некоторым неофициальным источникам биржа Huboi так же была взломана. Пользователь под ником SpeedflyChris (на Reddit) обнаружил перевод 12 000 биткоинов с китайской биржи Huobi в 2015 году и выдвинул теорию о том, что она подверглась хакерской атаке. При этом руководство Huobi отрицает факт взлома и утверждает, что это была обычная операция [23] [24].

BITFINEX
Дата: 2 августа 2016
Ущерб: 120,000 BTC ($72 млн) [18]
Злоумышленники воспользовались неправильным использованием мультиподписей для кошельков Bitfinex и BitGo, считавшихся более надежными за счет создания нескольких приватных ключей, распределенных между доверенными лицами, поскольку для доступа к кошельку нужно подтверждение всех участников. В этом случае у Bitfinex осталось 2 ключа, а один хранился у BitGo. Но стало известно, что сервера BitGo не были взломаны, а значит они добровольно подписывали транзакции взломщика, и технология multi-sign по сути не была использована.

.

BITHUMB
Дата: 29 января 2017
Ущерб: больше $1 млн
Руководство Bithumb заявило, что хакеры, скорее всего, получили доступ к базе данных пользователей через компьютер одного из сотрудников биржи. Предположительно преступники получили доступ к именам, адресам электронной почты и номерам мобильных телефонов более чем 31 800 клиентов [19].


04

04—
Рекомендации

РЕКОМЕНДАЦИИ

Ответственность за обеспечение безопасности несут и биржи криптовалют, и их пользователи

4.1. Для пользователей

- Используйте надежные и сложные пароли.
- Используйте разные адреса электронной почты и пароли на разных биржах.
- Включайте двухфакторную аутентификацию везде, где это возможно.
- Старайтесь не использовать биржи, которые не предлагают двухфакторную аутентификацию.
- Поменяйте свое отношение – угроза реальна.
- Будьте очень внимательны и проверяйте все дважды.
- Старайтесь не использовать публичный Wi-Fi.
- Поддерживайте безопасность своих устройств и своевременно обновляйте используемое ПО.
- Следите за своим присутствием в сети Интернет.
- Не афишируйте, что у вас есть криптовалюта.

4.2. Для бирж

- Используйте двухфакторную аутентификацию и сделайте ее обязательной, а не опциональной.
- Регулярно проводите аудит защищенности ИТ-инфраструктуры биржи и связанных с ней сервисов.
- Выделяйте ресурсы на обучение и повышение осведомленности в области безопасности персонала, начиная от топ-менеджеров (фаундеров) и заканчивая рядовыми сотрудниками.
- Разработайте план оперативного реагирования на инциденты информационной безопасности.
- Используйте возможности киберразведки (Threat Intelligence).
- Внедрите системы антифишинга.
- Установите AntiAPT-решения как Group-IB Threat Detection System (TDS).

4.3. ЗАЩИТА ОТ МОШЕННИЧЕСТВА ДЛЯ КРИПТОБИРЖ

Предотвращение мошенничества для криптоиндустрии (Group-IB Secure Portal)

ТОЧНАЯ ИДЕНТИФИКАЦИЯ ЛЕГИТИМНЫХ ПОЛЬЗОВАТЕЛЕЙ

Передовые технологии аутентификации с точностью, близкой к распознаванию по радужной оболочке глаза.

Снятие отпечатков устройства - идентификация пользовательского устройства на основе его уникальных конфигураций.

Анализ поведения пользователя - идентификация пользователя на основе его уникальных особенностей поведения.

ОБНАРУЖЕНИЕ НОВЫХ ИНДИКАТОРОВ И СХЕМ МОШЕННИЧЕСТВА

Мы используем алгоритмы машинного обучения для обнаружения аномалий в поведении пользователей. Мы маркируем тех, кто связан с мошенничеством и добавляем новые параметры в прогностическую модель. Это позволяет нам постоянно обнаруживать новые мошеннические схемы в различных сеансах и учетных записях, а также уведомлять клиентов о злоумышленниках.

