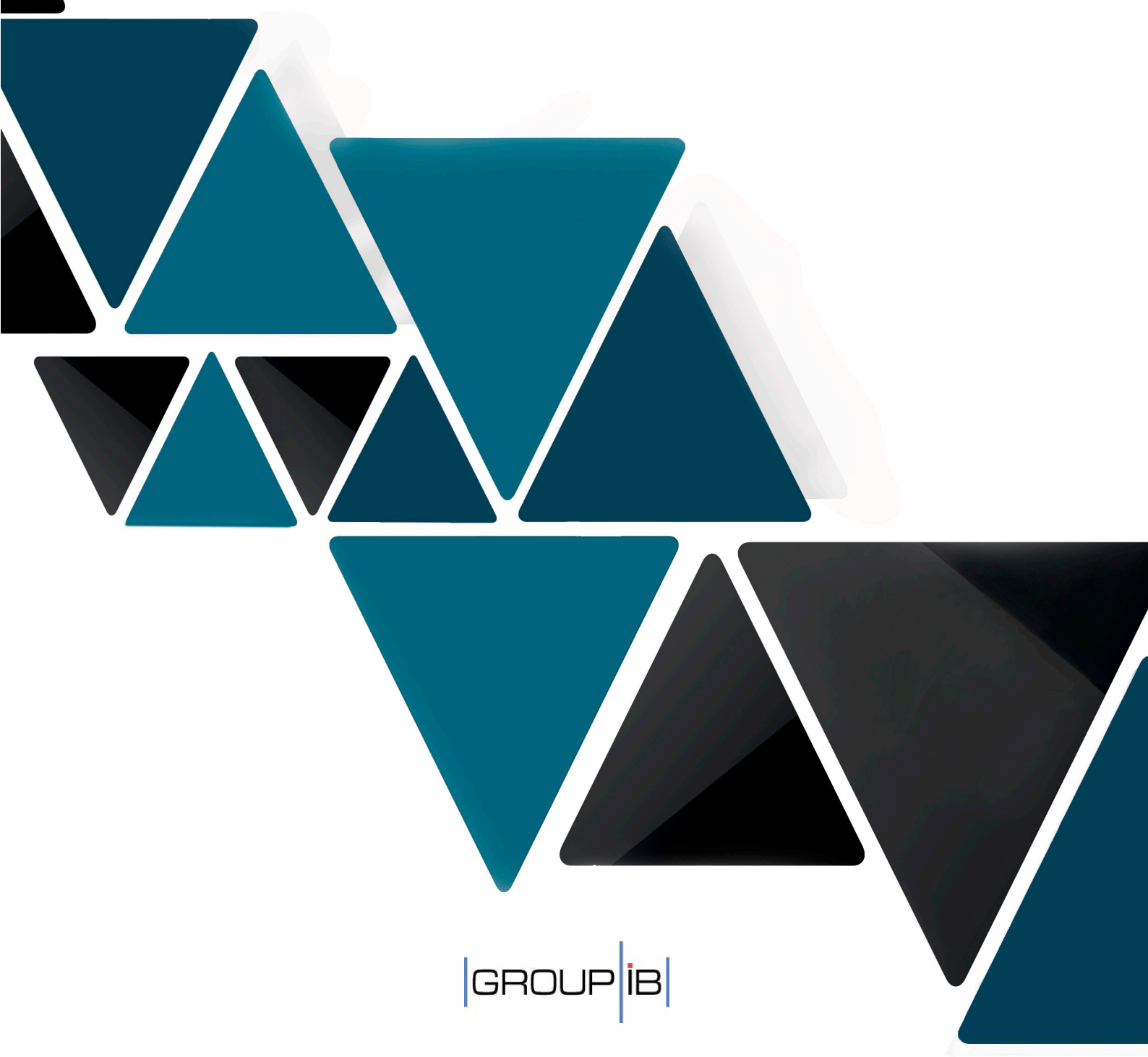
ОТЧЕТ GROUP-IB:

АТАКИ НА БРОКЕРСКИЕ И РАСЧЕТНЫЕ СИСТЕМЫ



GROUP IB

Резюме

В **феврале 2015 года** произошел первый в мировой практике крупный инцидент, когда троянская программа получила контроль над терминалом торговой системы для торгов на различных биржевых рынках, что привело к выставлению заявок на сумму более 400 млн долларов.

Используя вредоносное программное обеспечение, хакер применил инструмент «доллар/рубль расчетами сегодня» для продажи и покупки валюты от имени банка, что вызвало серьезные скачки курса доллара. За 14 минут хакер добился аномальной волатильности, что позволило покупать доллар за 55 рублей, а продавать по 62 рубля. До инцидента трейдеры торговались в рыночном диапазоне 60 - 62 рубля за доллар.

> Инцидент принес банку прямой многомиллионный ущерб и составил несколько сотен миллионов рублей

Для атаки использовалась вредоносная программа **Corkow** , также известная как Metel, которая имеет специальные модули для работы с трейдинговыми системами Quik от ARQA Technologies и TRANSAQ от ЗАО «Скрин маркет системз».

Сами мошеннические действия осуществлялись через терминал системы ИТС-Брокер от ООО «Платформа софт» через удаленный доступ, который и предоставил троян после определения, что с компьютера осуществляется работа с брокерскими системами.

> Сам факт мошенничества можно охарактеризовать как тестовую операцию, целью которой было подтвердить возможности оказывать серьезное влияние на рынок и, как следствие, заработать на этом.

В августе 2015 года произошел другой важный инцидент с использованием расчетной системы, объединяющей около 250 банков и позволяющей снимать средства с карт Visa и MasterCard по выгодным тарифам. Тогда через банкоматы одного из участников этой расчетной системы было выдано несколько сотен миллионов рублей, которые, как выяснилось позже, были результатом хакерской атаки с использование все того же трояна Corkow (Metel).

