АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET препарировала шпионское ПО InvisiMole, использующееся с 2013 года

18 июня 2018 года

Следить за высокопоставленными жертвами, оставаясь в тени. Это принцип работы двух вредоносных компонентов InvisiMole. Они превращают зараженный компьютер в видеокамеру атакующих, которая позволяет видеть и слышать все, что происходит в офисе или в любом другом месте, где находится устройство. Операторы InvisiMole легко подключаются к системе, следят за действиями жертвы и крадут ее секреты.

По данным телеметрии ESET, злоумышленники, стоящие за данной спайварью, активны как минимум с 2013 года. Тем не менее, этот инструмент кибершпионажа не только не был изучен, но и не детектировался до момента обнаружения продуктами ESET на зараженных компьютерах в России и Украине.

Кампания высокотаргетирована, что объясняет низкий уровень зараженности – всего несколько десятков компьютеров.

InvisiMole имеет модульную архитектуру, начинает свой путь с DLL-обертки (wrapper DLL), далее действуют два модуля, встроенные в его ресурсы. Оба модуля – многофункциональные бэкдоры, позволяющие малвари собрать максимум информации о цели.

Чтобы отвлечь внимание пользователя от зараженной машины, применяются дополнительные

меры. Это позволяет вредоносной программе оставаться в системе на протяжении длительного времени. Нам еще предстоит установить вектор заражения – в настоящее время возможны все варианты, включая ручную установку при наличии физического доступа к машине.

Установка и персистентность

Первая часть исследуемой малвари – DLL-обертка, скомпилированная с помощью Free Pascal Compiler. По данным нашей телеметрии, DLL помещается в папку Windows и маскируется под легитимный файл библиотеки `mpr.dll` с поддельной информацией о версии.

```
1
2  1 VERSIONINFO
3  FILEVERSION 6,1,7600,16385
4  PRODUCTVERSION 6,1,7600,16385
5  FILEOS 0x40004
6  FILETYPE 0x2
7  {
8  BLOCK "StringFileInfo"
9  {
10         BLOCK "040904B0"
11         {
12                 VALUE "CompanyName", "Microsoft Corporation"
13                 VALUE "FileDescription", "Multiple Provider Router DLL"
14                 VALUE "FileVersion", "6.1.7600.16385 (win7_rtm.090713-1255)"
15                 VALUE "InternalName", "mpr.dll"
16                 VALUE "LegalCopyright", "© Microsoft Corporation. All rights reserved."
17                 VALUE "OriginalFilename", "mpr.dll"
18                 VALUE "ProductName", "Microsoft® Windows® Operating System"
19                 VALUE "ProductVersion", "6.1.7600.16385"
20         }
21 }
22
23 BLOCK "VarFileInfo"
24 {
25         VALUE "Translation", 0x0409 0x04B0
26 }
27 }
```

Рисунок 1. Обертка DLL маскируется под легитимный файл библиотеки mpr.dll, копируя имя и информацию о версии

Мы не видели образцы с другими именами обертки, хотя в коде DLL есть указания на то, что файл может называться также `fxsst.dll` или `winmm.dll`.

Первый способ запуска малвари – техника подмены DLL (DLL hijacking). DLL-обертка помещается в ту же папку, что и `explorer.exe`, и загружается при запуске Windows вместе с процессом Windows Explorer вместо легитимной библиотеки, расположенной в папке `%windir%\system32`.

Мы обнаружили 32- и 64-битные версии малвари, что обеспечивает персистентность в обеих архитектурах.

В качестве альтернативы подмене DLL возможны другие методы загрузки и обеспечения персистентности. DLL-обертка экспортирует функцию `GetDataLength`. При вызове этой функции DLL проверяет, была ли она загружена процессом `rundll32.exe` с помощью `explorer.exe` или `svchost.exe` в качестве родительского процесса, и только после этого запускает полезную нагрузку. Это предполагает другие возможные методы обеспечения персистентности – внесение задач в планировщик (родительский процесс – `svchost.exe`) или

запись в ключ автозапуска реестра (родительский процесс – `explorer.exe`).

Вне зависимости от способа обеспечения персистентности поведение вредоносной программы и непосредственно полезной нагрузки во всех случаях одинаково. DLL-обертка загружает модуль, хранящийся в ресурсах под названиями `RC2FM` и `RC2CL`, и (если используется подмена DLL) легитимную библиотеку в процесс `explorer.exe`, чтобы не нарушать нормальную работу приложения и оставаться незамеченной.

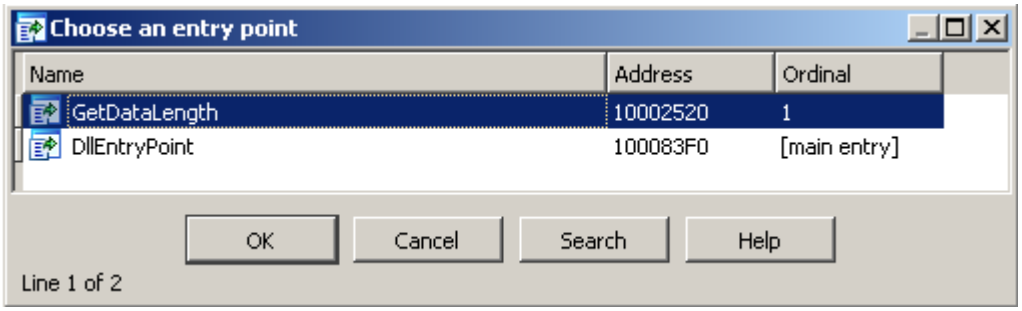

Рисунок 2. Экспортированные функции DLL-обертки

Технический анализ

Точная дата компиляции вредоносной программы неизвестна – последние образцы DLL-обертки изменены авторами, временные метки PE обнулены вручную. Однако в ходе исследования мы обнаружили более раннюю версию, датированную 13 октября 2013 года, так что новые версии явно скомпилированы позднее.