ВЫЯВЛЕНИЕ ПРИЗНАКОВ ПОДГОТОВКИ МОШЕННИЧЕСКИХ СХЕМ

Secure Portal использует уникальные данные от Лаборатории компьютерной криминалистики Group-IB и кибер разведки мирового класса Threat Intelligence Group-IB для обнаружения мошенничества на самых ранних стадиях и предупреждения об опасности до того, как будет нанесен ущерб.

ЗАРАЖЕННЫЕ УСТРОЙСТВА

IOCs и IMEI зараженных мобильных устройств мгновенно выявляют признаки получения удаленного доступа и вредоносной активности на устройстве пользователя.

- Легкий JavaScript модуль работает незаметно и не влияет на скорость загрузки страницы
- Все передаваемые для анализа данные анонимны, Secure Portal не имеет доступа кинформации ваших клиентов
- Облачный интерфейс с подробной информацией о подозрительных сеансах, статистикой и поиском
- API в реальном времени для мгновенного ответа

Больше информации:
www.group-ib.ru/secure_portal

05

05—
Авторы исследования

БЛАГОДАРИМ КОМАНДУ GROUP-IB THREAT INTELLIGENCE ЗА КОНСУЛЬТАТИВНУЮ ПОМОЩЬ И ПОДДЕРЖКУ

АВТОРЫ ИССЛЕДОВАНИЯ

Руслан Юсуфов
Директор специальных проектов

Елизавета Чаленко
Аналитик отдела по работе
с частными клиентами

06

06–
Методология

ИССЛЕДУЕМАЯ ВЫБОРКА СОСТОИТ ИЗ 720 УТЕЧЕК, КОТОРЫЕ ПРОИЗОШЛИ В 2014-2018 ГОДАХ И БЫЛИ СВЯЗАНЫ С 19 КРИПТОВАЛЮТНЫМИ БИРЖАМИ И СООТВЕТСТВУЮЩИМИ ДАННЫМИ

ПРИ ЭТОМ В ОБЛАСТЬ НАШЕГО ИССЛЕДОВАНИЯ ПОПАЛ ЦЕЛЫЙ РЯД КРУПНЕЙШИХ БИРЖ ПО ОБЪЕМАМ ТОРГОВЫХ ОПЕРАЦИЙ В ЯНВАРЕ 2018

МЕТОДОЛОГИЯ

Цель исследования – оценить количество утечек учетных записей с криптовалютных бирж и проанализировать характер этих инцидентов. В рамках проведенного исследования определены причины компрометации данных и даны рекомендации по защите от атак как биржам, так и пользователям. Объектом исследования являются скомпрометированные учетные записи пользователей криптовалютных бирж.

Исследуемая выборка состоит из 720 утечек, которые произошли в 2014–2018 годах и были связаны с 19 биржами криптовалют и соответствующими данными. При этом в область нашего исследования попал целый ряд крупнейших бирж по объемам торговых операций в январе 2018 года.

Наша исследовательская группа собрала данные по скомпрометированным учетным записям, полученные от Group-IB Threat Intelligence (см. Приложение 2).

Перед публикацией данного отчета каждой бирже была предоставлена возможность ознакомиться со всей полученной в результате исследования информацией, связанной с утечками данных их пользователей.

07

07—
Словарь

СЛОВАРЬ

Криптовалюта
Цифровая валюта, создание и контроль над которой основаны на использовании криптографических методов, а функционирование не зависит от центрального банка [25].

Вредоносная программа
Любое программное обеспечение, предназначенное для нарушения работы, причинения вреда или получения несанкционированного доступа к компьютерным системам [28], включая компьютерные вирусы, черви, трояны, программы-вымогатели, шпионские и другие вредоносные программы.

Командный сервер (C&C)
Сервер, который используется для удаленной отправки вредоносных команд и получения выходных данных с машин, входящих в состав ботнета, т.е. скомпрометированной сети компьютеров.