Специалисты Group-IB с помощью уникальной системы выявления угроз в корпоративной сети **Bot-Trek TDS** фиксируют наличие Corkow во многих банковских сетях России и единичные заражения на территории постсоветского пространства и Европы. По состоянию на начало 2015 года, **более 250 000 компьютеров** было заражено трояном Corkow и размер бот-сети ежедневно увеличивается. В том числе, было зафиксировано заражение более 100 финансовых организаций, в числе которых 80% из топ-20. После фиксации во многих банках были выявлены факты успешных денежных хищений.

Важно отметить, что на зараженном компьютере практически всегда установлена антивирусная защита популярных антивирусных производителей, а инфраструктура организации достаточно хорошо защищена системами обнаружения вторжений и другими техническими и программными средствами.

Учитывая способ распространения трояна, можно утверждать, что заражения имели случайный (нецелевой) характер. Однако, как показало наше предыдущее исследование по группе Anunak, наличие доступа на любой из компьютеров в корпоративной сети дает возможность получить доступ к самым защищенным банковским системам. Такая же ситуация была и с инцидентами с торговым терминалом и расчетной системой. Поэтому существует серьезный риск повторения этого инцидента и в других финансовых учреждениях не только в России, но и в любых других странах с похожей биржевой практикой (страны ЕС, Ближний Восток, Азия, США).

Corkow – это второй банковский троян, который использовался для сбора данных о трейдинговых системах. Интерес у хакеров к этому направлению ежегодно растет.

Выражаем большую благодарность в подготовке данного исследования компаниям Fox-IT, ESET и AVG.

Выводы:

- В феврале 2015 была проведена первая успешная атака на брокера, которая вызвала волатильность курса рубля в диапазоне от 55 до 66 рублей. Брокеру был причинен многомиллионный ущерб.
- Эта была тестовая атака демонстрирующая потенциальные возможности. На волатильности курса рубля заработали многие участники торгов, но не хакеры.
- В августе 2015 была проведена первая успешная атака с использование расчетной системы. Ущерб составил несколько сотен миллионов рублей.
- За атаками стоят русскоговорящие хакеры, использующие троян Corkow (Metel). Следы причастности спецслужб не выявлены.
- Хакеры из разных групп проявляют все больше интереса к возможностям проведения атак на брокеров и их клиентов, о чем свидетельствуют изменения во вредоносных программах.
- Основной целью хакеров являются компании России и СНГ, но с 2014 года фиксируется пятикратный рост детектов в США.
- Средства антивирусной защиты не способны эффективно противостоять этой угрозе. Во всех банках, где была зафиксирована эта вредоносная программа, был установлен и корректно работал антивирус. Вредоносная программа может находится в сети незамеченной более 6 месяцев.

Предыстория

Одними из первых бот-сетей, атаковавших пользователей трейденговой системы Quik была бот-сеть Ranbyus в 2012 году. Примеры интерфейсов панелей управления бот-сети Ranbyus разных версий показаны ниже. В каждой из них были созданы отдельные секции для изучения компьютеров, на которых была зафиксирована работа с брокерской системой Quik.