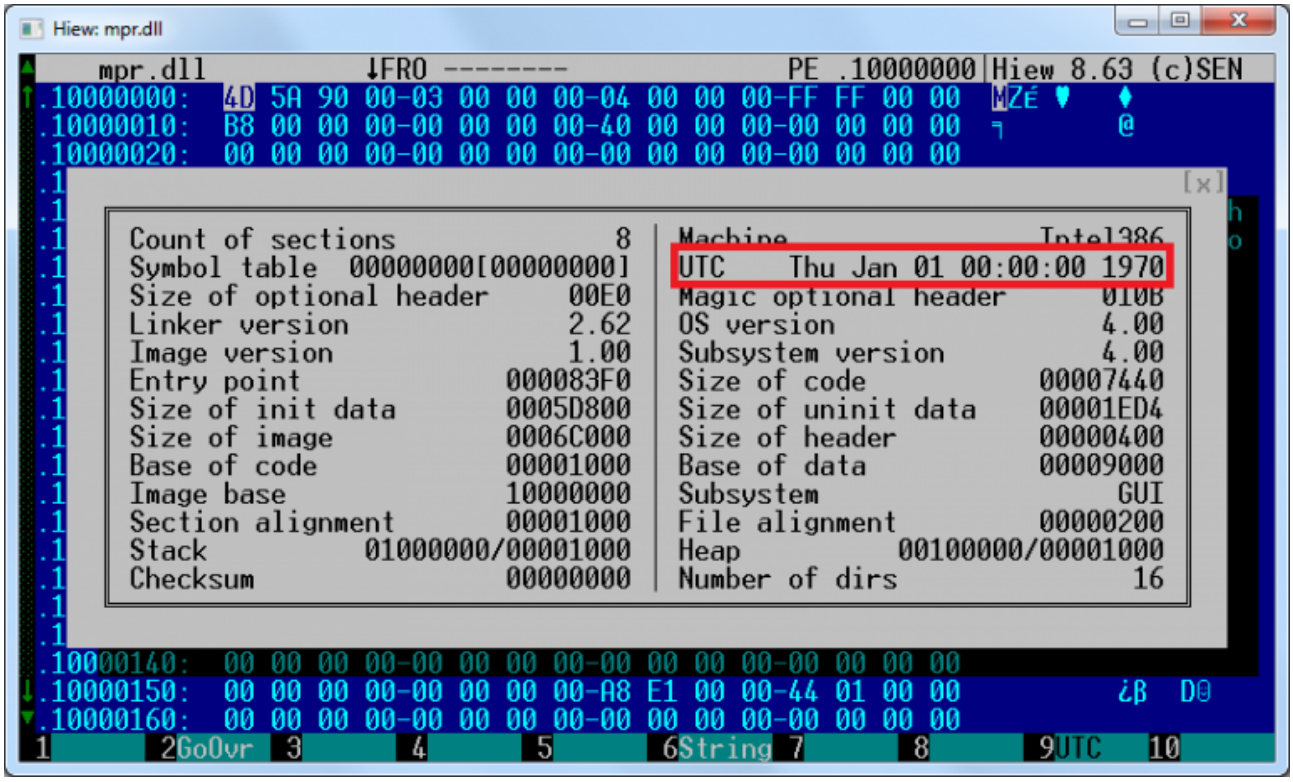

Рисунок 3. Во всех поздних образцах временные метки выставлены на нулевые значения

Шифрование и расшифровка

Для маскировки от вирусных аналитиков и системных администраторов авторы вредоносной программы используют шифрование строк, внутренних файлов, данных конфигурации и сетевых коммуникаций. В то время как модуль `RC2FM` использует кастомные шифры, DLL-обертка и модуль `RC2CL` применяют одну конкретную процедуру для всех целей, включая расшифровку других вредоносных модулей, встроенных в DLL-обертку.

Скрипт, с помощью которого можно выделить встроенные модули `RC2FM` и `RC2CL` из DLL-обертки, доступен в репозитории ESET на GitHub.