Ботнет
Сеть компьютеров, зараженных вредоносным программным обеспечением, управляемых киберпреступниками без ведома владельца – например, для рассылки спама [27].

Криптовалютная биржа/онлайн-сервис для обмена цифровых валют
Участник рынка, занимающийся обменом фиатных денег на электронную валюту или одной электронной валюты на другую. Онлайн-сервис обмена цифровых валют взимает за подобные операции определенную комиссию, а сами операции нередко проводятся именно через веб-сайты [26].

Кибербразведка (Threat Intelligence)
Основанные на фактических данных знания (включая контекст, механизмы, индикаторы, потенциальные последствия и практические рекомендации) о совершаемых или планирующихся атаках или рисках для определенных активов, которые могут использоваться для принятия информированных решений и проактивной реакции на эти угрозы [29].

08—
Приложения

ПРИЛОЖЕНИЕ 1: ОБЗОР БИРЖ КРИПТОВАЛЮТ

Название	Год	Торги 24H 31.01.18	Торговые пары	Число утечек	Инциденты с биржей
Binance	2017	$2 222 672 484	252	39	Нет
Bit-Z	2016	$236 374 114	69	2	Нет
Bitfinex	2012	$1 881 119 042	103	48	Да
Bithumb	2013	$1 783 489 020	12	1	Да
Bitstamp	2011	$514 697 740	14	48	Да
Bittrex	2014	$743 909 464	261	112	Нет
BTCC	2011	$103 530 000	4	9	Нет
CEX.io	2013	$53 713 354	23	95	Нет
Coinone	2014	$222 211 947	9	3	Нет
Gate.io	2017	$103 092 086	226	4	Нет
GDAX	2012	$926 158 460	12	2	Нет
Gemini	2014	$277 474 980	3	19	Нет
HitBTC	2014	$494 363 548	421	83	Да
Huobi	2013	$1 256 939 172	171	10	Возможно
Kraken	2011	$884 409 505	45	61	Нет
KuCoin	2017	$157 142 723	212	2	Нет
OKEx	2014	$2 701 097 580	422	5	Нет
Poloniex	2014	$383 900 716	99	174	Да
Wex.nz	2017	$69 440 237	35	3	Нет

Источник данных по торгам: coinmarketcap.com, объем торгов на 30 января 2018 г. [30]

Dashboard
Compromised data
Threats
Attacks
Hacktivism
Suspicious IP
Targeted malware
Brand abuse
Administration

Dashboard

Potential damage

Adjust estimates by altering the parameters used in the calculation by altering the numbers in the account settings section (gear icon)

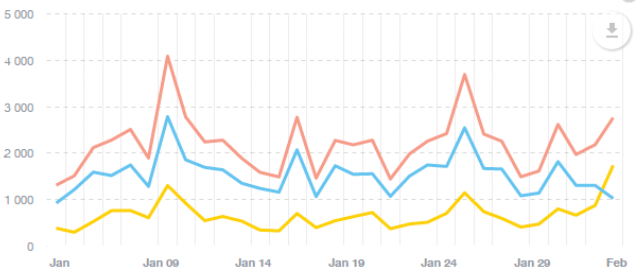
Range: 2017-01-04 - 2017-02-03

Total	Compromised Account Credentials	Phishing	Compromised Credit Cards
$40 023 625	7 891 $4 931 875	68 085 $33 560 250	12 252 $1 531 500
$108 000 ↑	1 908 ↑	-7 398 ↓	4 824 ↑

Phishing

Range: 2017-01-04 - 2017-02-03

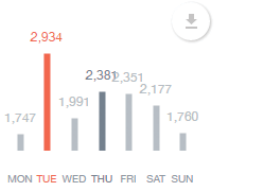
Malicious events · Events Blocked · Active events