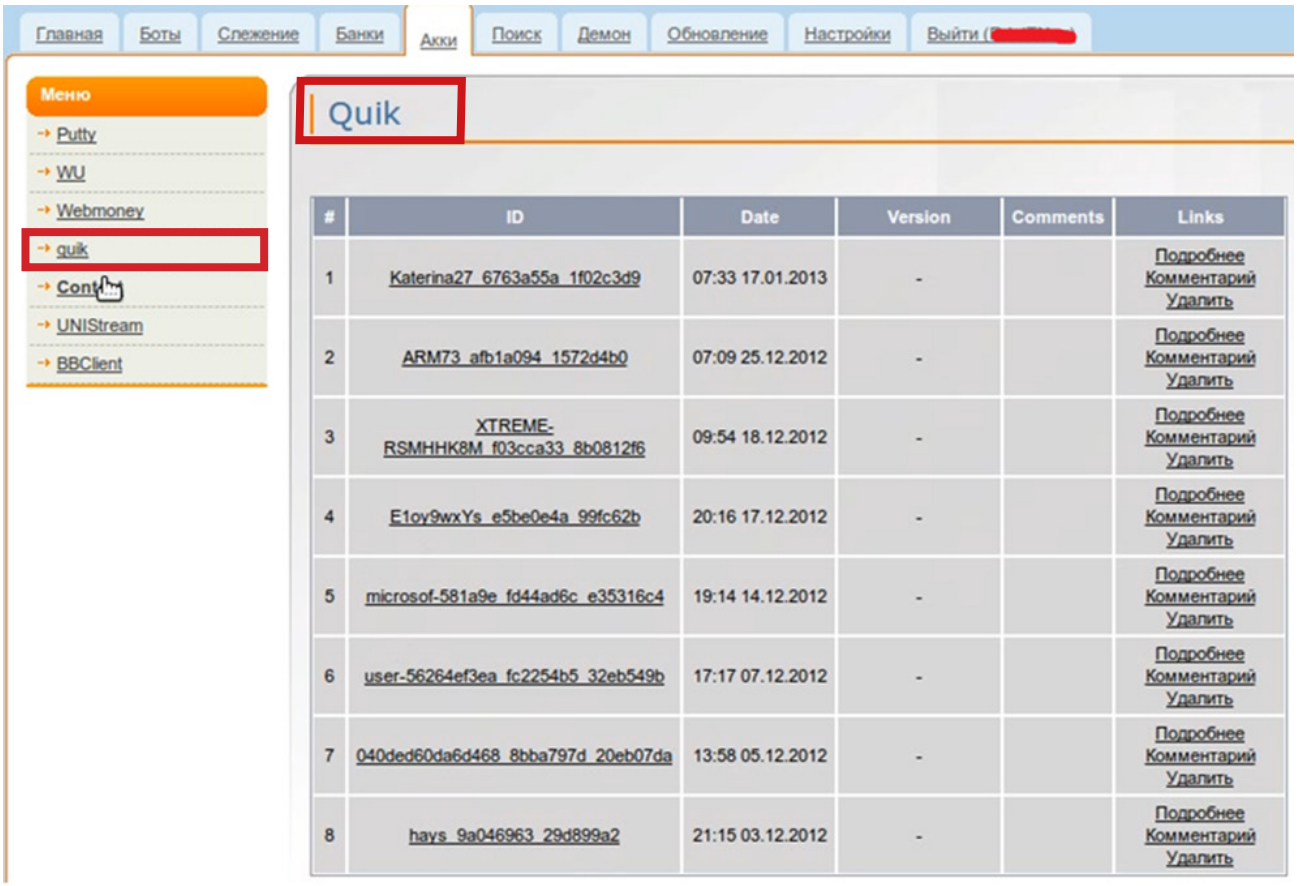


Рисунок 1. Панель управления Ranbyus с секцией Quik, осмотренная в январе 2013

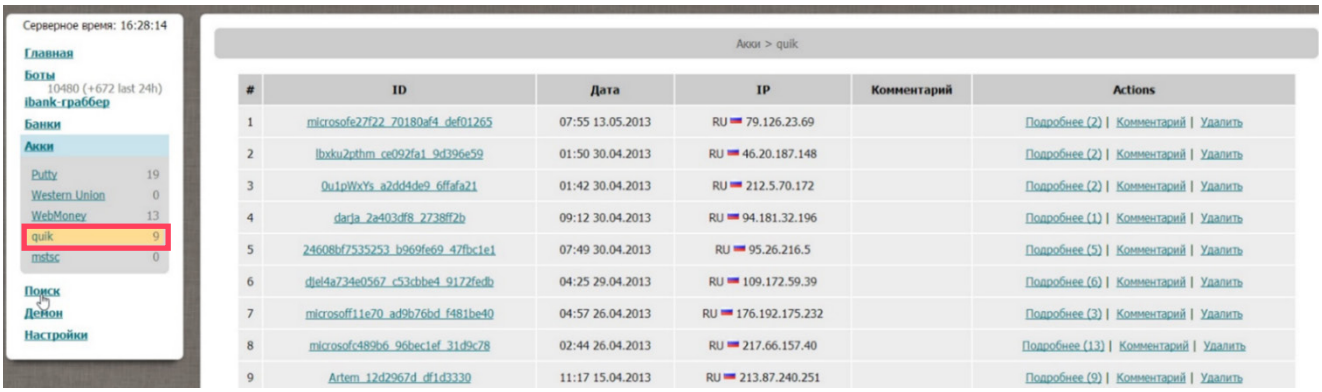


Рисунок 2. Панель управления Ranbyus с секцией Quik, осмотренная в мае 2013

В 2014 году Corkow имел модуль QUIK v.1.0. для сбора информации о трейдинговой системе Quik от ARQA Technologies. В 2015 году разработчики вредоносной программы Corkow обновили модуль QUIK до версии v.1.1. и выпустили еще один модуль TRZQ v.1.0. для копирования данных из приложения трейдинговой системы TRANSAQ от ЗАО «Скрин маркет системз».

Доработка старого модуля QUIK и разработка нового модуля TRANSAQ свидетельствует о повышении интереса со стороны злоумышленников к атакам на трейдинговые и брокерские системы.

Хронология атаки на брокера

Непосредственно атака длилась ровно 14 минут. И именно за эти несколько минут банку был нанесен ущерб. Однако, подготовка к атаке длилась гораздо дольше.

Хакеры попали на компьютер с торговой системой в сентябре 2014 года. С того самого времени она жила и постоянно обновлялась, чтобы избежать обнаружения средств антивирусной защиты, которые в банке были установлены и корректно работали. На момент исследования экземпляра вредоносной программы в марте, он не детектировался ни одним средством антиврусной защиты. На момент проведения исследования «Corkow.DLL» имел версию «7.118.1.1».

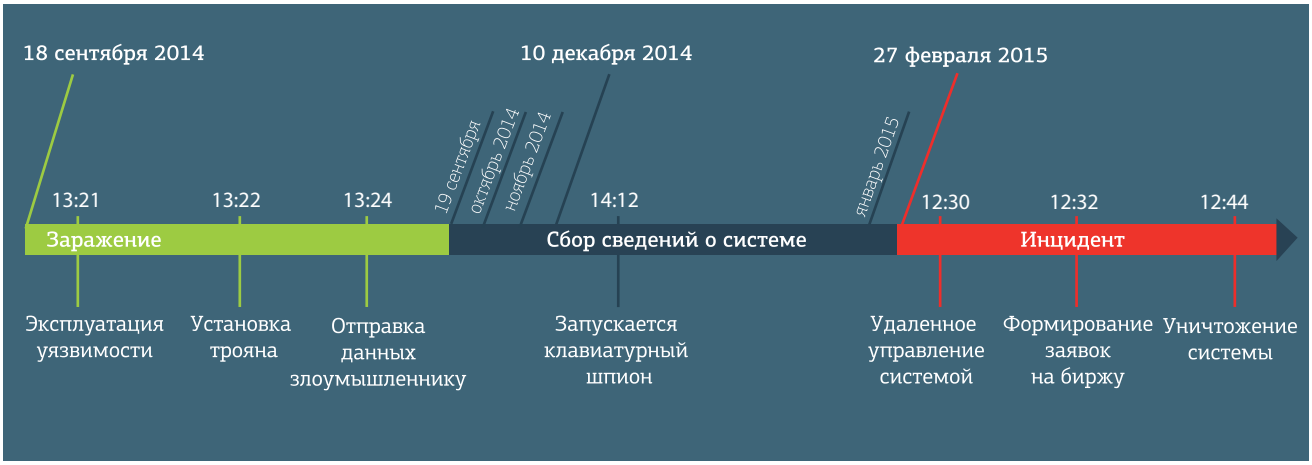


Рисунок 3. Хронология атаки

Начиная с декабря 2014 года на системе начинают создаваться отчеты клавиатурного шпиона.
В 27 февраля Corkow предоставляет удаленный доступ к системе, что позволило злоумышленнику запускать программы, управлять клавиатурой, мышкой параллельно с оператором системы.