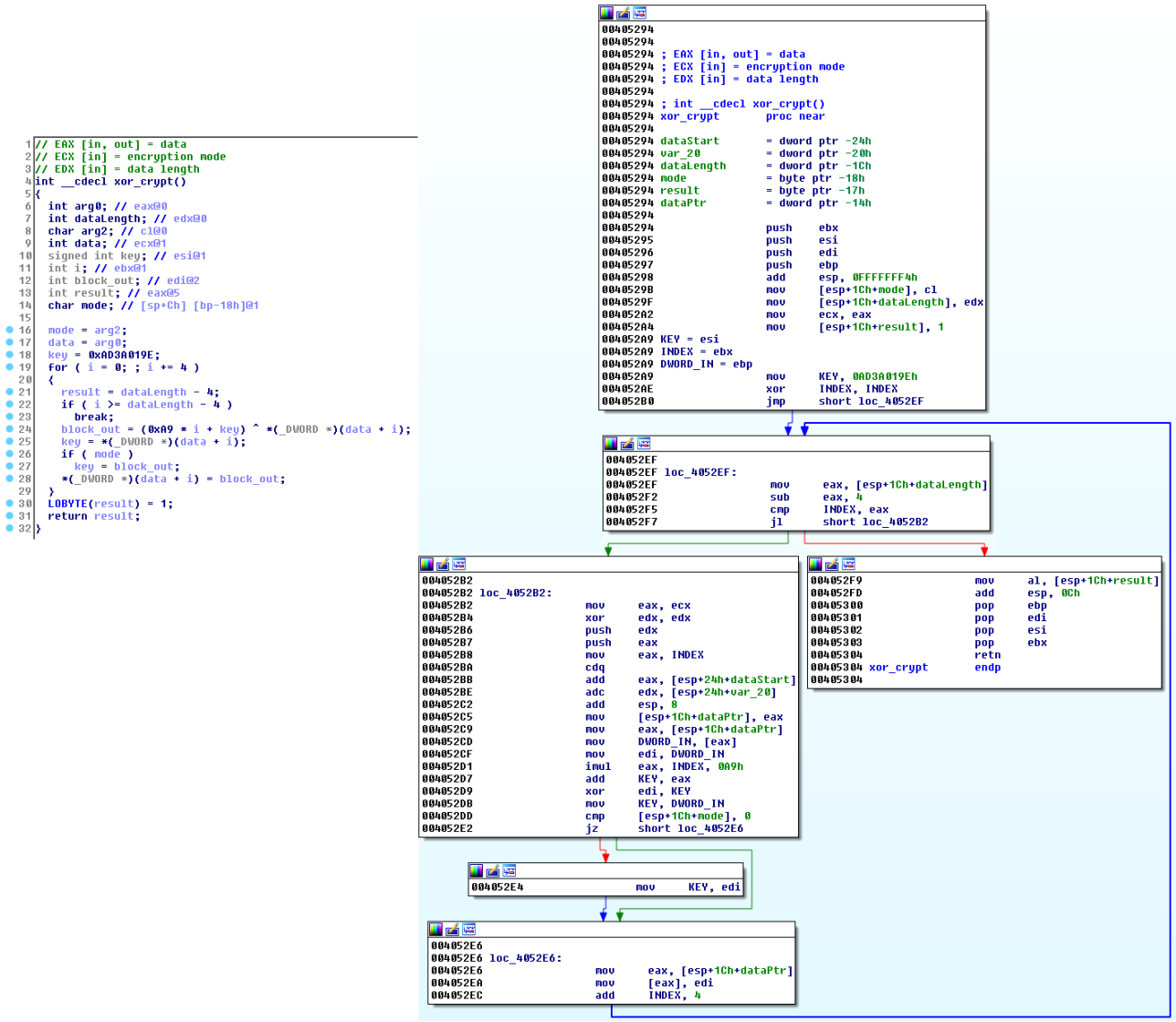

Рисунок 4. Процедура расшифровки в различных образцах (декомпилированная и дизассемблированная)

Модуль RC2FM

Первый, меньший модуль `RC2FM` содержит бэкдор, поддерживающий 15 команд. Они выполняются на зараженном компьютере по указанию атакующего. Модуль может вносить различные изменения в системе, а также включает инструменты для кибершпионажа.

В файлах реализована опция ведения журналов, но имя системного журнала не задано в изученном образце. Это дает основания предполагать, что функция использовалась только на стадии разработки.

Сетевая коммуникация

Этот модуль связывается с C&C-серверами, которые либо жестко закодированы в образце, либо позже добавляются атакующими.

Кроме того, модуль способен обращаться к C&C-серверу даже при настроенном прокси на зараженной машине. Если прямое соединение установить не удалось, модуль пытается подключиться к любому из своих C&C-серверов с помощью локально настроенных прокси или прокси, настроенных для разных браузеров (Firefox, Pale Moon и Opera).
RC2FM даже может проверить список недавно использованных приложений и попробовать найти переносимые исполняемые файлы браузеров:

```
FirefoxPortable.exe
OperaPortable.exe
Run waterfox.exe
OperaAC.exe
Palemoon-Portable.exe
```

Если жертва пользуется одним из этих переносимых браузеров *с настроенным прокси сервером*, малварь может обнаружить его в пользовательских настройках и применить для связи со своими C&C-серверами.

Коммуникация с C&C-сервером представляет собой серию HTTP GET и POST запросов, как показано на рисунке 5. Зашифрованный запрос содержит идентификатор ПК и временную метку, а также некоторую другую информацию (опционально). Важно отметить, что модуль `RC2FM` использует несколько методов шифрования (варианты простого XOR шифрования), в отличие от других компонентов InvisiMole.