68085 Phishing Identified

23 Average Take-Down time

29 Average Global Take-Down Time



Days of Highest Probability for Phishing Attacks

Malware

Malware targeting your business and your clients

for Windows · for Android

- Honli
- PONY FORMGRABBER
- Phishing
- Ramnit
- Gootkit

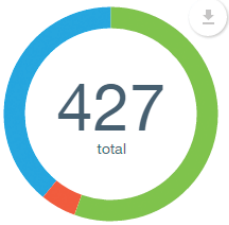
Details

Malicious e-mails

Range: 2017-01-04 - 2017-02-03

Distribution of drop email accounts capturing compromised credentials

gmail.com · yahoo.com



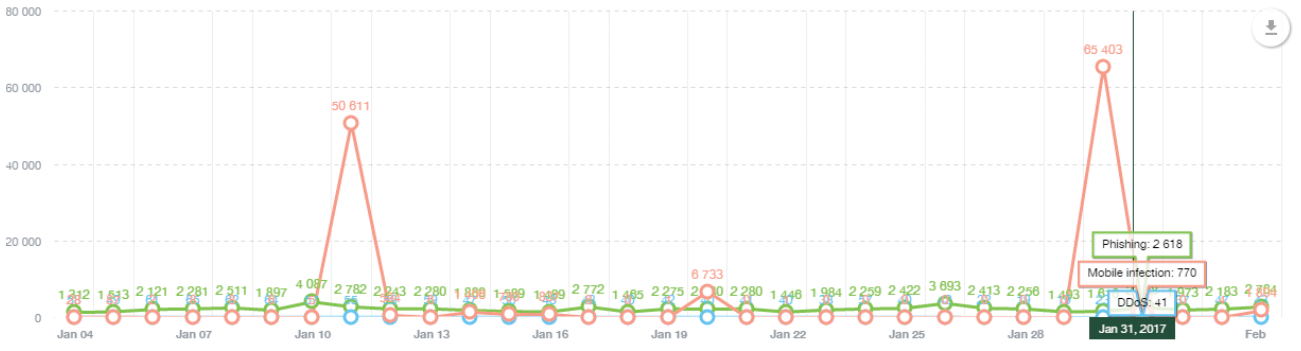
- admin@website.com
- supertool@mxtoolbox.com
- wirez@googledocs.org
- team_pbggggg@yahoo.com
- hahaha@ahaha.com

Details

Attacks

Range: 2017-01-04 - 2017-02-03

Phishing · DDoS · Mobile infection



Attacking Infrastructure

Range: 2017-01-04 - 2017-02-03

Phishing server · Phishing Kit email · Client location

ПРИЛОЖЕНИЕ 2: GROUP-IB THREAT INTELLIGENCE

Участвуя в расследованиях киберпреступлений с 2003 года, Group-IB сформировали базу данных о злоумышленниках и высокотехнологичную систему слежения за ними.

Наши эксперты узнают о будущих атаках на этапе подготовки инфраструктуры и заранее предупреждают клиентов Group-IB Threat Intelligence.

Информация об угрозах – жизненно важный компонент эффективной защиты бизнеса. Она позволяет предсказать атаки и готовиться к ним заранее, а не заниматься дорогим и длительным устранением их последствий.

Обрабатывая и анализируя данные из нескольких сотен источников, включая DarkWeb, мы предоставляем персонализированную, проверенную и значимую информацию, необходимую для подготовки к атакам и отражению актуальных угроз.

Технология Group-IB, основанная на запатентованных алгоритмах и машинном обучении, позволяет получать информацию, которая включает в себя данные не только о вредоносных программах или инфраструктуре киберпреступников - счета, банковские карты, международные идентификаторы мобильного оборудования (IMEI), но и о том - когда, где и как это было раскрыто.

Мы используем мониторинг в реальном времени и облачные сервисы, которые позволяют работать со статистикой, видеть и отслеживать тенденции, а также принимать эффективные решения на основе статистического анализа.

Больше информации:
www.group-ib.ru/intelligence

09—
O Group-IB

О GROUP-IB

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий; первый российский поставщик Threat Intelligence решений, вошедший в отчеты Gartner, IDC и Forrester.

