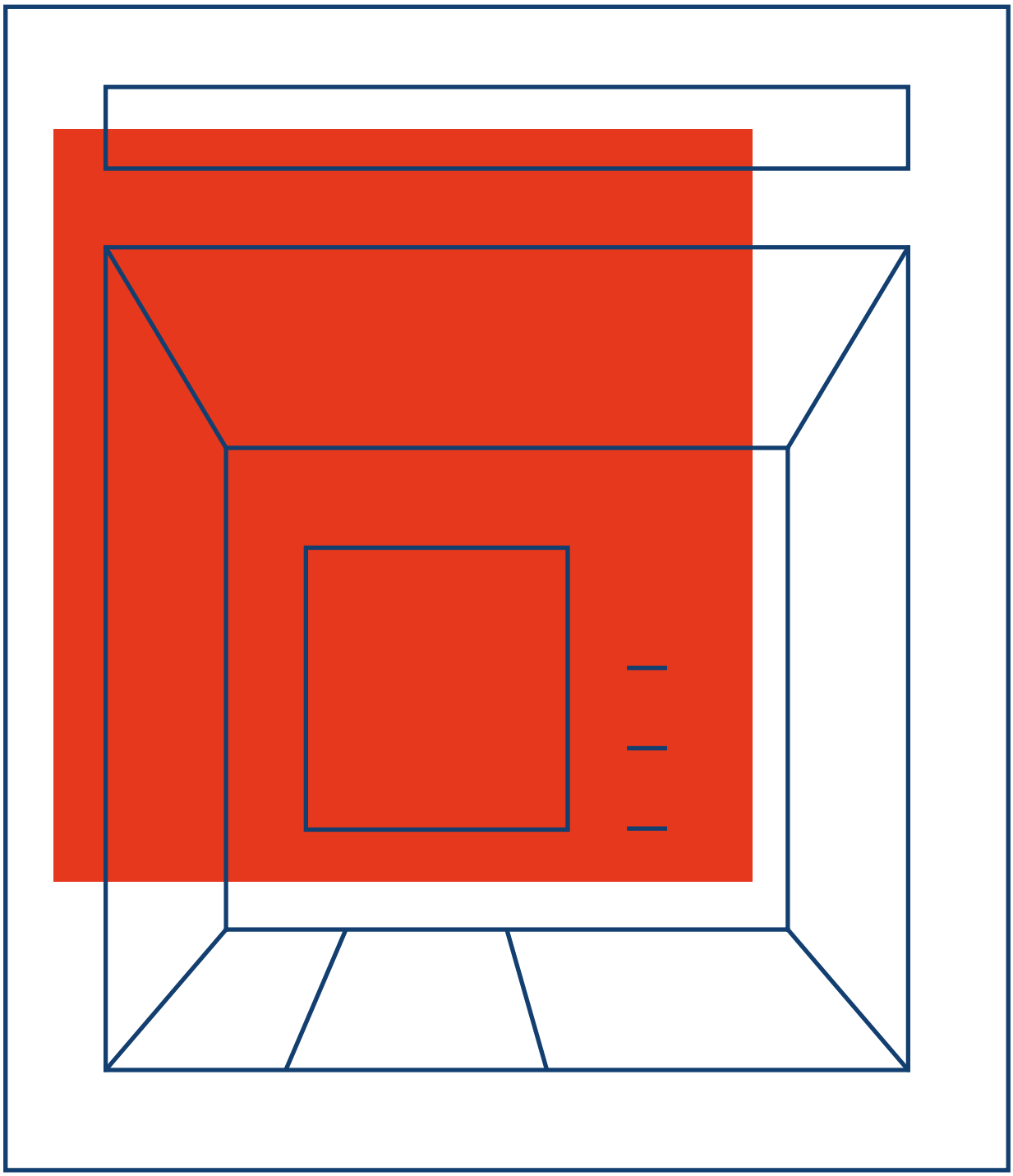
COBALT

Атаки на банки



GROUP IB

11.2016

Оглавление

Введение

В июле 2016 группа молодых людей в масках организованно атаковала 34 банкомата одного из крупнейших тайваньских банков First Bank, унеся с собой 83.27 миллионов тайваньских долларов (более 2 миллионов долларов США). Корпус банкомата не был вскрыт, на нем не было следов накладных устройств, преступники даже не использовали карты.

На записях камер наблюдения было видно, что, подойдя к банкомату, человек совершал звонок по мобильному телефону, после чего просто забирал купюры из приемника, который выдавал их автоматически. Такая «бесконтактная» атака на банкоматы произошла на острове впервые.

Уже в августе по аналогичной схеме было похищено 12 миллионов бат (около 350 тысяч долларов США) из 21 банкомата Government Savings Banks в Таиланде. В сентябре подобные атаки были зафиксированы в Европе, однако они не были преданы огласке.

В арсенале киберпреступников есть множество методов физических атак на банкоматы: скимминг, шимминг, захват карт (card trapping), кража и даже взрывы банкоматов стали привычным делом. Однако при физическом воздействии преступники получают возможность добраться до денег только из отдельного банкомата, оставляя при этом много следов.

Самые сообразительные хакеры стараются увеличить объем хищений и снизить риски, переходя от физических атак к логическим.

В ходе логической атаки злоумышленники получают доступ к локальной сети банка и уже из нее устанавливают полный контроль над банкоматами. По удаленной команде машины начинают выдавать наличность, а заранее подготовленные люди просто собирают деньги в сумки.

Имея полный контроль над сетью банкоматов, преступники могут выбирать дни и время, когда те загружены по максимуму, и в результате ущерб может достигать миллионов долларов, как это случилось с First Bank. При этом совершение такой атаки не требует дорогостоящей разработки сложного программного обеспечения: как вы узнаете из отчета, большинство использованных инструментов находится в открытом доступе.

Летняя волна хищений была лишь тестированием возможностей логических атак на банкоматы, которые в будущем станут одним из основных векторов целевых атак на банки.

Далее мы опишем, как одна из действующих преступных групп получает доступ к банкоматам, атакуя внутреннюю инфраструктуру банков в странах Западной и Восточной Европы, СНГ и Азиатско-Тихоокеанского региона.

Ключевые результаты

Преступная группа, которую мы назвали Cobalt в соответствии с использующимся ею фреймворком, **начала атаки в июне 2016 года**. Основной целью преступной группы являются сегменты по управлению банкоматами.

География активности

По состоянию на сентябрь 2016 года Cobalt атаковал банки в России, Великобритании, Нидерландах, Испании, Румынии, Белоруссии, Польши, Эстонии, Болгарии, Грузии, Молдавии, Киргизии, Армении и Малайзии.

Распространение

Для первоначального проникновения во внутреннюю сеть банка используется **точечная рассылка фишинговых писем с вредоносным вложением.** Фишинговые письма рассылаются от лица Европейского центрального банка, производителя банкоматов Wincor Nixdorf или от имени региональных банков. В качестве вредоносных вложений, атакующие используют документы с эксплойтами, а также письма с исполняемыми файлами в архиве с паролем.

В ранних атаках рассылка фишинговых писем производилась с виртуальных серверов с установленной системой анонимной рассылки писем «йаПосылалка v.2.0.» (другое название сервиса: «alexusMailer v2.0»), разработанной русскоговорящими специалистами.

Стоит отметить, что **кроме банков письма получали лизинговые и страховые компании**, входящие в состав группы компаний банка и нередко имеющие с ними одну сеть.

Проникновение

Атаки проводились **без дорогостоящей разработки специализированных троянов** с использованием легитимного программного обеспечения для тестов на проникновение – Cobalt Strike. Для компрометации доменных и локальных учетных записей преступники использовали утилиту Mimikatz или ошибку конфигурации контроллеров домена.

На получение полного доступа к контроллеру домена уходит от 10 минут до 1 недели.

Техники доставки фишинговых писем и получения управления над контроллером домена идентичны методам, использованным группой Buhtrap, которая с августа 2015 по январь 2016 похитила со счетов российских банков более 1,8 млрд рублей (о ней мы подробно рассказали в марте 2016).

После задержания группы лиц, занимавшихся обналичиваем похищенных денежных средств в мае 2016, бот-сеть Buhtrap была продана другим лицам, которые продолжают атаковать компании России и Украины.

Можно предполагать, что **как минимум часть участников Buhtrap группы вошла в Cobalt** или, что не менее вероятно, костяк Buhtrap просто переключился на атаки на банкоматы.

Атака на банкоматы

Для инициации выдачи денег банкоматом используется вредоносная программа, использующая стандартные функции по интерфейсу XFS через XFS Manager (eXtensions for Financial Services). По команде из внутренней сети банка **программа запускает выдачу купюр, которая продолжается до полного опустошения кассет**.

После каждой успешной операции по выдаче наличных программа записывает специальный лог (файл с именем «disp.txt») с информацией о количестве банкнот, выданных из каждой кассеты. Оператор передает этот лог-файл организатору атаки, который использует полученные сведения для **контроля цепи обналичивания**.

После выдачи денег все следы программы на банкомате уничтожаются с использованием легальной и бесплатной утилиты SDelete, доступной на сайте Microsoft. Кроме того, операторы выводят из строя внутренние серверы банка, с которого осуществлялись атаки, с помощью вредоносной программы MBRkiller, которая удаляет записи MBR (master boot record). **Столь тщательный подход к сокрытию следов сильно усложняет криминалистическое исследование.**

Программа, используемая для выдачи денег из банкоматов, является уникальной и используется одной группой.