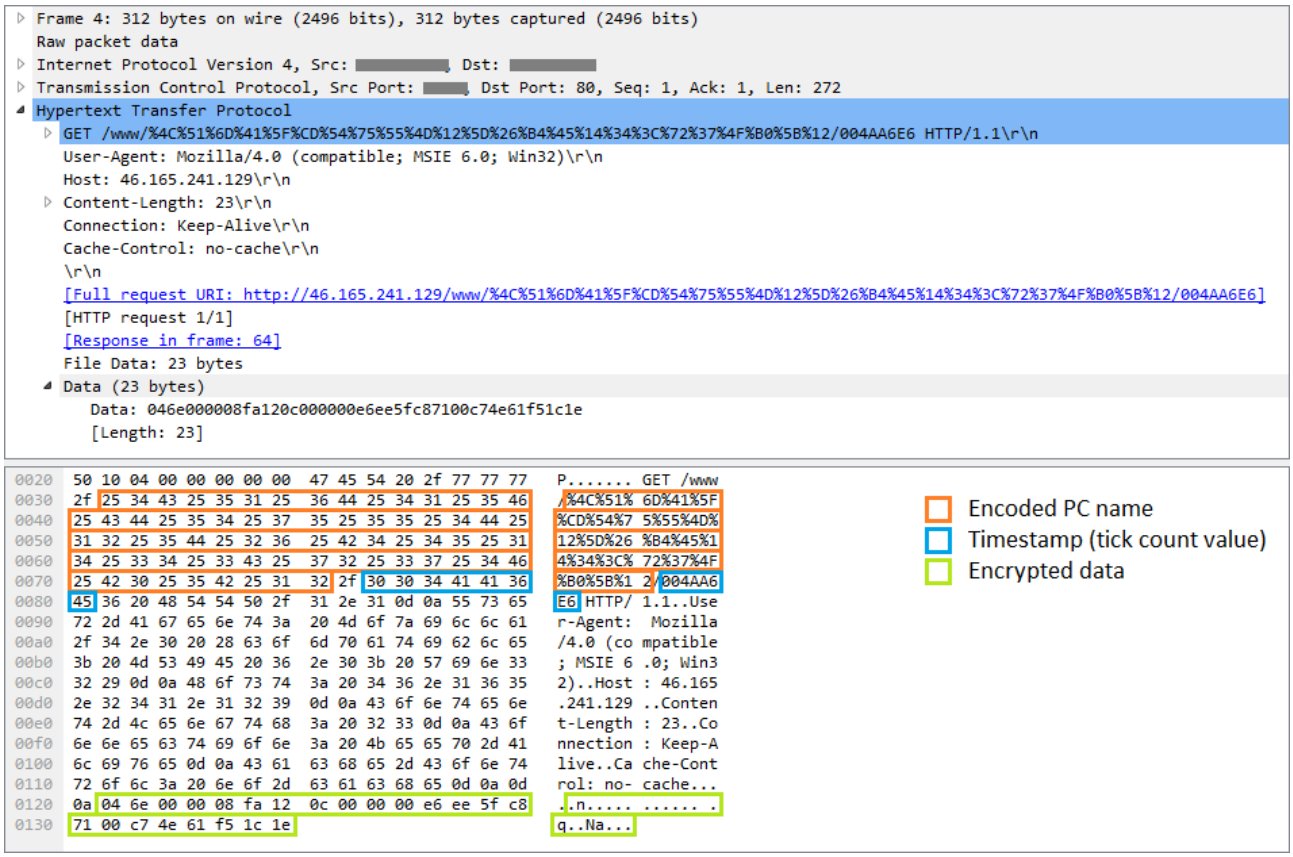

Рисунок 5. Пример запроса, отправляемого на C&C-сервер модулем RC2FM

После успешной регистрации жертвы на C&C-сервере в систему загружается дополнительная информация, которая будет интерпретирована по команде бэкдора.

Функциональные возможности

`RC2FM` поддерживает команды для листинга базовой системной информации и внесения простых изменений в систему, а также несколько шпионских функций. По требованию атакующих модуль может удаленно включать микрофон на скомпрометированном компьютере и записывать аудио. Запись кодируется в формате MP3 с помощью легитимной библиотеки `lame.dll`, которая загружается и используется вредоносной программой.

Еще один инструмент для кражи данных – скриншоты. Одна из команд бэкдора предназначена для создания снимков экрана.

Вредоносная программа следит за всеми встроенными и внешними дисками, отображаемыми в локальной системе. При подключении нового диска она создает список со всеми файлами и хранит его в зашифрованном виде.

Собранная информация будет передана атакующим после отправки соответствующей команды.

Команды бэкдора

Ниже представлены ID и описания поддерживаемых команд. Визуализация функции бэкдора в интерпретаторе показана на рисунке 6.

0 — Составить списки отображаемых дисков, файлов в папке, общих сетевых ресурсов
2 — Создать, переместить, переименовать, выполнить или удалить файл, удалить директорию, использующую заданный путь
4 — Открыть файл, установить указатель в начало файла
5 — Закрыть ранее открытый файл
6 — Записать данные в ранее открытый файл
7 — Изменить файловые атрибуты времени / удалить файл
8 — Открыть файл, установить указатель в конец файла
10 — Изменить файловые атрибуты времени / удалить файл
12 — Найти файлы по заданной маске файла в указанной директории
13 — Сделать скриншот
14 — Загрузить или изменить файлы с помощью внутренних данных
15 — Записать звук с помощью подключенных аудиоустройств, составить список доступных устройств, отправить запись, изменить конфигурацию
16 — Проверить наличие открытых файлов в модуле
17 — Обновить список C&C-серверов
19 — Создать, установить, копировать, перечислить или удалить заданные ключи реестра или значения