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

1000+ успешных расследований по всему миру, из них 150 особо сложных дел

80% резонансных высокотехнологичных преступлений в России расследуется с нашим участием

3,3 млрд возвращено потерпевшей компании по результатам одного из наших расследований

$300 млн помогли сохранить нашим клиентам продукты системы раннего предупреждения киберугроз

Больше информации:
www.group-ib.ru

Команда Group-IB – это эксперты, обладающие уникальной квалификацией, с большим практическим опытом, подтвержденным международными сертификатами SSCP, CISSP, CISA, OSCP, CEH, CWSP, GCFA.

Миссия Group-IB: защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

GROUP-IB CRYPTO

Комплексная защита ICO, криптовалютных кошельков, бирж и обменников. Компания Group-IB начала заниматься обеспечением информационной безопасности для компаний криптоиндустрии с сентября 2017 года и защитила каждый 10-й доллар, привлеченный на ICO в рамках реализованных проектов.
Суммарно, за 4 месяца команда Group-IB помогла обеспечить защиту ICO на сумму порядка $300 млн за прошлый год.

На данный момент Group-IB успешно защищает ICO проекты как в России, так и на международном рынке.
Среди наших клиентов - Blackmoon, Tokenbox, BANKEX, WAVES и другие.

Больше информации:
www.group-ib.ru/crypto

Официальный партнер Europol и Interpol

Первый российский поставщик threat intelligence решений, вошедший в отчеты Gartner и Forrester

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

Лидер российского рынка исследования киберугроз по версии IDC

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Постоянный член Всемирного экономического форума


10

10—
Источники

ИСТОЧНИКИ

[1] Google Trends. Available at: https://trends.google.com/trends/explore?date=2017-01-01%202018-01-31&q=bitcoin (Accessed: February 2, 2018)

[2] Google Trends. Available at: https://trends.google.com/trends/explore?date=2017-01-01%202018-01-31&q=bitcoin (Accessed: February 2, 2018)

[3] Google Trends. Available at: https://trends.google.com/trends/yis/2017/GLOBAL/ (Accessed: February 2, 2018)

[4] CoinMarketCap. Cryptocurrency Market Capitalizations. Available at: https://coinmarketcap.com/charts/ (Accessed: February 2, 2018)

[5] Coindesk. Available at: https://www.coindesk.com/price/ (Accessed: February 2, 2018)

[6] Google Trends. Available at: https://trends.google.com/trends/yis/2017/GLOBAL/ (Accessed: February 2, 2018)

[7] Cointelegraph, Jan. 2018. "Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day". Available at: https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day (Accessed: February 2, 2018)

[8] Kraken Blog, Dec. 2017. "Degraded Service, Upgrade Next Week". Available at: https://blog.kraken.com/post/1399/degraded-service-upgrade-next-week/ (Accessed: February 2, 2018)

[9] UK Business Insider, Dec. 2017. "Some of the biggest crypto exchanges are shutting out new users because they can't keep up with demand". Available at: http://uk.businessinsider.com/crypto-exchanges-are-shutting-out-new-users-because-they-cant-keep-up-with-demand-2017-12 (Accessed: February 2, 2018)

[10] UK Independent, Jan. 2018. "Binance: World's top cryptocurrency exchange adds 240,000 users in just one hour". Available at: http://www.independent.co.uk/news/business/news/binance-bitcoin-latest-cryptocurrency-exchange-trading-users-increase-numbers-hong-kong-a8153496.html (Accessed: February 2, 2018)

[11] Changpeng Zhao Twitter. Available at: https://twitter.com/cz_binance/status/948954415662219264?lang=en (Accessed: February 2, 2018)

[12] EY & Group-IB, 2017. "EY Research: Initial Coin Offerings (ICOs)". Available at: http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf (Accessed: February 2, 2018)

[13] Cambridge Centre for Alternative Finance, 2017. "Global Cryptocurrency Benchmarking Study". Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf (Accessed: February 2, 2018)