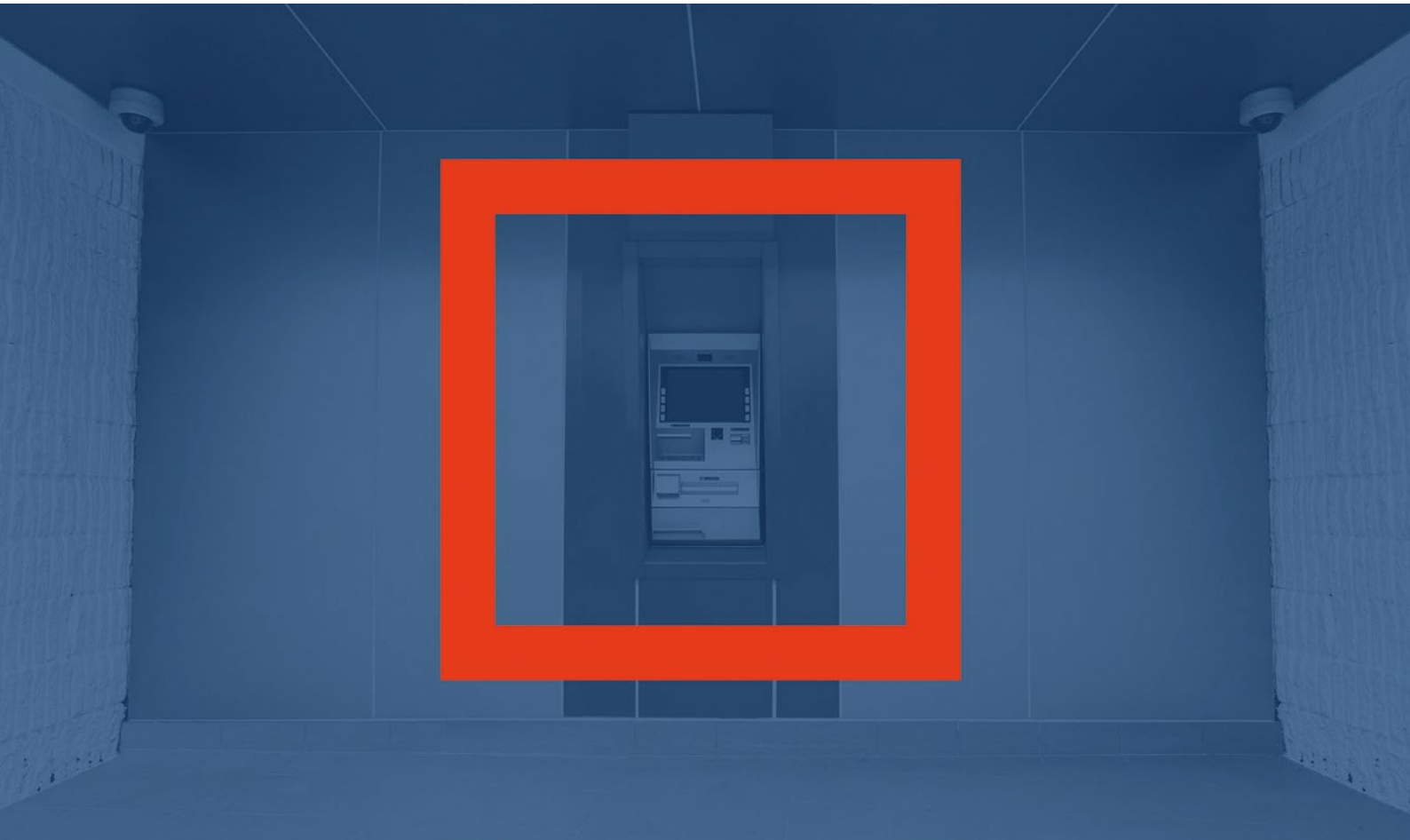
Рекомендации

Логические атаки можно выявить и предотвратить на разных этапах их развития. Для этого необходимо:

- использовать специальные системы обнаружения целенаправленных атак,
- отправлять подозрительные письма на динамический анализ в изолированной среде,
- отслеживать появление новых методов и инструментов атак с помощью киберразведки (threat intelligence).

При обнаружении следов атаки на любом этапе важно привлекать профессиональных криминалистов.

Самостоятельное реагирование может привести к тому, что преступники, несмотря на ваши действия, сохранят контроль над сетью и в конечном итоге добьются поставленных целей.



Основным способом проникновения в банковскую сеть является отправка фишингового письма с вложением, которое содержит эксплойт или исполняемый файл в архиве с паролем.

Фишинговые письма рассылаются от имени Европейского центрального банка, производителя банкоматов Wincor Nixdorf или от имени региональных банков. Несмотря на то, что в адресе отправителя указаны официальные домены Европейского центрального банка, Wincor Nixdorf, а также некоторых региональных банков, в действительности письма отправлялись с сервера с программным обеспечением, которое изменяло адрес отправителя, а банки и производители банкоматов не имели никакого отношения к этим рассылкам.

В июне для отправки поддельных писем использовалась система анонимной рассылки писем «йаПосылалка v.2.0.» (другое название сервиса: «alexusMailer v2.0»), разработанная русскоговорящими специалистами. **Позже для отправки фишинговых писем стали использоваться возможности Cobalt Strike,** о котором мы расскажем позже.

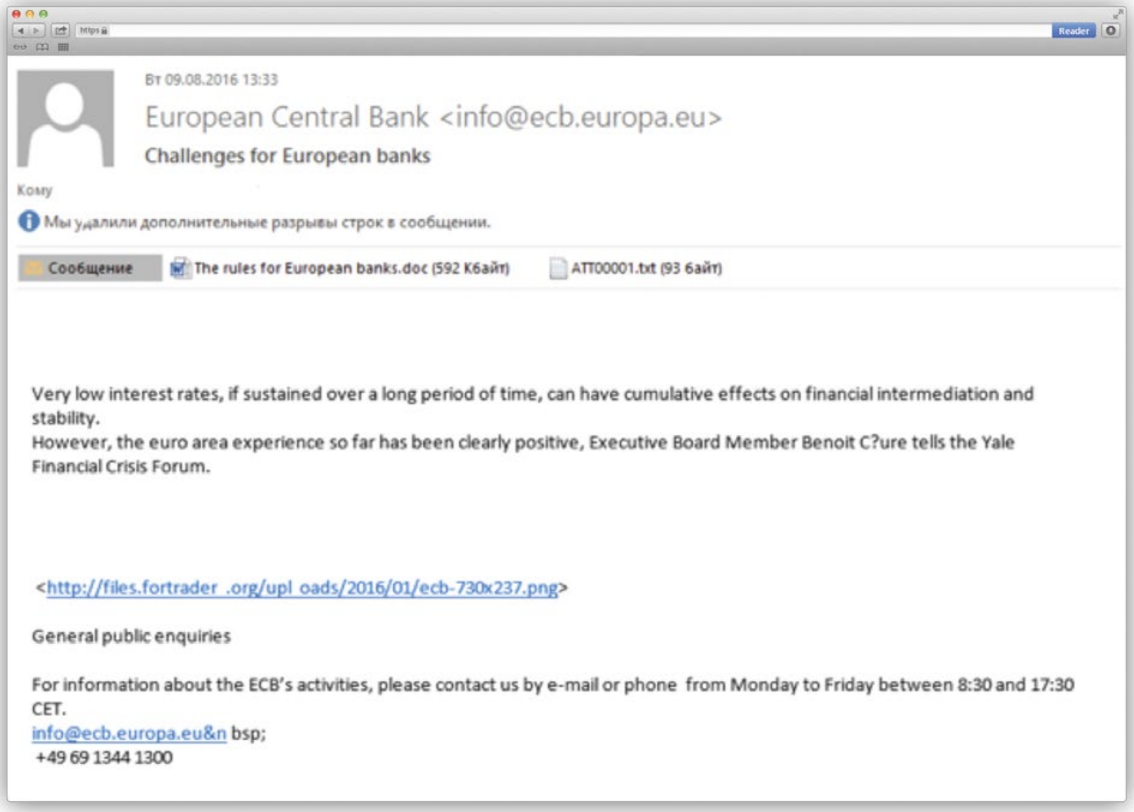
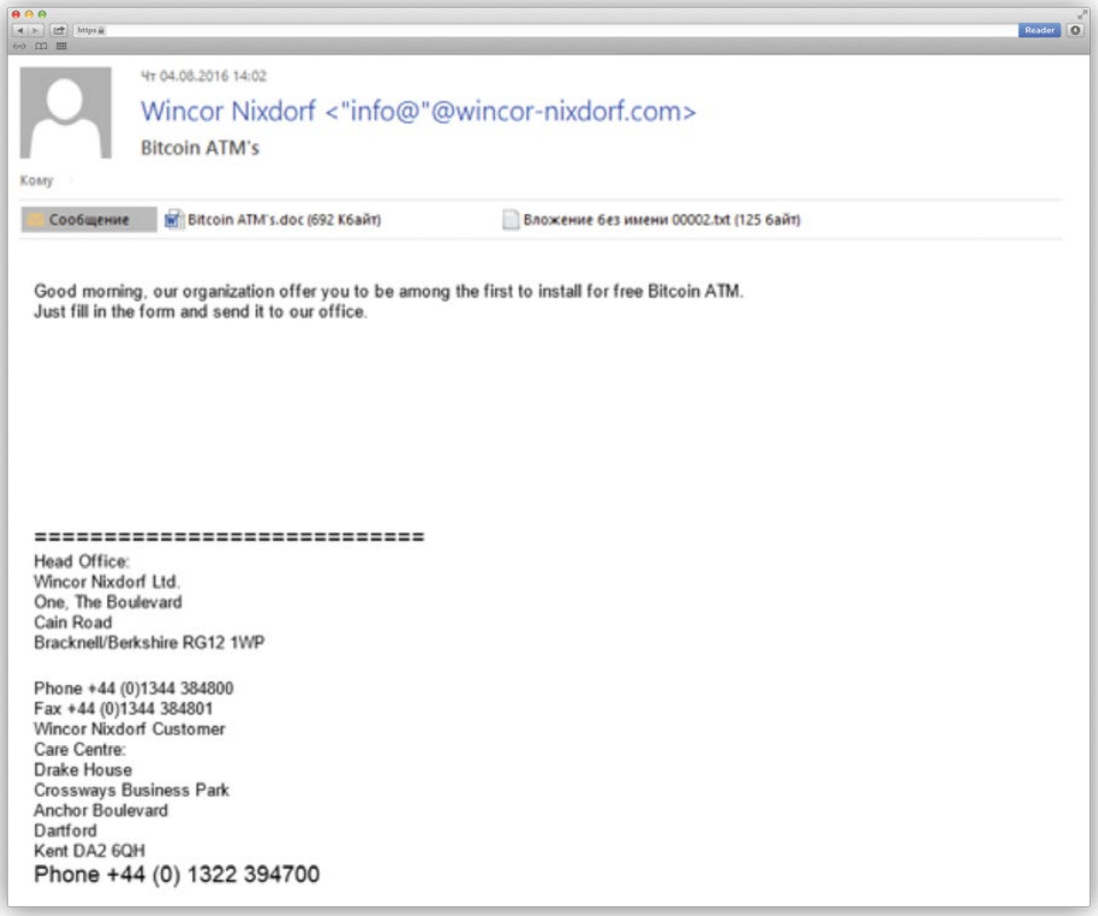