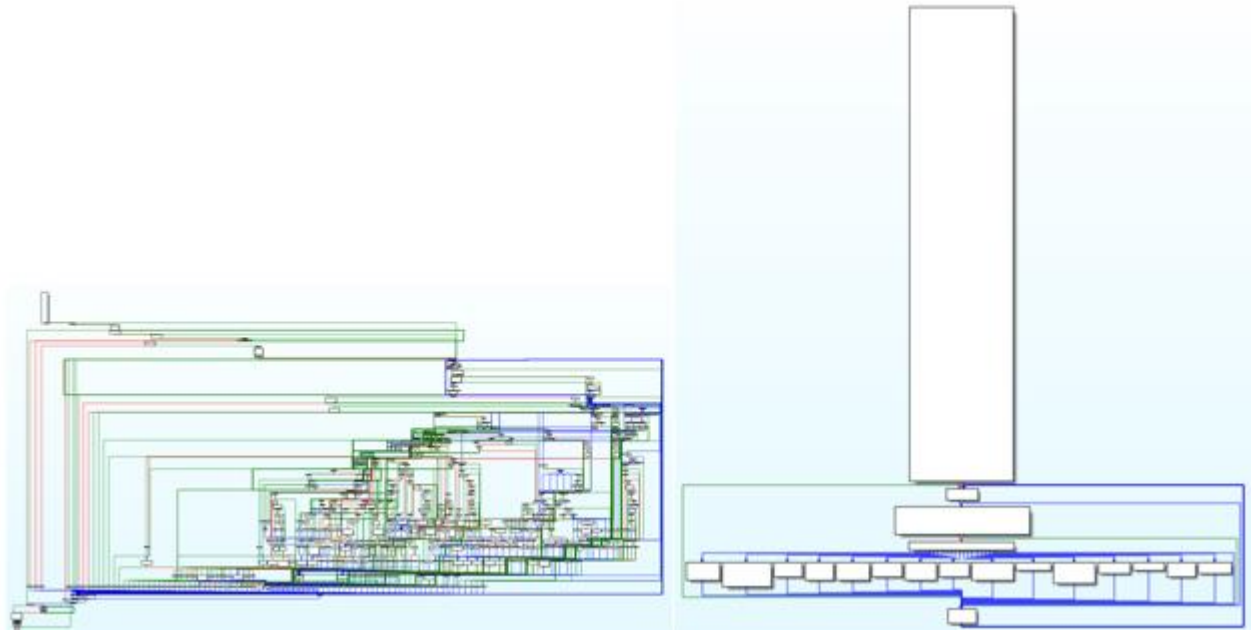

Рисунок 6. Функция бэкдора в интерпретаторе (оригинальная и после нашего анализа, измененная с помощью функции Group Nodes в IDA Pro для удобства чтения)

Модуль RC2CL

Модуль `RC2CL` – также бэкдор с широким списком инструментов шпионажа. Он запускается DLL-оберткой одновременно с модулем `RC2FM`. Это более сложный модуль, его функции, скорее, нацелены на максимальный сбор информации, чем на внесение изменений в систему.

Интересно, что в модуле `RC2CL` предусмотрена опция выключения функционала бэкдора и работы в качестве прокси. В этом случае малварь выключает файервол Windows и создает сервер, который поддерживает коммуникацию между клиентом и C&C-сервером или двумя клиентами.

Сетевая коммуникация

Малварь связывается с C&C-серверами через TCP-сокет. Отправляемые клиентом сообщения маскируются под протокол HTTP, но стоит обратить внимание на недействительный метод HTTP «HIDE» в примере на рисунке 7.

Запросы содержат идентификатор скомпрометированного ПО, тип запроса и зашифрованную информацию, которая подлежит отправке атакующим, то есть результат выполнения команд бэкдора или запрос на получение новых инструкций.

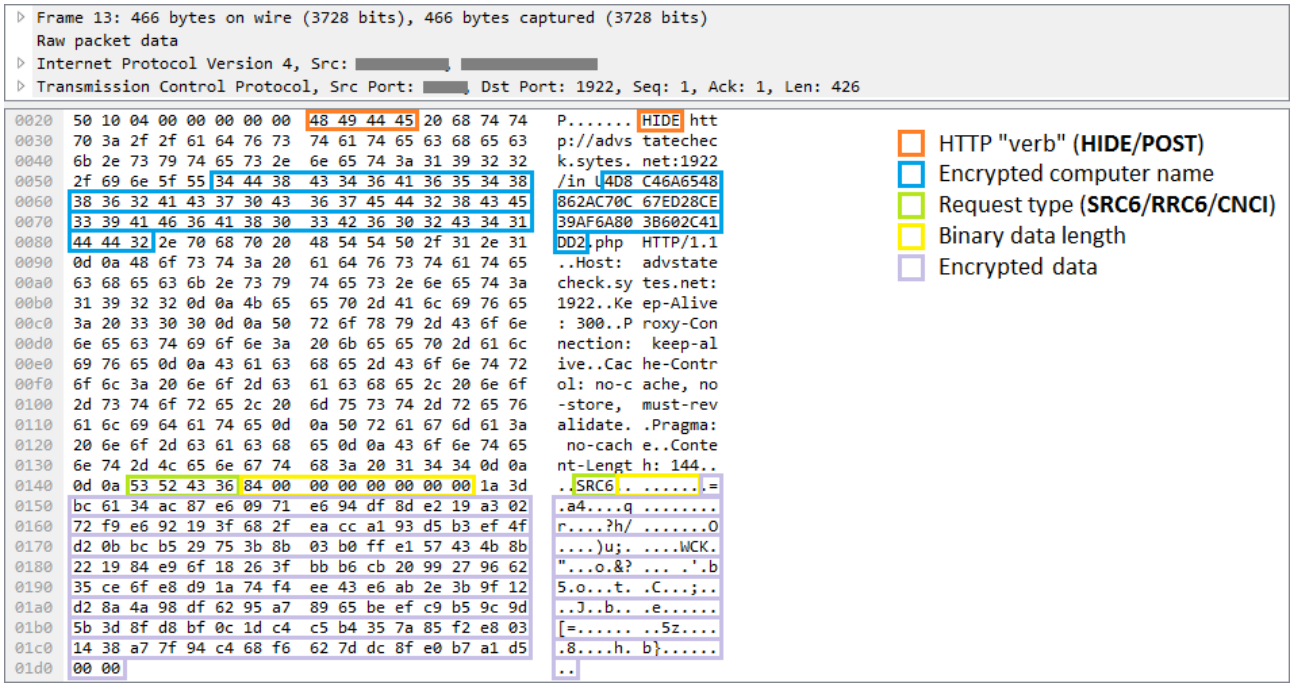

Рисунок 7. Пример запроса, отправляемого на командный сервер модулем RC2CL

Функциональные возможности

В зависимости от полученной команды бэкдор может выполнять различные операции в зараженной системе. Обычные бэкдоры выполняют манипуляции с файловой системой и ключами реестра, поддерживают исполнение файлов и удаленную активацию шеллов. Данная спайварь поддерживает все эти команды и даже больше – 84 команды позволяют атакующим собрать исчерпывающую информацию о жертве.