[14] University of Maryland and Johns Hopkins University, 2016. "How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior". Available at: https://dl.acm.org/citation.cfm?doid=2976749.2978307 and https://www.umiacs.umd.edu/~mmazurek/papers/ccs2016-learned-secure.pdf (Accessed: February 8, 2018)

[15] Duo Labs, 2017. "State of the Auth. Experiences and Perceptions of Multi-Factor Authentication". Available at: https://duo.com/assets/ebooks/state-of-the-auth.pdf (Accessed: February 8, 2018)

[16] The Register, Jan. 2018. "Who's using 2FA?". Available at: http://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/ (Accessed: February 2, 2018)

[17] Verizon, 2017. "Data Breach Investigations Report". Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (Accessed: February 2, 2018)

[18] Fortune, Aug. 2016. "Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong". Available at: http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/ (Accessed: February 2, 2018)

[19] Fortune, July 2017. "One of the Biggest Ethereum and Bitcoin Exchanges Got Hacked". Available at: http://fortune.com/2017/07/05/bitcoin-ethereum-bithumb-hack/ (Accessed: February 2, 2018)

[20] Coindesk, July 2015. "Details of $5 Million Bitstamp Hack Revealed". Available at: https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/ (Accessed: February 2, 2018)

[21] CoinTelegraph, Feb. 2015. "3-Way Bitcoin Exchange Hack Dwarfed by 15-month $300 million Bank Heist". Available at: https://cointelegraph.com/news/3-way-bitcoin-exchange-hack-dwarfed-by-15-month-us300-million-bank-heist (Accessed: February 2, 2018)

[22] Coindesk, Mar. 2014. "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack". Available at: https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/ (Accessed: February 2, 2018)

[23] Steemit, Dec. 2017. "Attacked the Tether may be involved in other major hacks". Available at: https://steemit.com/bitcoin/@rollsman/attacked-the-tether-may-be-involved-in-other-major-hacks (Accessed: February 2, 2018)

[24] David Gerard Blog. Available at: https://davidgerard.co.uk/blockchain/2017/11/22/correction-huobi-wasnt-hacked-in-2015-but-the-2015-bitstamp-hacker-did-withdraw-12000-btc-from-huobi/ (Accessed: February 2, 2018)

[25] CoinMarketCap. Available at: https://coinmarketcap.com/exchanges/volume/24-hour/ (Accessed: January 31, 2018)

[26] Oxford Dictionaries. "Cryptocurrency". Available at: https://en.oxforddictionaries.com/definition/cryptocurrency (Accessed: February 2, 2018)

[27] Investopedia . "Digital Currency Exchanger - DCE". Available at: https://www.investopedia.com/terms/d/digital-currency-exchanger-dce.asp (Accessed: February 2, 2018)

[28] Oxford Dictionaries. "Botnet". Available at: https://en.oxforddictionaries.com/definition/botnet (Accessed: February 2, 2018)

[29] Oxford Dictionaries. "Malware". Available at: https://en.oxforddictionaries.com/definition/malware (Accessed: February 2, 2018)

[30] Gartner. "Threat Intelligence". Available at: https://www.gartner.com/doc/2487216/definition-threat-intelligence (Accessed: February 2, 2018)

[31] Dashlane, March 2018. "Cryptocurrency Exchange Password Power Rankings 2018". Available at: https://blog.dashlane.com/cryptocurrency-exchange-password-power-rankings-2018/ (Accessed: March 22, 2018)

11— Контакты

GROUP-IB
Международная компания, специализирующаяся на предотвращении кибератак

115088, Москва,
ул. Шарикоподшипниковская, д. 1,
БЦ «Прогресс Плаза», 9 этаж

121205, Москва, Большой бульвар, 42к1,
Технопарк "Сколково", 4 ядро, 4 этаж

+7 495 984-33-64
crypto@group-ib.ru
group-ib.ru/crypto

GROUP IB


GLOBAL CYBER SECURITY COMPANY
GIB
GLOBAL CYBER SECURITY COMPANY