Рисунок 1.
Письмо от имени Европейского центрального банка



Чт 04.08.2016 14:02

Wincor Nixdorf <"info@"@wincor-nixdorf.com>

Bitcoin ATM's

Кому

Сообщение | Bitcoin ATM's.doc (692 Кбайт) | Вложение без имени 00002.txt (125 байт)

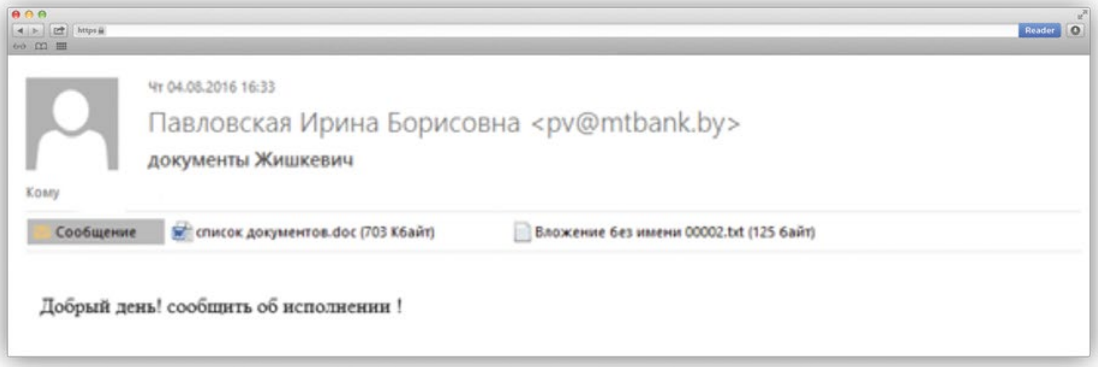
Good morning, our organization offer you to be among the first to install for free Bitcoin ATM.
Just fill in the form and send it to our office.

==========

Head Office:
Wincor Nixdorf Ltd.
One, The Boulevard
Cain Road
Bracknell/Berkshire RG12 1WP

Phone +44 (0)1344 384800
Fax +44 (0)1344 384801
Wincor Nixdorf Customer
Care Centre:
Drake House
Crossways Business Park
Anchor Boulevard
Dartford
Kent DA2 6QH
Phone +44 (0) 1322 394700

Рисунок 2. Письмо от имени Wincor Nixdorf



Чт 04.08.2016 16:33

Павловская Ирина Борисовна <pv@mtbank.by>

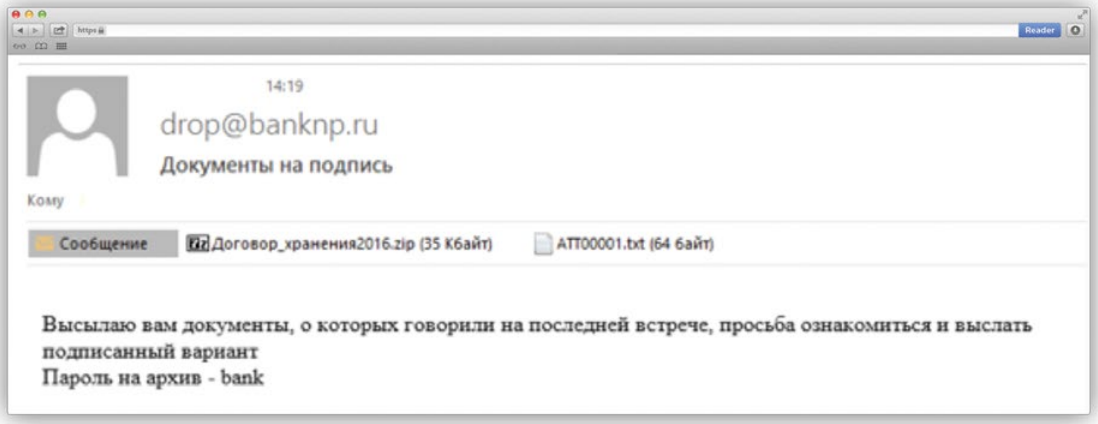
документы Жишкевич

Кому

Сообщение | список документов.doc (703 Кбайт) | Вложение без имени 00002.txt (125 байт)

Добрый день! сообщить об исполнении !

Рисунок 3. Письмо от имени белорусского банка



14:19

drop@banknp.ru

Документы на подпись

Кому

Сообщение | Договор_хранения2016.zip (35 Кбайт) | ATT00001.txt (64 байт)

Высылаю вам документы, о которых говорили на последней встрече, просьба ознакомиться и выслать подписанный вариант
Пароль на архив - bank

Рисунок 4. Письмо от имени российского банка

Проникновение

Отправка писем осуществлялась с двух серверов с IP адресами 88.212.208.115 и 5.101.124.34. **Оба сервера находятся в России.**

По технике доставки вредоносных программ атака напоминала действия группы Buhtrap, которая с августа 2015 по январь 2016 похитила из российских банков более 1,8 млрд рублей (о ее методике и инструментах мы подробно рассказали в отчете).

2016 год

МАРТ
Последняя подтвержденная атака на банк группой **Buhtrap**

МАЙ
Арест группы по отмыву денег для Buhtrap

ИЮНЬ
Первая атака на российский банк с помощью **Cobalt Strike**

ИЮЛЬ
Атаки на банки Армении, Белоруссии, Польши, Германии

АВГУСТ
Атаки на банки Грузии, Белоруссии, Румынии, Киргизии, Польши, Эстонии, Испании, Нидерландов, Великобритии, Малайзии

СЕНТЯБРЬ
Подтвержденные хищения из банкоматов за пределами России

Скачайте отчет «Buhtrap: Эволюция целенаправленных атак на банки» на group-ib.ru/reports

Для распространения вредоносных программ по банкам в русскоговорящем сегменте преступники использовали вложения с именами «Договор_хранения2016.zip» и «список документов.doc». Для фишинговых атак в других странах они использовались файлы «The rules for European banks.doc» и «Bitcoin ATM's.doc». **Максимальное распространение получил документ от имени Европейского центрального банка, разосланный в августе 2016 года.** Пример результатов его загрузки на Virus Total показан ниже.