Вредоносная программа изучает зараженный компьютер и передает атакующим различные данные: системную информацию (список активных процессов, запущенных служб, загруженных драйверов или доступных дисков), сетевую информацию (таблица IP адресов, скорость интернет-соединения).

InvisiMole может сканировать доступные на скомпрометированной системе беспроводные сети. Спайварь фиксирует такую информацию, как SSID и MAC адреса обнаруженных точек доступа Wi-Fi. Эти данные потом можно сверить с публичными базами, что позволяет атакующим отследить геолокацию жертвы.

Другие команды позволяют получить информацию о пользователях скомпрометированной машины, их аккаунтах и предыдущих сеансах.

Особый интерес представляет установленное на скомпрометированной машине ПО. Какие программы установлены в системе? Какие из них автоматически запускаются при старте системы или входе пользователя? Какие программы использует конкретный пользователь? Если атакующих что-то интересует, достаточно ввести одну команду, чтобы получить нужные данные.

Малварь может получить команду на поиск недавно открытых документов и других интересных файлов. Она может просматривать определенные директории и внешние устройства, отчитываться об изменениях и извлекать файлы, выбранные атакующими.

Малварь может включать или выключать систему управления учетными записями (UAC), либо обходить ее и работать с файлами в защищенных директориях без прав администратора (подробнее по ссылке). Если малварь запущена под процессом `explorer.exe`, который автоматически получает повышенные права, она может создавать COM-объект и использовать его для удаления и перемещения файлов в областях, требующих права администратора.

Более того, InvisiMole может удаленно включать веб-камеру и микрофон жертвы, шпионить путем фотосъемки или звукозаписи. Атакующие могут следить за активностью на устройстве, делая скриншоты. Что особенно интересно, InvisiMole позволяет делать скриншоты не только целого экрана, но и каждого открытого окна. Это позволяет атакующим собирать информацию, даже когда окна закрывают друг друга.

Одна из команд бэкдора позволяет заменить содержимое драйверов со следующими именами:

```
blbdrive.sys
compbatt.sys
secdrv.sys
```

Мы не наблюдали применение данной команды атакующими, но можем предположить, что она используется для обеспечения дополнительной персистентности на 32-битных системах.

Бэкдор способен вмешиваться в работу системы (например, разлогиниться за пользователя, завершить процесс или выключить систему), но преимущественно обеспечивает выполнение пассивных операций. Программа по возможности пытается скрыть свою активность.

Так, спайварь исследует интересные места в системе, изучает недавно открытые документы или изменяет некоторые файлы. Эти действия оставляют следы и могут вызвать подозрение жертвы, поскольку после каждой подобной операции меняется время последнего изменения файла и/или доступа к нему. Чтобы предотвратить обнаружение, малварь восстанавливает дату предыдущего изменения или открытия файла, чтобы скрыть от пользователя свои манипуляции.

Еще один пример того, как авторы спайвари пытаются избежать обнаружения – работа с оставляемыми на диске следами. Вредоносная программа собирает большой объем конфиденциальных данных, которые некоторое время хранятся в файлах и удаляются после успешной загрузки на C&C-серверы. Проблема в том, что опытный системный администратор может восстановить удаленные файлы, что поможет в расследовании атаки после того, как жертва узнает о компрометации. Это возможно, поскольку некоторая информация остается на диске даже после удаления файла. Чтобы это предотвратить, InvisiMole имеет функцию безопасного удаления всех файлов. Это означает, что сначала идет перезапись данных нулевыми или рандомными байтами, и только после этого – удаление файла.

Встроенная память

Конфигурация бэкдора и собранные данные хранятся по двум адресам – это рабочая директория и ключи реестра. Значительная часть команд бэкдора предназначена для манипуляций с этими местами хранения данных и их содержимым.

Расположение рабочей директории определено с помощью команд с удаленного сервера. Директория используется как временное хранилище файлов, содержащих собранную со скомпрометированного компьютера информацию. Эти файлы имеют общий способ именования, алгоритм шифрования и структуру. Они шифруются простым вариантом шифра XOR, который используется в компонентах малвари. Тип файла может быть получен из 4-байтной контрольной последовательности, расположенной в начале файла.

Помимо хранения собранных данных, директория используется в качестве домашней для копии легитимного приложения WinRAR.exe. Малварь копирует его и использует для архивации краденных данных.

В реестре хранятся данные конфигурации, а также список файлов в рабочей директории. Данные запакованы с помощью процедуры Zlib, реализованной в бинарном файле малвари, и зашифрованы с помощью того же шифра, что и внутренние файлы.