В результате несанкционированного доступа к терминалу торговой системы злоумышленник, используя инструмент «доллар/рубль расчетами сегодня» совершил 7 сделок на покупку и продажу долларов США. Заявки имели следующий вид:

- тип заявки - «рыночный», что означает согласие купить или продать определенное количество лотов (определенный объем валюты) по лучшим ценам, зарегистрированным в Торговой Системе.

- тип заявки - «снять остаток», что означает исполнение заявки в максимально возможном объеме сразу же после ее регистрации в Торговой Системе, а ее остаток удаляется из Торговой Системы.

Рисунок 4. Технический анализ торгов

Было выставлено 5 заявок на покупку 437 миллионов долларов и 2 заявки на продажу 97 миллионов долларов. Однако, была исполнена только часть заявок и в результате было куплено 158 536 000 и продано 93 925 000 долларов США.

На графике по торгам в этот день отчетливо видна «свеча», показывающая разницу курса от 55 до 66 рублей.

Через 14 минут после первой заявки хакер дал команду Corkow на удаление своих следов и вывода системы из строя.

Рисунок 5. Данные инцидента

Результат атаки

Действия хакера вызвали очень большую волатильность в течение 6 минут, что позволило совершить сделку на покупку долларов по курсу 59,0560 и через 51 секунду продать по курсу 62,3490.

Чтобы обогатиться на специально спровоцированной разнице курса, злоумышленник должен был обладать большой суммой личных средств для проведения сделок. Например, при указанных выше курсах при наличии 22 миллионов долларов, он смог бы заработать только 72,4 миллиона рублей. Т.е. при такой схеме злоумышленник должен был вступить в сговор с кем-то из крупных клиентов брокерских систем, кто обладал необходимой суммой для покупки/продажи валюты. Такой сценарий возможен, но для злоумышленника было проще поступить иначе.

Имея в своем распоряжении ограниченное количество средств на покупку/продажу валюты по спровоцированному курсу, злоумышленники могли воспользоваться фьючерсным рынком, где мультипликатор на валютные сделки может достигать 20. Т.е. хакер мог увеличить величину открытой позиции в 20 раз, а свой капитал в 8 раз. В данной схеме злоумышленнику не надо вступать в сговор с крупными клиентами торговых систем, обладать значительно суммой денег.

Кроме того, на волатильности заработали не только мошенники, но и многие обычные клиенты биржи, и наибольшее внимание к себе привлекают именно они, а сделки на фьючерсном рынке моут пройти незамеченными. В итоге на этой махинации банк, чей терминал был скомпрометирован, понес большой финансовый и репутационный ущерб, поскольку многие игроки на рынке не доверяют версии со взломом и охотно все списывают на ошибку оператора торговый системы. Кроме ущерба, многие, кто торговал в тот момент на рынке, успешно заработали на скачке курса, но сам атакующий не заработал ничего. Все указывает на то, что данные действия были своеобразной проверкой и подтверждением возможности оказывать серьезное влияние на рынок и, как следствие, получение возможности заработать на этом.

Способы распространения вредоносной программы

Для распространения Corkow злоумышленники активно использую метод Driveby, который заключается в распространении вредоносных программ при взломанных посещении легитимных сайтов. В качестве набора эксплойтов используется Nitris Exploit Kit, (ранее известный как CottonCastle), который не продается в открытом доступе и предоставляется только проверенным покупателям. Сам набор эксплойтов хорошо описан в блоге Malware don't need Coffee.

Мы фиксировали распространении Corkow при посещении сайтов разной тематики: отслеживание почтовых переводов, новостные порталы, электронные книги, сайты компьютерной графики, музыки и т.д. Явно выраженной тематики сайтов не выявлено, что говорит о том, что злоумышленники хотят охватить максимальную аудиторию, а не только корпоративный сектор.

Наши сенсоры Bot-Trek TDS стоят во мнигих финансовых учреждениях и, к сожалению, мы видим, что в 80% банков троянская программа Corkow присутствует в защищенной корпоративной сети. Учитывая способ распространения трояна и исследования обстоятельств заражений банковских сетей можно утверждать, что все заражения имели случайный характер. Однако, как показывало наше предыдущее исследование по группе Anunak, наличие доступа на любой из компьютеров в корпоративной сети дает возможность получить доступ к самым защищенным банковским системам.

Ниже представлен список сайтов, при посещении которых пользователям загружался троян Corkow.

> Общая посещаемость указанных сайтов более 800 тысяч пользователей в сутки. Средний коэфициент заражений для Nuclear Exploit Kit составляет 11%, что означает, что хакеры могли ежедневно заражать около 90 тысяч компьютеров, таким образом, быстро увеличивая размер своей бот-сети.