Date	File name	Source	Country
2016-08-19 12:31:08	The rules for European banks.doc	eb3f6189 (web)	RU
2016-08-19 11:45:47	The rules for European banks.doc	6d4b7a9b (web)	ES
2016-08-18 13:58:58	The rules for European banks.doc	eb3f6189 (web)	RU
2016-08-18 08:04:02	TherulesforEuropeanbanks.doc	f72bfc97 (web)	EE
2016-08-17 06:24:35	The rules for European banks.doc	40ae9ac0 (web)	RO
2016-08-16 15:28:27	/home/support/SAMPLES/The_rules_for_E...	2941e051 (api)	RU
2016-08-16 15:05:16	The rules for European banks.doc	d6d3fd27 (web)	NL
2016-08-16 12:52:29	The rules for European banks.doc	4e6c28c0 (web)	BY
2016-08-16 12:19:08	The rules for European banks.doc	4eeb0fa0 (web)	RO
2016-08-16 12:07:54	The rules for European banks.doc	d2a26a35 (web)	PL

Мы получили часть писем, отправленных с этих серверов, изучили вредоносные вложения, нашли связанные с ними экземпляры вредоносных программ и проверили, откуда в момент атаки загружались подозрительные файлы на Virus Total. Таким образом, нам удалось установить более полный **список целей атак, в который вошли банки из России, Великобритании, Нидерландов, Испании, Румынии, Польши, Эстонии, Болгарии, Белоруссии, Молдавии, Грузии, Армении, Киргизии и Малайзии.**

Стоит отметить, что **кроме банков письма получали лизинговые и страховые компании, входящие в состав группы компаний банка.** В некоторых случаях такие компании имеют общие сети, что использовалось атакующими для получения доступа к интересующим их системам.

После того как вредоносное вложение было запущено, на системе начинался процесс закрепления в системе, который можно описать следующим образом:

1. Во вложении находились **вредоносные RTF-документы**, эксплуатирующие уязвимость CVE-2015-1641. При этом использовался стандартный шеллкод, генерируемый такими инструментами для тестирования на проникновение, как Metasploit и Cobalt Strike.

2. Если уязвимость успешно эксплуатировалась, **в оперативную память загружалась полезная нагрузка, которая называется Beacon, входящая в состав Cobalt Strike.** Cobalt Strike — это богатый фреймворк для проведения тестов на проникновение, позволяющей доставить на атакуемый компьютер полезную нагрузку и управлять ею.

   Взаимодействие с серверной частью Cobalt Strike происходит посредством создания скрытых каналов с использованием протоколов DNS, HTTP, HTTPS для предотвращения обнаружения сетевого взаимодействия с помощью стандартных систем IDS/IPS.

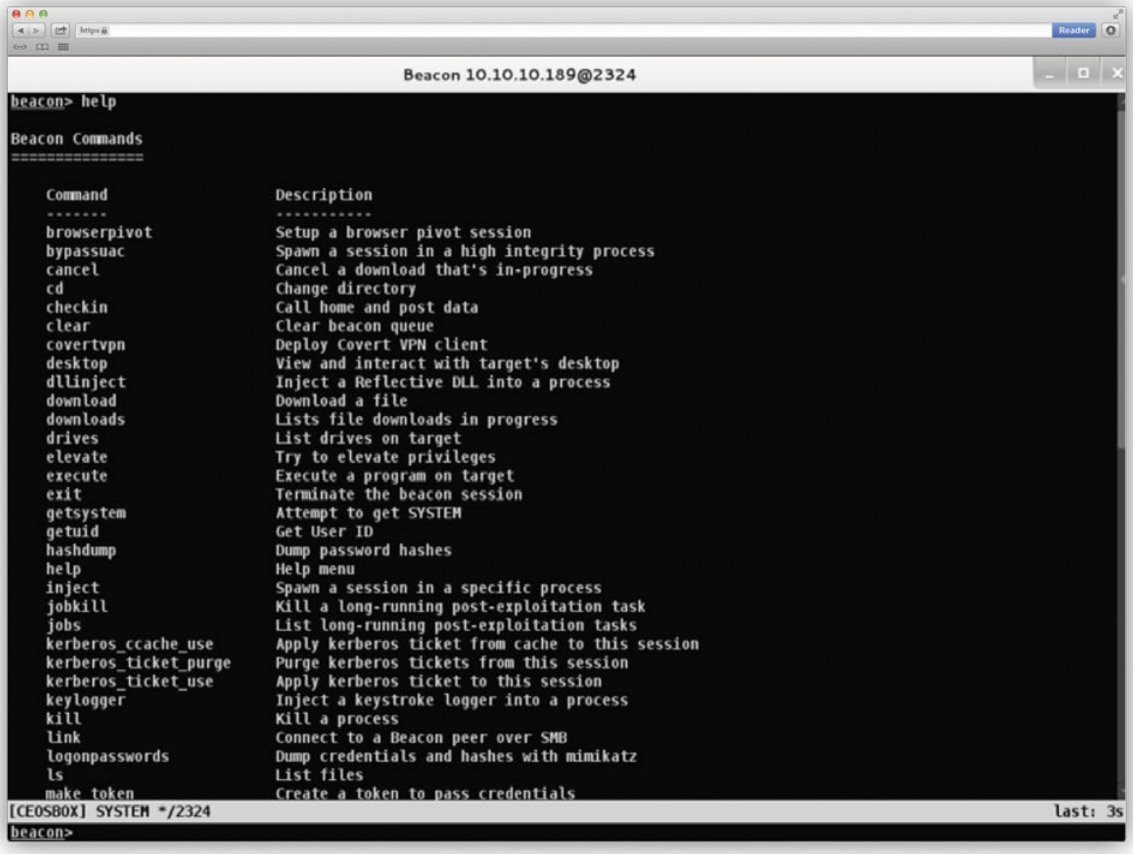


Рисунок 6.
Список команд для Beacon

Закрепление на локальной системе

3. Если по каким-то причинам письмо с эксплойтом не давало результата, атакующие присылали письмо с запароленным архивом, в котором находился тот же самый Beacon.

   В любом случае, после запуска вредоносного вложения Beacon загружался только в оперативную память. **Это означает, что после перезагрузки операционной системы атакующие теряли контроль над этим компьютером.**

   Чтобы обеспечить постоянную работоспособность на системе, автоматически срабатывал специальный модуль Beacon, который проверял, какие приложения прописаны в автозагрузку, и заменял некоторые из них своим исполняемым файлом с таким же именем.

   В реальных атаках мы наблюдали замену файлов с именами iusb3mon.exe (Intel(R) USB 3.0 eXtensible Host Controller) и jusched.exe (Sun Java Update Scheduler). **В результате такой замены службы, которые должны были автоматически запускать легальные программы, запускали вредоносные приложения.**

4. В тот же каталог, где находились замененные легальные исполняемые файлы, копировалась и библиотека с именем crss.dll. Каждый раз при старте операционной системы замененные приложения загружали эту библиотеку в память. Ее основной задачей была загрузка из интернета модуля Beacon в оперативную память.

Таким образом обеспечивалась жизнеспособность основной программы. После каждой перезагрузки операционной системы основной модуль удалялся. Все описанные выше шаги выполнялись автоматически после запуска вредоносного вложения.

Однако на случай, если зараженный компьютер выключат или переустановят операционную систему, нужно было наладить постоянный доступ к локальной сети. Для необходимо было повысить привилегии.

Для беспрепятственного исследования локальной сети банка и получения доступа к изолированным сегментам сети и информационным системам атакующему нужны права администраторов домена. Методы получения этих привилегий на 100% идентичны методам, используемым группой Buhtrap.

Метод No1
Ошибка конфигурации контроллера домена

Начиная с Windows Server 2008 в групповых политиках была добавлена дополнительная функциональность — Group Policy Preferences (GPP). GPP позволяют администраторам применять множество политик, таких как автоматическое назначение сетевого диска в момент входа пользователя в свой компьютер, обновление имени встроенной учетной записи администратора, создание новых пользователей, внесение изменений в реестр и т.п.

Такие действия как добавление локального пользователя, подключение сетевого диска или принтера могут потребовать указания пароля. Когда такие политики будут загружаться для применения на отдельном компьютере, они будут делать это вместе с указанным паролем. Пароль, зашифрованный с помощью алгоритма AES-256 и дополнительно кодированный по Base64, хранится в конфигурационном файле GPP Groups.xml.

Этот XML-файл создается создается не всегда, а когда, например, создается или меняется встроенная учетная запись администратора. Файл хранится на контроллере домена в подкаталоге директории SYSVOL и, как и сам каталог, доступен любому пользователю в домене.

Атакующие используют Groups.xml для извлечения пароля администратора домена следующим образом:

1. После получения доступа в локальную сеть способом, описанным в предыдущем разделе, они находят контроллеры домена, которые указаны в настройках компьютера.

2. На контроллерах домена они проверяют наличие директории SYSVOL и файла Groups.xml, который доступен по следующему пути: **«\\[server_name]\sysvol\[domain_name]\Policies\[group_policy_name]\Machine\Preferences\Groups\Groups.xml»**

3. Из файла Groups.xml они извлекают логин и пароль администратора домена из полей cpassword и userName. На рисунке показано, как выглядит зашифрованный пароль.