Имя подкаталога	Имя файла	Последовательность управления	Содержимое файла
\	~mrc_%random%.tmp	932101DA	Аудиозаписи
\	~src_%random%.tmp	958901DA	Аудиозаписи
\	~wbc_%random%.tmp	938901DA	Фото с веб-камеры
sc\	~sc%random%.tmp	DFE43A08	Скриншоты
~zlp\	zdf_%random%.data	B1CBF218	Сжатые Zlib пакеты
~lcf\	tfl_%random%	C0AFF208	Внутренние данные
fl_%timestamp%\strcn %num%\	fdata.dat	A1CAF108	Данные с внешних дисков
fl_%timestamp%\strcn %num%\	index.dat	BAAB0019	Данные с внешних дисков
Winrar\	WinRAR.exe	-	Копия легитимного приложения
Winrar\	comment.txt	-	-
Winrar\	descript.ion	-	-
Winrar\	Default.SFX	-	-
Winrar\	main.ico	-	-

Команды бэкдора

Больше восьмидесяти команд бэкдора используют рабочую директорию и ключи реестра для хранения промежуточных результатов и данных конфигурации. График с отображением бэкдора в интерпретаторе – на рисунке 8.

Примерно треть всех команд относится к чтению и обновлению данных конфигурации, хранимых в реестре. ID и описания остальных команд перечислены ниже.

4 — Составить список информации о файлах в директории
6 — Загрузить файл
20 — Составить список активных процессов
22 — Завершить процесс по ID
24 — Исполнить файл
26 — Удалить файл
28 — Получить таблицу IP-форвардинга
30 — Записать данные в файл
31 — Бездействие
38 — Составить список аккаунтов
40 — Составить список служб в системе
42 — Составить список загруженных драйверов
43 — Собрать базовую системную информацию (имя компьютера, версия ОС, статус памяти, локальное время, информация о дисках, информация о сконфигурированных прокси, текущая политика предотвращения выполнения данных для системы и процессов и др.)
44 — Составить список установленного ПО
46 — Составить список локальных пользователей и информация о сеансах
48 — Составить список приложений, используемых пользователями
52 — Создать структуру директории
78 — Создать удаленный шелл
81 — Выполнить команду через удаленный шелл
91 — Включить / выключить контроль учетных записей пользователей
93 — Завершить сеанс пользователя / выключить / перезапустить систему
101 — Отслеживать и записывать изменения в указанных директориях
103 — Удалить директорию
109 — Включить / выключить монитор / включить режим ожидания
120 — Сделать скриншот дисплея / активных окон
126 — Сделать скриншот дисплея / активных окон и обновить данные конфигурации
130 — Список информации о ресурсах на неразмеченных дисках
132 — Переименовать / переместить файл, изменить время создания / открытия / записи файла на заданное
134 — Составить список недавно открытых файлов
152 — Отключить (ранее подключенные) съемные диски
155 — Создать / удалить ключ реестра, установить / удалить значения ключа реестра, либо перечислить значения реестра / ключей / данных
159, 161 — Выключить маршрутизацию / файервол, создать прокси-сервер на определенном порте
172 — Повторять вывод диалогового окна с требованием перезагрузить компьютер
175 — Обойти контроль учетных записей пользователей для манипуляций с файлом
177 — Создать и записать файл, выставить данные о времени создания / открытия / изменения
181 — Убрать все точки восстановления системы
183 — Сбросить (легитимный) компонент приложения WinRAR
185 — Добавить файлы в запароленный архив (парлоль = «12KsNh92Dwd»)
187 — Расшифровать, распаковать и загрузить DLL, загрузить файлы exe из ресурсов RC2CL, RC2FM

189 — Создать точку восстановления системы
191 — Извлечь запароленный архив (12KsNh92Dwd)
193 — Изменить зашифрованный файл
195 — Перезапустить после завершения основного процесса
197 — Отправить 198 байтов жестко запрограммированных данных в образце
199 — Переименовать / переместить файл
206 — Расшифровать, распаковать и загрузить DLL, загрузить файлы exe из ресурсов RC2CL, RC2FM
211 — Загрузить собранную информацию (скриншоты, аудиозаписи и др.)
213 — Составить список активных окон
218 — API для записи аудио с входа устройств
220 — API для съемки фотографий с веб-камеры
224 — Составить список файлов, исполняемых при каждом старте системы
226 — Составить список включенных беспроводных сетей (MAC-адрес, SSID, сигнальный интервал)
228 — Сбросить сжатый Zlib пакет