Название сайта	Категория	Средняя посещаемость в сутки
post-tracker.ru	Почта	38 478
zr.ru	Автомобили	112 271
business-gazeta.ru	Новости	68 746
proshkolu.ru	Образование	47 249
opengost.ru	Государственные стандарты	8 545
krokha.ru	Женский портал	-
eurolab.ua	Медицина	156 552
newsdon.info	Новости	40 614
dirt.ru	Спорт	7 100
anime-zone.ru	Мультфильмы	4 297
rus.kg	Новости	936
badger.ru	Магазин	-
fedpress.ru	Новости	25 804
carsguru.net	Объявления	52 157
findfood.ru	Кулинария	56 307
beboss.ru	Объявления	4 863
vidal.ru	Медицина	25 678
reghelp.ru	Объявления	10 339
rabotagrad.ru	Объявления	5 581
proshkolu.ru	Объявления	-
muztorg.ru	Магазин	26 332
mirf.ru	Журнал	5 226
medgorodok.ru	Медицина	8 696
dobrota.ru	Медицина	-
cooksa.ru	Кулинария	19 929
consmed.ru	Медицина	32 712
buro247.ru	Мода	-
3dmir.ru	Компьютерная графика	2 508
novorus.info	Новости	40 614
kidbe.ru	Женский портал	14 778
eknigi.org	Электронные книги	-
2x2.su	Объявления	-

Таблица 1. Список сайтов, при посещении которых пользователям загружался троян Corkow.

Территория распространения

По статистике обнаружений в разные периоды времени видно, что Corkow используется для атак по пользователям России и стран СНГ, однак стоит отметить, что с 2014 года фиксируется рост обнаружений в США в 5 раз. Более того, количество обнаружений Corkow в первом квартале 2015 года в США превышает количество обнаружение в странах СНГ.

Country	2011	2012	2013	2014	Q1 2015
Russia	61425	132327	19156	26493	4719
Ukraine	7076	9891	4558	6108	883
Belarus	2748	1892	584	82	18
Kazakhstan	1132	1997	254	43	22
Turkey	762	453	27	100	79
Spain	457	164	30	160	26
Italy	238	115	375	131	43
Mexico	209	362	33	82	44
Peru	191	167	5	123	35
Poland	181	86	28	94	33
United States	164	102	49	534	159
Chile	114	192	52	36	11
Thailand	114	51	8	204	97
Argentina	107	65	6	31	16
Germany	107	23	30	82	26
Greece	91	42	22	59	14
Brazil	89	69	10	43	32
France	81	65	10	79	44

Таблица 2. Статистика детектов трояна Corkow по годам и странам

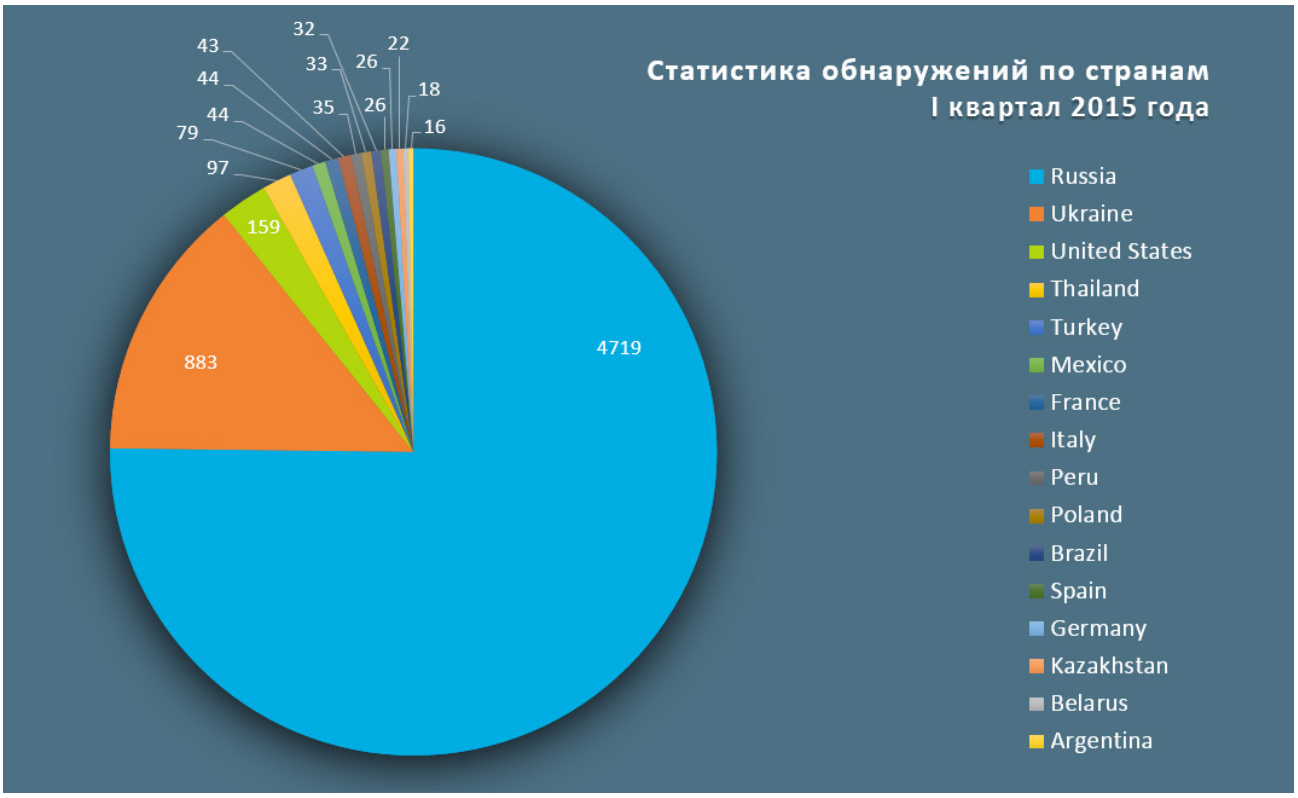


Рисунок 6. Статистика обнаружений по странам за 1 квартал 2015 года

Тактика действий

После активного распространения через набор эксплойтов Niteris атакующий осуществляли поиск среди ботов тех, которые были установлены в банковских сетях. Проверку на принадлежность к банковский сети делали по IP-адресу, журналам перехватчика паролей и результатам работы модулей под трейдинговые системы.