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
   <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name=
   "Administrator" image="0" changed="2016-02-11 10:13:31" uid=
   "{0E00B161-AAE4-4B39-A986-F18E9F423283}" userContext="0"
   removePolicy="0">
   <Properties action="C" fullName="Admin" description="Admin"
   cpassword="JBLVqAc7C57vQp+2r5S3N8leZraFQJof2cNlCd99YWY"
   changeLogon="0" noChange="0" neverExpires="1" acctDisabled="0"
   userName="Administrator"/></User>
   <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name=
   "User" image="0" changed="2016-02-11 10:13:49" uid=
   "{DC63BBEB-81B8-4A7C-81E6-C347CAD8F50B}">
   <Properties action="C" fullName="User" description="User"
   cpassword="KIpruAJgGAvuzk+Po6eSPA" changeLogon="1" noChange="0"
    neverExpires="0" acctDisabled="0" userName="User"/></User>
</Groups>
```

Рисунок 7. Фрагмент файла Groups.xml

4. Для получения пароля в открытом виде атакующие декодируют пароль по Base64, получая строку вида 4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b — это пароль, зашифрованный с помощью AES-256.

5. Полученный зашифрованный пароль расшифровывается с помощью ключа 4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b, опубликованного на официальном сайте Microsoft MSDN.

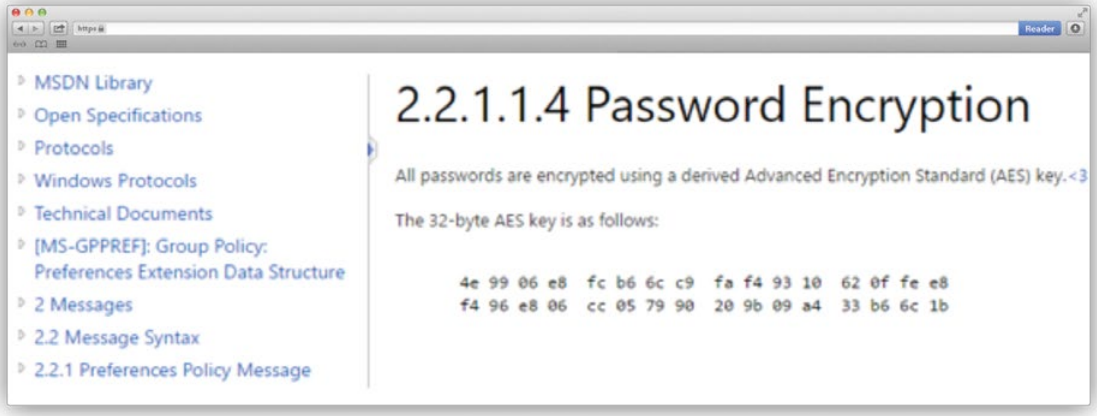


Рисунок 8. Ключ шифрования на сайте Microsoft MSDN

6. После успешной расшифровки пароля они получают доступ к контроллеру домена и, используя описанный ниже метод, могут получить доступ к паролю любой учетной записи.

При такой конфигурации контроллера домена атакующие получали к нему доступ за 10 минут.

Метод No2
Утилита Mimikatz

Утилита Mimikatz позволяет извлекать учётные данные Windows из LSA в открытом виде из оперативной памяти операционной системы всех авторизованных пользователей. Для успешной эксплуатации необходимо иметь возможность присоединить библиотеку к процессу lsass.exe, для чего нужны права локального администратора. Исходный код Mimikatz опубликован на GitHub, доступен всем и встроен в некоторые инструменты для тестов на проникновение, включая Cobalt Strike.

Если атакующие уже имеют права локального администратора и доступ к контроллеру домена

После того, как атакующие получали доступ к контроллеру домена методом No1, они запускали на серверах Mimikatz и с ее помощью собирали пароли всех администраторов, которые были подключены к этому серверу. Для этого достаточно набрать в командной строке