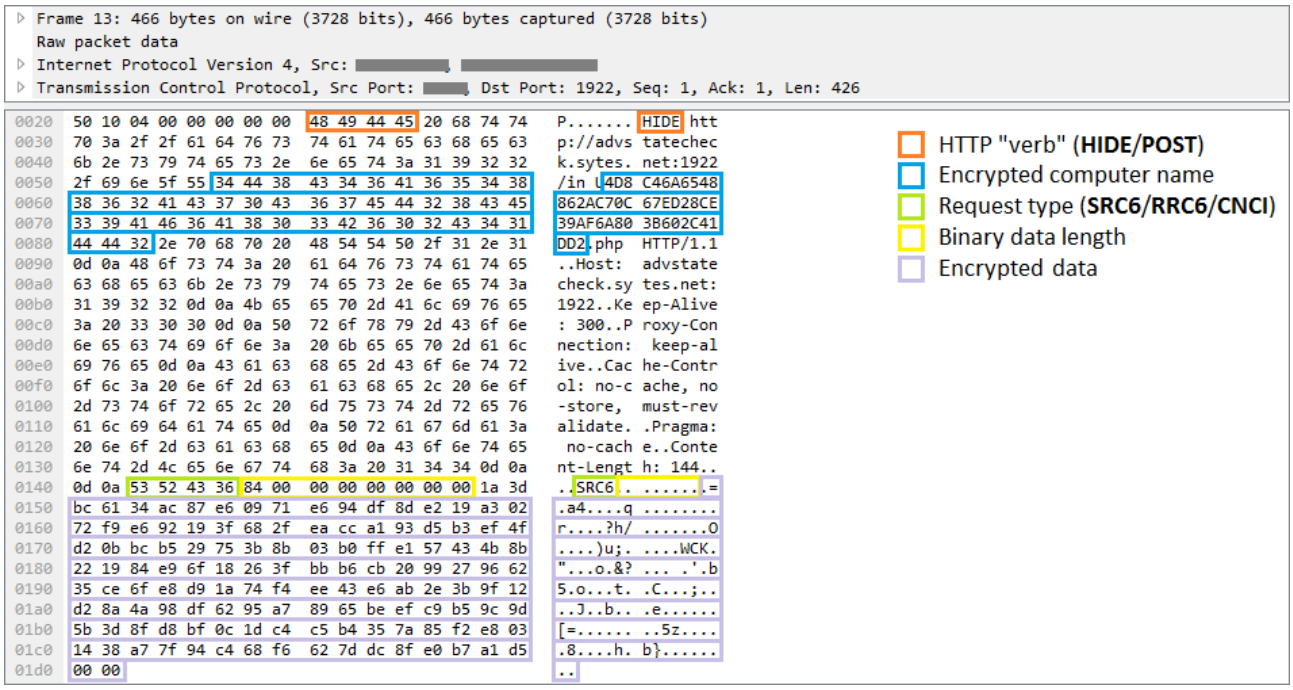

Рисунок 8. Функция бэкдора в интерпретаторе (оригинальная и измененная с помощью функции Group Nodes в IDA Pro для удобства чтения)

Заключение

InvisiMole – полнофункциональное шпионское ПО, широкие возможности которого позволяют конкурировать с другими известными инструментами кибершпионажа.

Можно только догадываться, почему авторы используют два модуля с дублирующими функциями. Можно было бы предположить, что меньший модуль, `RC2FM`, используется на первом этапе разведки, а больший, `RC2CL`, запускается только на машинах, заинтересовавших операторов. Но это не так – два модуля запускаются одновременно. Второе возможное объяснение: модули собраны разными авторами, а затем объединены, чтобы обеспечить операторов максимумом инструментов.

InvisiMole использует лишь несколько техник, чтобы избежать обнаружения и анализа. Тем не менее, поскольку спайварь применялась в атаках на небольшое число высокопоставленных объектов, ей удавалось избегать обнаружения как минимум пять лет.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации (IoCs)

Детектирование продуктами ESET

```
Win32/InvisiMole.A trojan
Win32/InvisiMole.B trojan
Win32/InvisiMole.C trojan
Win32/InvisiMole.D trojan
Win64/InvisiMole.B trojan
Win64/InvisiMole.C trojan
Win64/InvisiMole.D trojan
```

Хеши SHA-1

```
5EE6E0410052029EAFA10D1669AE3AA04B508BF9
2FCC87AB226F4A1CC713B13A12421468C82CD586
B6BA65A48FFEB800C29822265190B8EAEA3935B1
C8C4B6BCB4B583BA69663EC3AED8E1E01F310F9F
A5A20BC333F22FD89C34A532680173CBCD287FF8
```

Имена доменов C&C-серверов

```
activationstate.sytes[.]net
advstatecheck.sytes[.]net
akamai.sytes[.]net
statbfnl.sytes[.]net
updchecking.sytes[.]net
```

IP-адреса C&C-серверов и период активности

```
2013-2014 - 46.165.231.85
2013-2014 - 213.239.220.41
2014-2017 - 46.165.241.129
2014-2016 - 46.165.241.153
2014-2018 - 78.46.35.74
2016-2016 - 95.215.111.109
2016-2018 - 185.118.66.163
2017-2017 - 185.118.67.233
2017-2018 - 185.156.173.92
2018-2018 - 46.165.230.241
2018-2018 - 194.187.249.157
```

Ключи реестра и значения

RC2FM

```
[HKEY_CURRENT_USER\Software\Microsoft\IE\Cache]
"Index"
```

RC2CL

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Console]
or [HKEY_CURRENT_USER\Software\Microsoft\Direct3D]
```

```
"Settings"
"Type"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE]
or [HKEY_CURRENT_USER\Software\Microsoft\Direct3D]
"Common"
"Current"
"ENC"
"FFLT"
"Flag1"
"FlagLF"
"FlagLF2"
"IfData"
"INFO"
"InstallA"
"InstallB"
"LegacyImpersonationNumber"
"LM"
"MachineAccessStateData"
"MachineState 0"
"RPT"
"SP2"
"SP3"
"SettingsMC"
"SettingsSR1"
"SettingsSR2"
```

Файлы и папки

RC2FM

```
%APPDATA%\Microsoft\Internet Explorer\Cache\AMB6HER8\
%volumeSerialNumber%.dat
content.dat
cache.dat
index.dat
%APPDATA%\Microsoft\Internet Explorer\Cache\MX0ROSB1\
content.dat
index.dat
%random%.%ext%
%APPDATA%\Microsoft\Internet Explorer\Cache\index0.dat
```

RC2CL

```
Winrar\
comment.txt
descript.ion
Default.SFX
WinRAR.exe
main.ico
fl_%timestamp%\strcn%num%\
fdata.dat
index.dat
~mrc_%random%.tmp
~src_%random%.tmp
~wbc_%random%.tmp
sc\~sc%random%.tmp
~zlp\zdf_%random%.data
~lcf\tfl_%random%
```