Далее на интересующих ботов загружалась дополнительная программа для удаленного управления. Кроме легитимного «Ammy Admin» атакующие использовали «Visconti Backdoor», который создан на базе легитимного софта типа RMS (remote manipulator system), распространяется на русскоговорящих хакерский форумах и предоставляет злоумышленнику следующие функции:

- Скрытая установка на машину жертвы, закрепление в системе как легитимное ПО;
- Просмотр рабочего стола, запись экранного видео и аудио (возможно по установленному расписанию);
- Кейлоггер;
- Удаленный доступ к диспетчеру задач, просмотр имеющихся процессов и служб, возможность останавливать их;
- Получение данных о технических параметрах машины жертвы и операционной системы;
- Выполнение команд в CMD;
- Удаленный запуск файлов и приложений на машине жертвы;
- Получение файлов, буфера обмена с компьютера жертвы;
- Скрытое удаленное подключение от имени учетной записи жертвы (RDP);
- Удаленный редактор реестра;
- Возможность дать компьютеру жертвы команду на выключение, перезагрузку, спящие режим, отключение монитора;
- Обход UAC;
- Работа на любых версиях Windows (с XP до 10), как 32-bit, так и 64-bit;
- Самоудаление из системы жертвы.

Используя удаленный доступ хакеры начинали исследование внутренней сети с целью выявления интересующих серверов. Для получения логинов и паролей использовались кейлоггеры встроенные в Corkow, а также уже хорошо известный инструмент Mimikatz позволяющий извлекать учётные данные Windows из LSA в открытом виде.

Также атакующие применяют разные сканнеры для поиска внутри корпоративной сети хостов с работающими VNC и Radmin сервисами.

При попадании на рабочее место оператора какой-либо банковской системы производилась установка Corkow, который фиксировал работу оператора путем создания снимков экранов и фиксированием нажатий клавиш встроенным клавиатурным шпионом.

Описание вредоносной программы

Исследуемый файл представляет собой библиотеку, способную производить загрузку и исполнение файлов, находящихся на удаленном сервере, удалять файлы, перезагружать и нарушать работоспособность ЭВМ пользователя, собирать данные об ЭВМ, пользователе и его действиях (нажатия клавиш и снимки экрана), а также отсылать эту информацию на различные адреса. Также исследуемая программа предоставляет сервер удаленного доступа к ЭВМ.

Библиотека содержит модули, список которых представлен в таблице 1. Имена модулей и их версий получены при распаковке библиотеки в динамическую память.

Модуль	Версия	Описание
MON	1.9.0	Собирает информацию о ЭВМ, пользователе, ОС и отслеживает запущенные процессы.
KLG	1.3.1	Ведет журнал всех нажатых клавиш.
HVNC	2.0	Модуль удаленного доступа к ЭВМ.
FG	2.0	Ведет журнал посещаемых сайтов в контексте браузера и сохраняет данные авторизации.
QUIK	1.1	Модуль для копирования данных из приложения трейдинговой системы Quik.
IB2	1.3.1	Модуль для копирования данных из приложения «IBank2»
SBRF	1.3.8	Модуль для копирования данных из приложения «Wclnt.exe»
AMY	1.4	Модуль встроенной программы для удаленного управления «Ammy Admin»
iFOBS	1.6	Модуль для копирования данных из приложения «iFOBSClient.exe»
TRZQ	1.0	Модуль для копирования данных из приложения трейдинговой системы TRANSAQ

Таблица 3. Модули «Corkow.dll»

Основной функционал

- Дешифрование и загрузка дополнительных модулей в сторонние процессы. Процесс поиска подходящего процесса для внедрения запускается в отдельной потоке, который в бесконечном цикле просматривает запущенные процессы.
  - Модуль FG внедряется в процессы, содержащие в своем имени следующие подстроки: «firefox.exe»,
    «iexplore.exe», «chrome.exe», «opera.exe», «browser.exe», «iTunes.exe»;
  - Модуль QUIK внедряется в процесс, содержащий в имени подстроку «info.exe»;
  - Модуль TRZQ внедряется в процесс, содержащий в имени подстроку «transaq.exe»;
  - Модуль SBRF внедряется в процесс, содержащий в имени подстроки «wclnt.exe», «ip-client.exe»;
  - Модуль «iFOBS» внедряется в процесс, содержащий в имени подстроку «iFOBSClient.exe»
  - Модуль «IB2» внедряется в процессы, содержащие в своем имени следующие подстроки: «java.exe»,
    «javaw.exe»
- Модуль MON распаковывается в памяти и запускается в виде отдельного потока;
- Модуль HVNC распаковывается в памяти и запускается в виде отдельного потока;
- Модуль FG в контексте процесса осуществляет перехват функций, собирает информацию о нажатых клавишах, посещенных вебсайтах и данных авторизации. Полученную информацию шифрует и записывает в файл, указанный в разделе «Работа с файловой системой»;
- Модуль MON собирает информацию о запущенных процессах. Периодически получается информация о запущенных процессах (имя файла, статус защищенности, получаемый при помощи функции «SfcIsFileProtected»), пользователь, запустивший процесс, уникальный номер процесса, аргументы запуска), а также последний пользовательский ввод, получаемый при помощи функции «GetLastInputInfo»), и отправляется на удаленный сервер, при этом при каждой отправке указывается текущее время. Имеет функционал по созданию снимков экрана;
- Модуль «iFOBS» собирает информацию о данных приложения для ДБО «iFOBS». Может создавать снимки экрана и копировать ключевую информацию.
- Модуль «SBRF» собирает информацию о данных приложения для ДБО «Сбербанк Онлайн».
- Модуль QUIK внедряется в процесс, содержащий подстроку «info.exe». Данный модуль предназначен для сбора данных программы QUIK, предоставляющей интерфейс доступа к различным фондовым рынкам электронных бирж. Копирует данные файлов для отправки на сервер:
  - «Login.data»
  - «qrypto.cfg»
  - «ClientInfo.txt»
  - «limits.dat»
  - «ip.cfg»
  - «info.ini»
  - «ka_pr.ini»
  - «qcrypto.ini»
  - «randseed.bin»
  - «quik.txk»
  - «Pubring.txk»
  - «Secring.txk»

А также файлы ключей из папки «/Keys» директории программы.