```
mimikatz sekurlsa::logonpasswords
```

и логин с паролем всех пользователей показывались на экране.

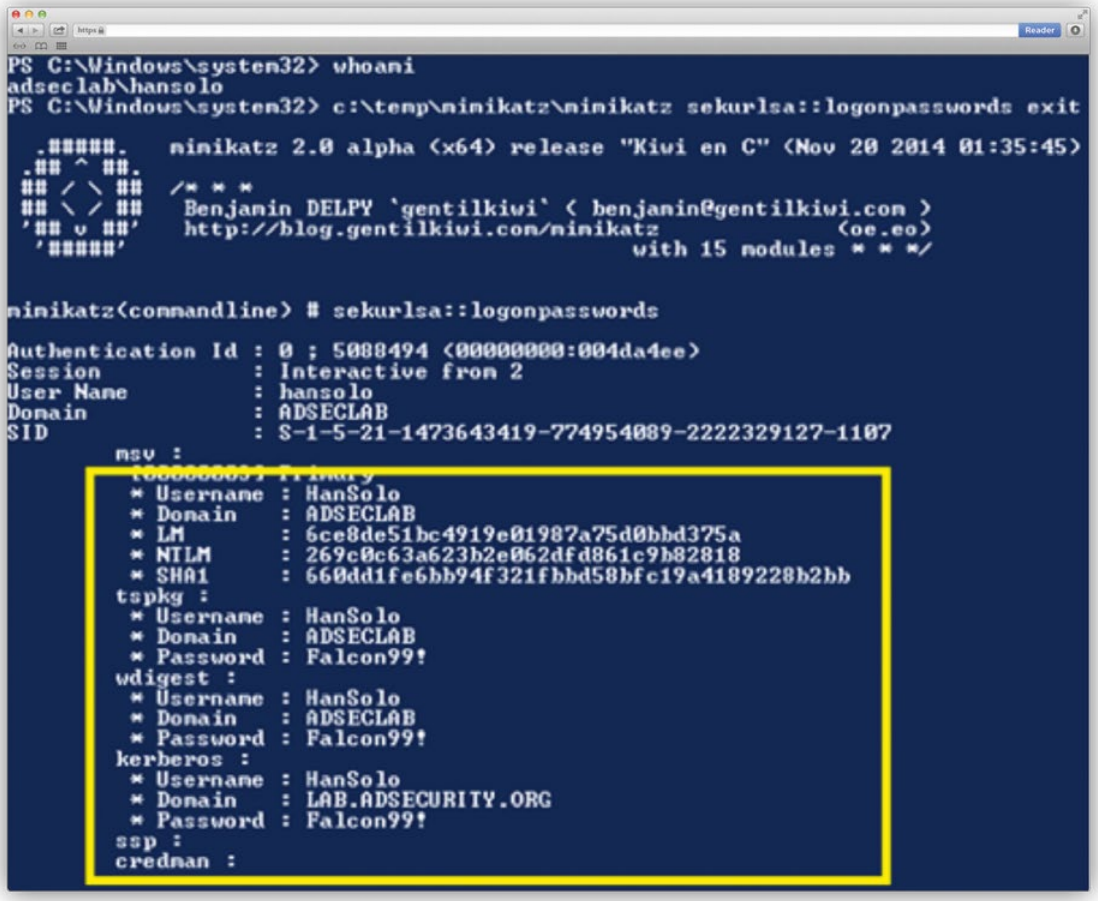


Рисунок 9.
Результат работы утилиты Mimikatz

Если атакующие уже имеют права локального администратора без доступа к контроллеру домена

Когда атакующие попадали на компьютер с правами администратора, не имеющим при этом прав доступа к контроллеру домена, они начинали **подключаться к другим рабочим станциям и серверам с реквизитами имеющейся учетной записи** и запускать Mimikatz до тех пор, пока не находился пользователь с необходимыми правами.

С правами локального администратора атакующие получали доступ к контроллеру домена в течении 1 дня.

Если атакующие не имеют прав локального администратора

Как мы писали выше, для работы Mimikatz необходим доступ к процессу lsass.exe, что требует прав локального администратора. Если изначальный доступ в сеть был получен путем компрометации учетной записи без прав локального администратора, то в ход пускались эксплойты для повышения локальных привилегий. Если на операционной системе были установлены необходимые обновления и исправления, атакующие начинали подключаться к другим хостам с этой доменной учетной записью и проверяли их на наличие уязвимостей, которые позволили бы им поднять права до уровня локального администратора.

В такой ситуации на получение доступа к контроллеру домена у атакующих уходило от 1 дня до недели.

Для повышения привилегий на локальной системе атакующие использовали уязвимости CVE-2014-4113, CVE-2015-1701, CVE-2015-2363 и CVE-2015-2426, которые позволяли поднять привилегии до уровня SYSTEM на x32 и x64 операционных системах.

Mimikatz Golden Ticket

Мы не встречали использование Cobalt этого метода, поскольку получения доступа к доменным учетным записям решало все их проблемы, однако в других инцидентах они могут задействовать именно его. Метод заключается в получении Golden Ticket, который дает **максимальный доступ к любой учетной записи.**

В Active Directory есть системная учетная запись krbtgt (Key Distribution Center Service Account). Она всегда отключена по умолчанию, ее нельзя переименовать или удалить, нельзя использовать для входа в домен.

Получив доступ к контроллеру домена, злоумышленники могу скопировать всю базу Active Directory, например, выполнив команду mimikatz.exe “privilege::debug” “lsadump::samrpc /patch” exit из извлечь из нее NTLM-хеш учетной записи krbtgt.

Используя полученный хэш и идентификатор домена, с помощью того же Mimikatz они могут создать файл с золотым TGT-билетом, с помощью которого можно получить доступ к любой записи в домене.

После описанных выше шагов у атакующих был удаленный доступ к сети и привилегии, позволяющие им делать в локальной сети все, что им необходимо. Далее требовалось закрепиться в локальной сети для сбора данных и наладить резервные каналов доступа на случай, если активность будет зафиксирована и служба безопасности начнет принимать контрмеры.

Закрепление на зараженном компьютере/сервере

Итак, у атакующих есть как минимум один хост с Beacon. Им необходимо иметь доступ к множеству компьютеров, в том числе к тем, которые не имеют выхода в интернет. **Для этого в локальной сети банка они выстраивали свою мини-сеть из зараженных компьютеров, которыми можно было управлять через единую консоль Cobalt Strike**, установленную на удаленном сервере и предоставляющей возможность коллективной работы.

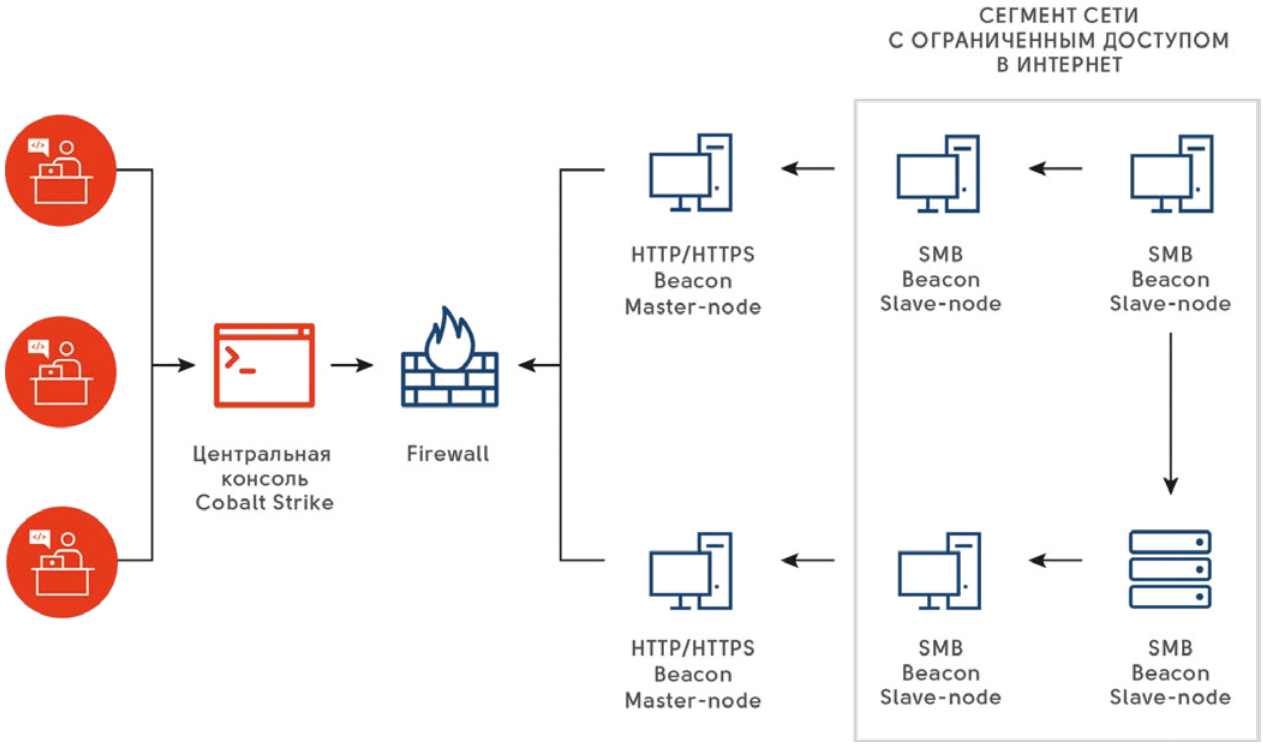
Процесс можно описать следующим образом:

- На хостах с доступом в интернет запускалась версия Beacon, которая устанавливала соединение с удаленным сервером управления по скрытому каналу. Для предотвращения обнаружения такого сетевого взаимодействия с помощью стандартных систем IDS/IPS использовались протоколы DNS, HTTP, HTTPS. Таких хостов было немного, и они обеспечивали возможность взаимодействия с другими хостами в локальной сети. Назовем их **master-node.**

- Наибольший интерес в банке представляют изолированные хосты, не имеющие доступа в интернет. Но даже если доступ разрешен, создание соединения с удаленным сервером на критичных системах вызывает подозрения у бдительной службы безопасности. Чтобы управлять такими хостами и не вызывать подозрения у систем обнаружения аномалий, атакующие использовали специальную версию Beacon, которой можно управлять только из локальной сети по протоколу SMB с использованием pipe. Назовем их **slave-node**.

- Cobalt Strike позволяет связывать master-node и slave-node через специальный канал по протоколу SMB. Таким образом, slave-node становятся доступны в удаленной центральной консоли управления Cobalt Strike. **Т.е. изолированные хосты получают доступ в интернет через master-nod, которые становятся шлюзом для slave-node.**

Такая схема позволяла преступникам выстроить достаточно надежный механизм постоянного доступа в локальную сеть атакуемого банка, оставаясь при этом максимально незаметными.



Чтобы выдворить атакующих из сети, необходимо как минимум выявить все хосты, выполняющие роль master-node, и вывести их из сети единовременно, иначе у преступников появляется шанс восстановить работу в течении нескольких минут.

Обеспечение резервного канала доступа

После успешной компрометации локальной сети и домена атакующие могли использовать легитимные каналы удаленного доступа, например, подключаться через терминальные серверы, либо по VPN с правами администратора или обычного пользователя.

Несмотря на то, что Cobalt Strike имеет встроенный модуль удаленного доступа по VNC, атакующие перестраховывались и загружали модифицированный установщик TeamViewer — легальный инструмент удаленного доступа. Восстановить установщик полностью не удалось, поэтому мы предполагаем, что основным отличием от официального приложения является сокрытия оповещения о том, что к компьютеру осуществлено удаленное подключение, как это было в атаках других преступных групп в России.

На записях камер видеонаблюдения атака на банкоматы выглядела следующим образом:

- К банкоматам в разных концах города подходил человек с мобильным телефоном.
- По телефону он что-то сообщал своим партнерам и готовил сумку.
- Через несколько минут банкомат начинал порциями выдавать деньги.
- После того как деньги в банкомате заканчивались, человек повторно связывался с партнерами и уходил.
- Опустошенный банкомат перезагружался.

Съемом денег занимались небольшие группы, которые переходили к заранее определенным банкоматам и снимали деньги в течение нескольких часов. Далее мы опишем то, что происходило за пределами видимости видеокамер.

Роли в группе

Как показывают исследования всех атак, одновременно атакуется сразу несколько банков. На то, чтобы получить доступ в банк, скомпрометировать всю сеть, найти, откуда можно получить доступ к банкоматам, оценить, сколько понадобиться людей на сбор денег из банкоматов, уходит минимум несколько дней. Чтобы поддерживать весь этот процесс, необходимы время и команда с четкими зонами ответственности.

ОРГАНИЗАТОР АТАКИ

Ядро любой группы. Обычно это один или пара человек, которые разрабатывают схему, нанимают людей, распределяют роли и обеспечивают финансирование процесса. Важнейшей задачей для организатора является контроль как операторов, так и мулов, в том числе с использованием функционала вредоносных программ (об этом ниже).

ОПЕРАТОРЫ

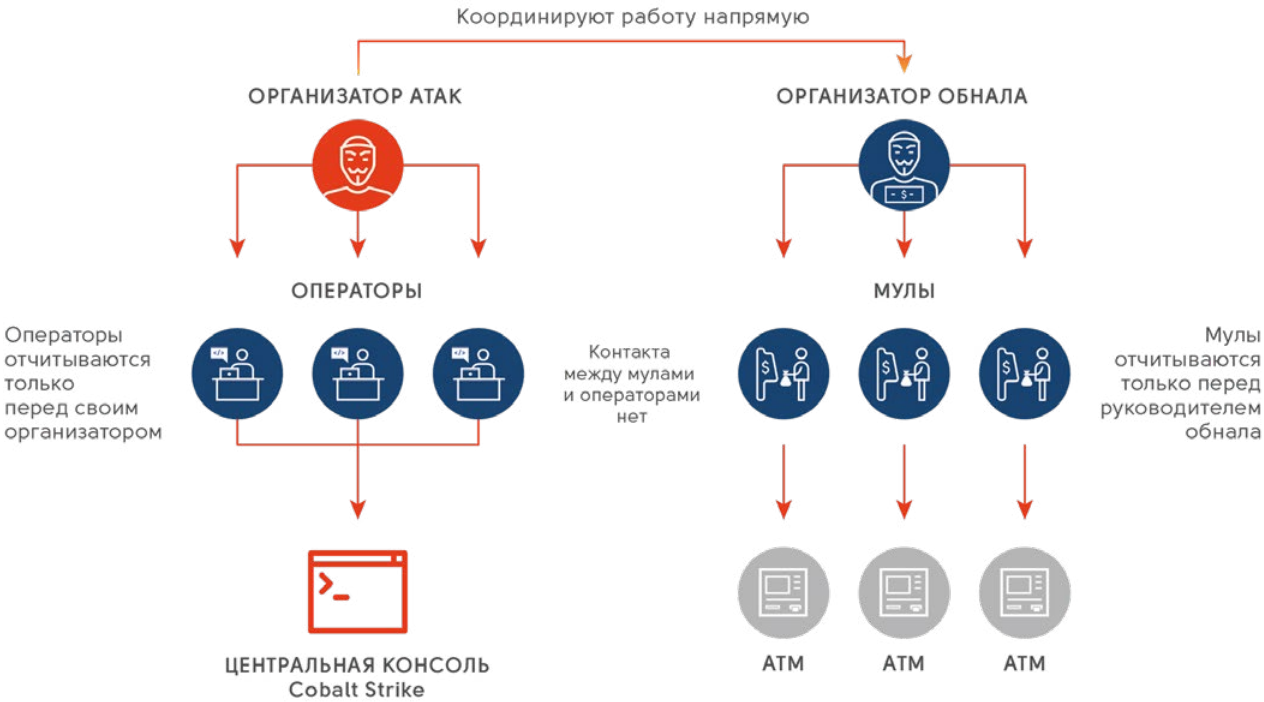
Люди, непосредственно осуществляющие взлом внутренних сетей банков и дающие банкоматам команды на выдачу денег. Обычно их несколько человек, поскольку параллельно атакуется сразу несколько банков. Операторы контролируют количество выданной наличности и отчитываются перед организатором.

ОРГАНИЗАТОР ОБНАЛА

Взаимодействует непосредственно с организатором атаки, ничего не зная об операторах. В его задачи входит координация действий по обналичиванию денег и контроль за мулами. Именно ему мулы звонят с отчетом о количестве полученных из банкомата денег, которые он впоследствии передает организатору.

МУЛЫ

Люди с минимальными техническими навыками, не имеющие отношения к взлому банков. Их основная задача – забрать деньги из банкомата и отчитаться перед организатором обнала, который удаленно контролирует их активность. Именно мулов задерживают на основании записей камер наблюдения.



Через несколько дней после атак на банкоматы First Bank в Таипее были задержаны граждане Латвии и Румынии. Оставшиеся 13 подозреваемых, включая граждан России, успели покинуть остров. **Часто мулы въезжают в страну по туристическим визам специально для осуществления атаки и покидают ее как только операция окончена.**

Получение доступа к банкоматам

После установления контроля над внутренней сетью банка и обеспечения резервных каналов доступа, преступники переходили к поиску сегментов сети, из которых можно получить доступ к банкоматам, и рабочих мест сотрудников, которые должны следить за банкоматами.

Получив доступ к компьютеру или серверу, с которого разрешен доступ к банкоматам, атакующие использовали стандартные инструменты удаленного доступа, используемые в банке. Как правило, это протокол удаленного управления Microsoft Remote Desktop Protocol.

Получив доступ к банкоматам, они загружали на них специальное программное обеспечение, которое позволяло им управлять выдачей наличных.

Программное обеспечение для атаки на банкоматы

После получения удаленного доступа к банкоматам на него загружаются три файла:

- скрипт del.bat, который запускал программу SDelete с нужными параметрами.

  Содержимое скрипта del.bat
  ```
  sdelete.exe -accepteula -p 32 d2.exe
  sdelete.exe -accepteula -p 32 xtl.exe
  sdelete.exe -accepteula -p 32 *.txt
  sdelete.exe -accepteula -p 32 d2s.exe
  del sdelete.exe
  del del.bat
  ```

- легитимная программа SDelete (опубликована на сайте Microsoft). Ее предназначение — удаление файлов специальным образом, чтобы их было невозможно восстановить в ходе криминалистического исследования.

- вредоносная программа, использующая стандартные функции по интерфейсу XFS через XFS Manager (eXtensions for Financial Services). Именно эта программа по команде из внутренней сети банка начинает выдачу денег.

Исходный код программы не был защищен, что сильно упрощает ее анализ и дает возможность вносить корректировки в логику ее работы. Это означает, что автор вредоносной программы не планировал ее распространение, а скорее всего входит в состав группы атакующих.

Вредоносная программа позволяет при помощи XFS API взаимодействовать с диспенсером в банкомате и давать команды на опустошение кассет с наличностью. Она функционирует в соответствии с аргументами, которые должны передаваться при запуске. Всего таких аргументов 5, и значение каждого из них необходимо указать.

Аргументы командной строки должны располагаться в следующим порядке:

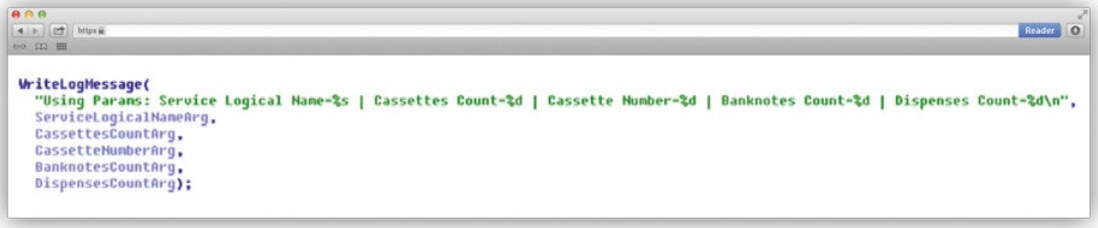
- **ServiceLogicalName** — имя сервиса, используемое в качестве аргумента для функции WFSOpen (например «Cash Dispenser Module»).
- **Cassettes Count** — общее число кассет, присутствующих на устройстве. Значение должно быть в интервале от 1 до 15.
- **Cassette Number** — номер кассеты, из которой следует выдать наличность. Значение должно быть в интервале от 1 до 15.
- **Banknotes Count** — число банкнот, которое необходимо выдать из кассеты. Значение должно быть в интервале от 1 до 60.
- **Dispenses Count** — какое количество раз необходимо повторить выдачу наличности. Значение должно быть в интервале от 1 до 60.

```
if ( (unsigned int)(BanknotesCountArg - 1) > 0x3B )
{
  WriteLogMessage("Error! Banknotes Count should be from 1 to 60\n");
  return 1;
}
if ( (unsigned int)(CassetteNumberArg - 1) > 0xE )
{
  WriteLogMessage("Error! Cassette Number should be from 1 to 15\n");
  return 1;
}
if ( CassettesCountArg - 1 > 0xE )
{
  WriteLogMessage("Error! Cassettes Count should be from 1 to 15\n");
  return 1;
}
if ( (unsigned int)(DispensesCountArg - 1) > 0x1F3 )
{
  WriteLogMessage("Error! Dispenses Count should be from 1 to 500\n");
  return 1;
}
```

Рисунок 10. Фрагмент кода программы для банкомата, отвечающий за прием параметров

Все эти значения указываются в консоли оператором, который подключен к банкомату удаленно.

Если все аргументы были переданны корректно, выводится сообщение, отображающее параметры, в соответствии с которыми будут производиться дальнейшие действия.

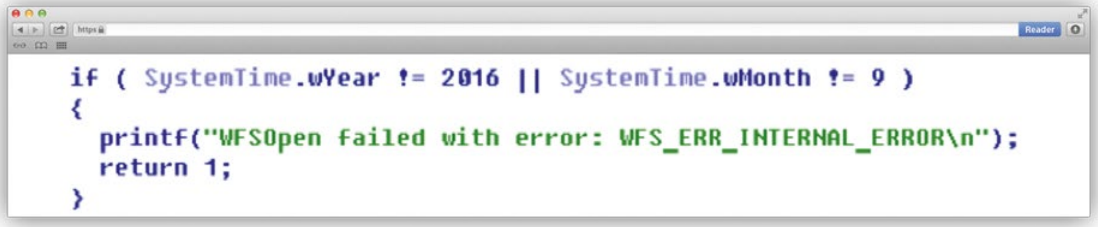


```
WriteLogMessage(
  "Using Params: Service Logical Name=%s | Cassettes Count=%d | Cassette Number=%d | Banknotes Count=%d | Dispenses Count=%d\n",
  ServiceLogicalNameArg,
  CassettesCountArg,
  CassetteNumberArg,
  BanknotesCountArg,
  DispensesCountArg);
```

Рисунок 11. Фрагмент кода программы для банкомата, отвечающий за создание лога

Далее заполняется массив, каждый элемент которого соответствует номеру кассеты в устройстве. Количество элементов массива должно совпадать с общим количеством кассет. Значение, которое хранит каждый элемент массива, означает количество банкнот, которые необходимо выдать из соответствующей кассеты. Нумерация элементов массива начинается с 1.

В процессе функционирования программа получает данные о системном времени, и, в случае если оно не соответствует указанному в коде программы, завершает свою работу.