- Модуль HVNC содержит функционал предоставления удаленного управления компьютером, на котором запущена исследуемая программа. Удаленное управление предоставляется путем создания сессии удаленного пользователя и дополнительного рабочего стола ОС Windows. Таким образом, действия, производимые посредством данного модуля, будут скрыты от пользователя компьютера. После распаковки и запуска модуля сообщает на управляющий сервер информацию о ЭВМ, пользователе, ОС и номер версии модуля.

- Модуль AMY содержит функционал по запуску программы «Ammy Admin» с аргументами –service и –nogui и передаче конфигурации программы на удаленный сервер. При наличии конфигурации запущенной программы злоумышленник может подключиться к ЭВМ и управлять ей удаленно.

- Получение информации об аппаратных электронных ключах. Для этого исследуемая программа производит перечисление всех подключенных к ЭВМ USB устройств и поиск среди них следующих имен:

Rutoken Magistra; USB Token Device; USB Token; USB_Token; USB-Token; Token; VPNKey; VPN Key; VPN-Key; VPN_Key; ICCD USB-Token; BIFIT ICCD; BIF IT-ICCD; BIFIT_ICCD; ICCD_USB_Token; EZCCID; Smart Card Reader.

- Скачивает и сразу удаляет файлы из таблицы 3. Предположительно, делается это в целях затруднения анализа сетевого трафика и скрытия запросов к командным серверам.

- Периодически отправляет собранную информацию от модулей на командный сервер.

Имеется функционал по добавлению исследуемого файла в автозагрузку путем модификации реестра.

Отправляемые данные

Corkow отправляет информацию о своем статусе на удаленный командный сервер (C&C) через http POST запрос. Список управляющих серверов жестко прописан в коде каждого семпла. На усправляющий сервер отправляются строки вида:

<Machine GUID>.<дата установки ОС>.<серийный номер тома диска %SYSTEMDRIVE%><|><версия corkow.dll><|><разрядность ОС><|>1<|><версия ОС>

s=<текущее время >
tzb=<часовой пояс >
cdi=<разница между двумя вызовами API функции time>
rsi=<разница между двумя вызовами API функции time>
on=<разница между двумя вызовами API функции time>
lng=<язык ОС, возвращенный API GetSystemDefaultUILanguage >
plds=<список модулей и их версии>
hp=<название исполняющего процесса>
un=<имя учетной записи пользователя>
clr=<версия установленного .NET>
svi=<серийный номер тома диска %SystemDrive %>
mst=<время >
bst=<время >
hpid=<номер процесса PID>
hpst=<время создания процесса, полученного при помощи API GetProcessTimes >
bts=<разрядность>
dbgi=<настройки с именем DebugInfo>
lbr=<настройки с именем LastBadReply>

В ответ бот может получать команды. Полный список исполняемых команд представлен ниже.

Команда	Аргументы	Назначение
NOP	-	Не выполнять никаких действий.
Reboot	-	Принудительная перезагрузка ЭВМ пользователя.
Wipe	-	Удаление файлов без возможности их восстановления.
	Path	Путь, определяющий файл для удаления.
	Mask	Маска файлового поиска, определяющая файлы для удаления.
SelfRemove	-	Удаление исследуемой программы.
	DestroySystem	Флаг, определяющий необходимость нарушения работоспособности ЭВМ пользователя после удаления исследуемой программы. При активном флаге будет осуществлена попытка удаления файлов, приведенных в приложении 1 а также перезапись MBR.
CfgWrite	-	Изменение параметров конфигурации исследуемой программы.
	PayloadID	Идентификатор библиотеки.
	Section	Раздел конфигурации.
	Param	Имя параметра.
	Value	Значение параметра.
Update	-	Обновление исследуемой программы.
	Url	Сетевой адрес загружаемого модуля обновления.
	Version	Версия загружаемого модуля обновления. В случае ее значение ниже таковой у исследуемой программы, обновление произведено не будет.
	LoadImmidiatly	Флаг, отключающий отложение операции обновления после загрузки модуля.
DownloadAndExecuteEXE или DAMPDLL	-	Загрузка файла с удаленного сервера и его запуск. В случае «DAMPDLL» происходит загрузка динамически связываемой библиотеки формата PE в адресное пространство процесса, в контексте которого выполняется исследуемая программа.
	Url	Сетевой адрес загружаемого файла.
	CommandLine	Аргументы командной строки, передаваемые файлу при его запуске.
	CryptMode	Значение «Static» или «Dynamic». Дешифрование загруженного файла происходит при помощи того же алгоритма, который используется для шифрования передаваемых данных. В первом случае используется ключ, передаваемый через аргумент «StaticKey» (см. ниже). Во втором случае в качестве ключа используется доменное имя, получаемое из сетевого адреса загружаемого файла.
	StaticKey	Ключ для дешифрования загружаемых файлов.
ChangeURLs	CommandUrls	Заменяет адреса командных серверов
	SendURLs	Заменяет адреса серверов для приема данных

Таблица 4. Команды, поступающие от управляющего сервера.