```
if ( SystemTime.wYear != 2016 || SystemTime.wMonth != 9 )
{
  printf("WFSOpen failed with error: WFS_ERR_INTERNAL_ERROR\n");
  return 1;
}
```

Рисунок 12. Фрагмент кода программы для банкомата, отвечающий за создание лога

Далее программа производит ряд стандартных действий, которые необходимо проделать до операции выдачи наличности, и, если все они завершились успешно, банкомат выдает купюры мулу. Эта операция,будет повторена столько раз, сколько указано в аргументе «Dispenses Count».

При успешном завершения каждой такой операции в файл с именем «disp.txt», расположенный в в том же каталоге, что и вредоносная программа, записывается текстовая строка «Cassettes Count:Banknotes Count», где «Cassettes Count» и «Banknotes Count» значения соответствующих аргументов.

Было обнаружено две версии такой программы. Одна имела имя d2.exe, а вторая d2sleep.exe. Разница между ними заключалась лишь в том, что вторая выдавала наличность с небольшой паузой — 1 секунда.

После того как в банкомате заканчивались купюры, **оператор запускал программу SDelete, которая удаляла использованные файлы по специальному алгоритму, не позволяющему восстановить информацию**. После этого банкомат перезагружался. Кроме того, операторы выводили из строя внутренние серверы банка, с которого осуществлялись атаки на банкоматы, с помощью вредоносной программы MBRkiller, которая удаляла записи MBR (master boot record). Все это сильно усложняет криминалистическое исследование атаки.

На телефонах задержанных мулов были найдены сообщения с шестизначными кодами. Обычно такие коды присылаются организатором, чтобы активировать работу вредоносной программы на конкретном банкомате.

Скорее всего, в арсенале преступников есть и другие программы для атак на банкоматы.

Обеспечение контроля

Чтобы операторы не могли воспользоваться программой для атак на другие банкоматы без привлечения организатора, в ее код встроена проверка времени запуска. Если системное время атакуемого банкомата не соответствует месяцу, указанному в коде, команды не будут выполняться. При этом программа не будет выдавать ошибок, и, скорее всего, операторы не знают о такой встроенной проверке.

После каждого успешного выполнения операции по выдаче наличных программа записывает специальный лог (файл с именем «disp.txt») с информацией о количестве банкнот, выданных из каждой кассеты. Оператор передает этот лог-файл организатору, который использует полученные сведения для контроля цепи обналичивания.

Связь с Buhtrap

ВОЗОБНОВЛЕНИЕ АТАК НА ЮРИДИЧЕСКИЕ ЛИЦА С ИСПОЛЬЗОВАНИЕМ БОТ-СЕТИ BUHTRAP

МАРТ

Последняя подтверждённая атака на банк группой **Buhtrap**

МАЙ

Арест группы по отмыву денег для Buhtrap

ИЮНЬ

Первая атака на российский банк с помощью **Cobalt Strike**

ИЮЛЬ

Атаки на банки Армении, Белоруссии, Польши, Германии

АВГУСТ

Атаки на банки Грузии, Белоруссии, Румынии, Киргизии, Польши, Эстонии, Испании, Нидерландов, Великобритии, Малайзии

СЕНТЯБРЬ

Подтвержденные хищения с банкоматов за пределами России

В мае 2016 года была задержана группа лиц, занимавшаяся обналичиваем похищенных денежных средств для группы Buhtrap. После этого хищения со счетов банков с помощью одноименного трояна прекратились, однако бот-сеть продолжила существовать: уже в мае денег лишилось несколько зараженных Buhtrap компаний.

Исследуя подобные инциденты, мы обнаружили в сетях атакованных компаний две версии средства удаленного управления Light Manager: первая версия была установлена давно (в ряде случаев – больше года назад), вместе с основной вредоносной программой, а вторая — в июне 2016 года. Мы предполагаем, что сразу после майского задержания бот-сеть Buhtrap была продана другим злоумышленникам, которые пользуются ею для хищений со счетов компаний.

Вместе с тем, наши исследования атак Cobalt на банкоматы российских и европейских банков показали, что техники доставки фишинговых писем и получения доступа к контроллеру домена идентичны использованным группой Buhtrap.

Это позволяет предполагать, что как минимум часть участников этой преступной группы вошла в Cobalt или, что не менее вероятно, костяк Buhtrap просто переключился на атаки на банкоматы.

Абсолютно все целенаправленные атаки на банки можно было предотвратить или выявить на разных этапах их развития. Ниже мы приводим простые рекомендации, которые позволят более эффективно выявить действия атакующих.

В общих случаях эти рекомендации помогут предотвратить хищения, но свести риски к минимуму можно только отслеживая активность группировок с помощью киберразведки (threat intelligence) и используя специализированные решения для обнаружения целевых атак.

Предотвращение проникновения

Основным способом проникновения в банковскую сеть является отправка фишингового письма с вложением, которое содержит эксплойт или исполняемый файл в архиве с паролем. Чтобы предотвратить заражение в результате работы эксплойта, достаточно своевременно обновлять программное обеспечение Microsoft. Эта преступная группа не использовала уязвимостей нулевого дня, и более того, эти эксплойты были достаточно старыми. **Поэтому даже обычное обновление программного обеспечения не позволяло атакующим попасть в корпоративную сеть.** В некоторых атакованных банках это требование не соблюдалось.

В тех случаях, когда атакующие сталкивались с обновленным программным обеспечением, они отправляли вложения с исполняемым файлов в архиве с паролем. **Такие атаки можно отбить, отправляя подобного рода письма в карантин на динамический анализ в изолированной среде.**

Предотвращение на этапе реализации атаки

Реализация атаки после первоначального получения доступа в сеть банка может занять дни, а иногда месяцы. Используйте это время для выявления действий атакующих.

- Проверьте настройки контроллера домена и наличие файла Groups.xml в каталоге SYSVOL с зашифрованным паролем на стандартном ключе AES-256, как это было описано в разделе о получении привилегий.
- Установите на банкоматы программное обеспечение для контроля целостности.
- Проведите проверку по индикаторам, представленным в следующем разделе.

Если вы обнаружили следы целенаправленной атаки для ее исследования на любом из ее этапов нужно привлекать профильные компании.

Неправильное реагирование приводит к тому, что часть действий атакующих остается незамеченными, они сохраняют контроль над сетью и в конечном итоге добиваются поставленных целей.

IP адреса серверов, с которых велась рассылка фишинговых писем:

88.212.208.115
5.101.124.34

Названия вредоносных вложений:

The rules for European banks.doc
Bitcoin ATM's.doc
Договор_хранения2016.zip
список документов.doc

Ссылки на загрузку Beacon от Cobalt Strike:

hxxp://korolev-okna.ru/beacon.exe
hxxp://50.115.164.10/update.exe
hxxp://176.31.79.123/~tolipresorts/nig.exe
hxxp://durok.net/0x/1.exe
hxxp://www.sport7boxe.com/METOO.exe
hxxp://methninja.tk/private/hawkraw.exe
hxxps://23.152.0.210/GizS

IP-адреса серверов управления Cobalt Strike:

188.214.129.65
94.130.120.179
23.152.0.210
95.215.45.221
84.200.84.241
95.183.51.24

MD5 вредоносных файлов:

966cc404a4f6bf6d77565004a952b3e3	Cobalt Strike
db6a8169f55a20838c0ca6f383c11e23	Cobalt Strike
7fa1af2adba39ef6efe0f870c057554d	Cobalt Strike
89889adb22c63186eb8c72323f34b1fd	Cobalt Strike
0d21832c171e817e947837bbfb67380e	Cobalt Strike
0c34ae326a8fd68d4a67ea3484b7cf81	Cobalt Strike
555399c93b5f01fd9fad5f903da768d3	Cobalt Strike
56487b799755f50c6e56c41870d43624	Cobalt Strike
fe44c14403f36c6e451bda391a1d1ca7	Cobalt Strike
d529218495f0318b99e60477368bb55e	ATM malware program
f5aea645966319c96d4dbcadce2a10e0	ATM malware program
036faf1f7e39e44c0db25b9149b45786	MBRKiller
eb162cc34efae1cb621cc7157ef36514	Modified SDelete
c91658349005a2f1c92a20132de38486	Cobalt Strike launcher from autorun
3ea9ef46e89f07920d87255aef9261ba	Cobalt Strike launcher from autorun
cafab9cc40ad0bd1cbec2164e17c8216	Cobalt Strike beacon downloader
35e0449cbe9fbe43e95b920c246828b2	Cobalt Strike beacon downloader
bfb9688ac2747017c7975921ffe77be9	The rules for European banks.doc
b175140a52aca83833a8203ac81e7475	The rules for European banks.doc
712e11e5217ef06847ea96a83e952566	The rules for European banks.doc
5d11c7b17633332b787992ee617d3552	The rules for European banks.doc
9d443e225e21f160014e79b62c5aea3d	Bitcoin ATM's.doc
83dee40f12f67634c5da640f6d6f2efb	Договор_хранения2016.zip
1d07edbd16cbe529500c37245e613a47	Договор_хранения2016.exe
3b2b116db9569f50c9e7a272c7530b18	список документов.doc

Подписчики сервиса кибербразведки Bot-Trek Intelligence узнали о тактике атак Cobalt еще в августе 2016. Наши консультации помогли жертвам вовремя остановить атаку, полностью очистить сеть и закрыть атакующим доступ к банкоматам.

Мы можем быть полезны на всех этапах атаки. Позвоните или напишите нам, чтобы узнать больше.

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

Bot-Trek Intelligence

Кибербразведка по подписке — мониторинг, анализ и прогнозирование угроз для компании, ее клиентов и партнеров

Bot-Trek TDS + TDS Polygon

Система обнаружения целевых атак и выявления ранее неизвестного вредоносного кода

Центр реагирования CERT-GIB

Круглосуточная помощь опытных специалистов в реагировании на инциденты

Расследования и криминалистика

Безупречный сбор доказательной базы и оперативное установление личностей преступников

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

В 2015 году Group-IB была названа в числе 7 самых влиятельных игроков в сфере информационной безопасности по версии британского издания Business Insider.

Узнайте больше на **group-ib.ru**