Приложение - Индикаторы компрометации

Список управляющих серверов (C&C)

Дополнительные индикаторы предоставляются по запросу

CORE VERSION	PE time stamp
1.17.6.4	
1.19.9.0	
2.1.4.0	
2.5.7.0 2.6.4.0	
2.5.8.0 2.6.2.0	
3.0.6.0 3.3.0.0 3.6.0.0 3.6.2.0 3.7.8.0 3.8.9.0	
3.8.9.6 3.9.9.0 4.1.0.0 4.1.0.1 4.1.7.0 4.3.1.2 4.3.9.1 4.3.9.5 4.3.9.7	Dec 13 02:07:37 2011 Dec 23 00:02:04 2011 Jan 11 09:25:12 2012 Jan 11 09:35:46 2012 Feb 09 08:17:08 2012 Mar 01 04:36:57 2012
4.3.9.8	
4.4.7.0 4.4.7.1 4.4.7.2 4.4.7.7 4.7.5.0	Apr 12 04:39:33 2012

4.8.1.0	
4.8.7.0 4.9.3.0 5.5.1.0 5.5.1.2 5.7.6.0 5.7.9.1 5.9.3.1	Jul 12 13:43:51 2013
5.7.6.0 5.7.9.1 5.9.3.0 6.0.3.0	
6.0.6.0	
6.0.8.1 6.0.8.2 6.2.0.0 6.2.0.1 7.5.0.0 7.6.13.1 7.6.13.2 7.6.13.4 7.6.13.5 7.6.13.6 7.6.13.7 7.6.13.8 7.6.13.9 7.7.5.1	Sep 26 20:42:10 2013 Jan 16 17:49:55 2014 Jan 16 18:01:42 2014 Feb 19 21:17:36 2014
6.0.8.2 6.2.0.1 6.4.1.3 7.5.0.1 7.7.6.1	Sep 26 20:44:01 2013 Nov 18 19:07:10 2013 Dec 26 06:32:38 2013
6.0.8.4 6.2.0.1	Sep 27 12:06:51 2013 Oct 08 14:23:06 2013
7.9.0.1 7.9.0.5 7.9.1.1 7.10.0.1	May 28 18:08:09 2014 May 28 18:23:42 2014 Jun 11 21:14:26 2014
7.16.0.1 7.20.0.11	Jul 01 23:03:16 2014 Jul 21 22:02:08 2014

7.16.1.0 7.45.1.1 7.47.1.1 7.56.1.1 7.70.1.1 7.74.1.1	Jul 01 23:27:25 2014 Aug 07 05:40:04 2014 Sep 18 16:16:43 2014
7.78.1.1	
7.34.0.1 7.34.0.2 7.45.0.2 7.46.0.1 7.56.0.1 7.70.0.2 7.70.0.3 7.74.1.1	Aug 05 09:29:09 2014 Aug 05 09:30:00 2014 Aug 07 05:32:04 2014 Aug 13 10:34:35 2014 Aug 20 16:32:14 2014 Sep 09 19:01:42 2014
7.85.0.1 7.92.0.1 7.92.1.2	Nov 06 09:14:46 2014
7.85.1.1 7.92.1.2	Oct 20 21:37:36 2014 Nov 07 01:07:58 2014
7.102.0.1	
7.107.0.1 7.107.1.1	Dec 10 22:03:23 2014
7.107.1.1	Dec 10 22:03:23 2014
7.118.1.1	
7.120.0.11 7.120.0.32	

Mutexes

Значения типа Mutex прописаны вредоносными программами

Mutex path
«Session\< id of desktop session for the injection process >\HighMemoryEvent_<id of process>»
Global\TermSrvReadyEvent

Пути инсталляции

Corkow инсталируется и запускается по следующим регитсрационным путям:

Possible Working Paths
«%Temp%\tmpXXXX.tmp
«%TEMP%

Yara rule

```
rule CorkowDLL
{
   meta:
      description = «Rule to detect the Corkow DLL files»
   strings:
      $mz = { 4d 5a }
      $binary1 = {60 [0-8] 9C [0-8] BB ?? ?? ?? ?? [0-8] 81 EB ?? ?? ?? ?? [0-8] E8 ?? 00 00 00 [0-8] 58 [0-8]
2B C3}
      $binary2 = {(FF 75 ?? | 53) FF 75 10 FF 75 0C FF 75 08 E8 ?? ?? ?? ?? [3-9] C9 C2 0C 00}
      $export1 = «Control_RunDLL»
      $export2 = «ServiceMain»
      $export3 = «DllGetClassObject»

   condition:
      ($mz at 0) and ($binary1 and $binary2) and any of ($export*)
}
```

О компании Group-IB

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

Имеет 12-летний опыт в области компьютерной криминалистики, предотвращения финансовых и репутационных потерь, консалтинга и аудита систем информационной безопасности, а также является разработчиком инновационных программных продуктов Bot-Trek, которые уже работают в более чем 50 компаниях в России, США и Европе:

Система детектирования целевых атак и сложных заражений Bot-Trek Threat Detection Service (TDS)

Сервис защиты онлайн-платежей и любых порталов Bot-Trek Intelligent Bank (IB),

Сервис киберразведки Bot-Trek Cyber Intelligence (CI) — платформа, позволяющая заказчику проводить мониторинг, анализировать и прогнозировать потенциальные угрозы информационной безопасности, актуальные для компании, ее партнеров и

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

Команда Group-IB – это эксперты, обладающие уникальной квалификацией, с большим практическим опытом, подтвержденным международными сертификатами CISSP, CISA, CISM, CEH, CWSP, GCFA и свидетельствами государственного образца в области защиты информации.

Представители компании являются членами различных экспертных советов и докладчиками крупнейших международных конференций по проблемам компьютерной безопасности.

Лицензии компании:

- Лицензия Федеральной Службы по Техническому и Экспортному Контролю (ФСТЭК России) на деятельность по технической защите конфиденциальной информации, серия КИ 0107 № 005310, регистрационный номер 2209;
- Лицензия Федеральной Службы Безопасности (ФСБ России) на работу со сведениями, составляющими государственную тайну серия ГТ № 0064472, регистрационный номер 4490.

+7 (495) 984-33-64
www.group-ib.com
info@group-ib.com
facebook.com/groupib
youtube.com/groupib
twitter.com/groupib
linkedin/company/group-ib