InvisiMole: складне шпигунське програмне забезпечення, яке залишалося невиявленим з 2013 року

Націлене на високопрофільні об’єкти, полює на секретну інформацію та діє таємно.

Такий принцип роботи двох шкідливих компонентів InvisiMole. Вони перетворюють інфікований комп'ютер у відеокамеру, дозволяючи зловмисникам бачити і чути, що відбувається в офісі жертви. Кіберзлочинці ховаються в системі, уважно стежачи за діяльністю жертв та викрадаючи їх секретну інформацію.

За даними телеметрії ESET, шкідливе програмне забезпечення було активним щонайменше з 2013 року, проте інструмент для кібершпигунства ніколи не аналізувався та залишався непоміченим до того часу, поки його не виявили системи ESET на інфікованих комп'ютерах в Україні та Росії.

Кампанія є цілеспрямованою, тому шкідливе програмне забезпечення має низький рівень інфікування з кількома десятками інфікованих комп'ютерів.

InvisiMole має модульну архітектуру, починаючи своє поширення з модифікованої DLL та двох вбудованих модулів. Обидва модулі – багатофункціональні бекдори, які разом забезпечують можливості збирати якомога більше інформації про інфіковану ціль.

Для приховування власної діяльності від інфікованого користувача використовуються додаткові заходи, які дозволяють шкідливій програмі залишатися в системі протягом тривалого часу. Поки триває дослідження щодо того, як шпигунське програмне забезпечення потрапляло на інфіковані машини. Можливими є всі вектори інфікування, включаючи інсталяцію з фізичним доступом до машини.

Інсталяція та стійкість

Першою частиною шкідливого програмного забезпечення є модифікована DLL, скомпільована за допомогою Free Pascal Compiler. Відповідно до даних телеметрії ESET, ця DLL розміщена у папці Windows та маскується під легітимну бібліотеку mpr.dll з підробленою інформацією версії у своїх ресурсах.

```
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 – Модифікована DLL маскується під легітимну бібліотеку mpr.dll як за назвою, так і за інформацією версії

Спеціалісти ESET не зафіксували модифікованої DLL з іншим ім'ям; однак у коді DLL є вказівки на те, що вона також могла бути названа `fxsst.dll` або `winmm.dll`.

Перший спосіб запуску шкідливого програмного забезпечення — це використання підміни DLL. Розміщуючись у тій самій папці, що і explorer.exe, модифікована DLL завантажується під час запуску Windows у процесі Windows Explorer замість легітимної бібліотеки, що розміщена в папці system32.

Будучи розміщеною у тій самій папці, що і `explorer.exe`, модифікована DLL завантажується під час запуску Windows у процесі провідника Windows замість оригінальної бібліотеки, розташованої у папці `%windir%\system32`.

Спеціалісти виявили як 32-бітну, так і 64-бітну версію шкідливого програмного забезпечення, що робить даний метод функціональним для обох архітектур.

Як альтернатива DLL, можливі також інші способи завантаження та інсталяції. Модифікована DLL експортує функцію `GetDataLength`. Під час виклику функції DLL перевіряє, чи була вона завантажена процесом `rundll32.exe` за допомогою `explorer.exe` або `svchost.exe`, і лише тоді запускає компонент. Це передбачає інші можливі методи стійкості шляхом планування завдання (наприклад, використання `svchost.exe` як батьківського процесу) або шляхом інсталяції у ключі автозавантаження реєстру (`explorer.exe` використовується як батьківський процес).

Незалежно від методу стійкості поведінка шкідливого програмного забезпечення та фактичний компонент однакові у всіх випадках. Модифікована DLL завантажує модулі з іменами `RC2FM` та `RC2CL`, і (якщо було застосовано підміну DLL), нарешті завантажується фактична легітимна бібліотека в процес `explorer.exe`, щоб не порушувати нормальну роботу програми та залишатися непоміченими.

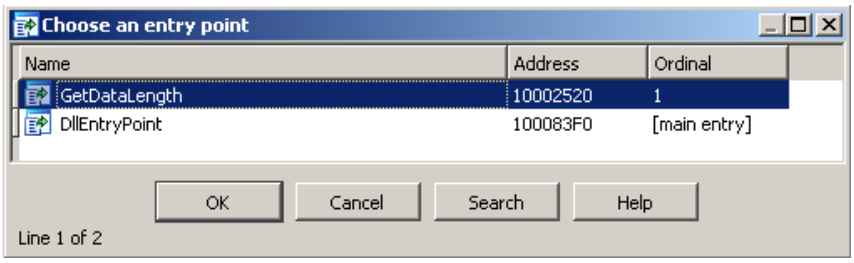


Рисунок 2 – Експортовані функції модифікованої DLL

Технічний аналіз

Точна дата, коли шкідливе програмне забезпечення було скомпільовано, невідома, останні зразки модифікованої DLL були відредаговані авторами шкідливої програми, а часові позначки PE вручну встановлені на нульове значення. Проте в ході дослідження спеціалісти ESET виявили ранню версію шкідливого програмного забезпечення з часовою позначкою PE 13 жовтня 2013 року, тому дата компіляції останньої версії є, напевно, новішою.

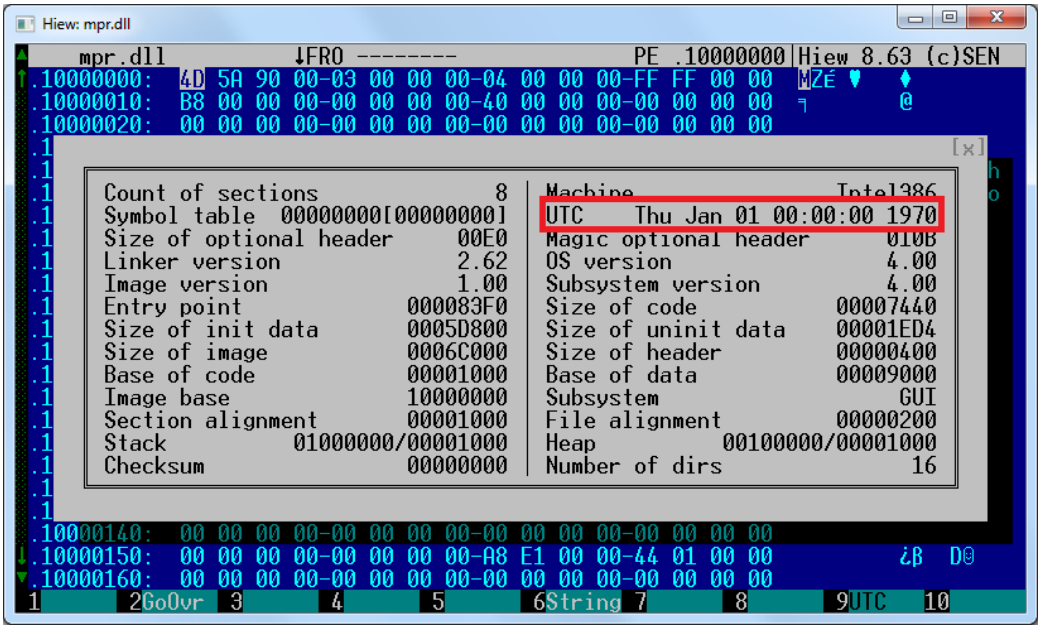
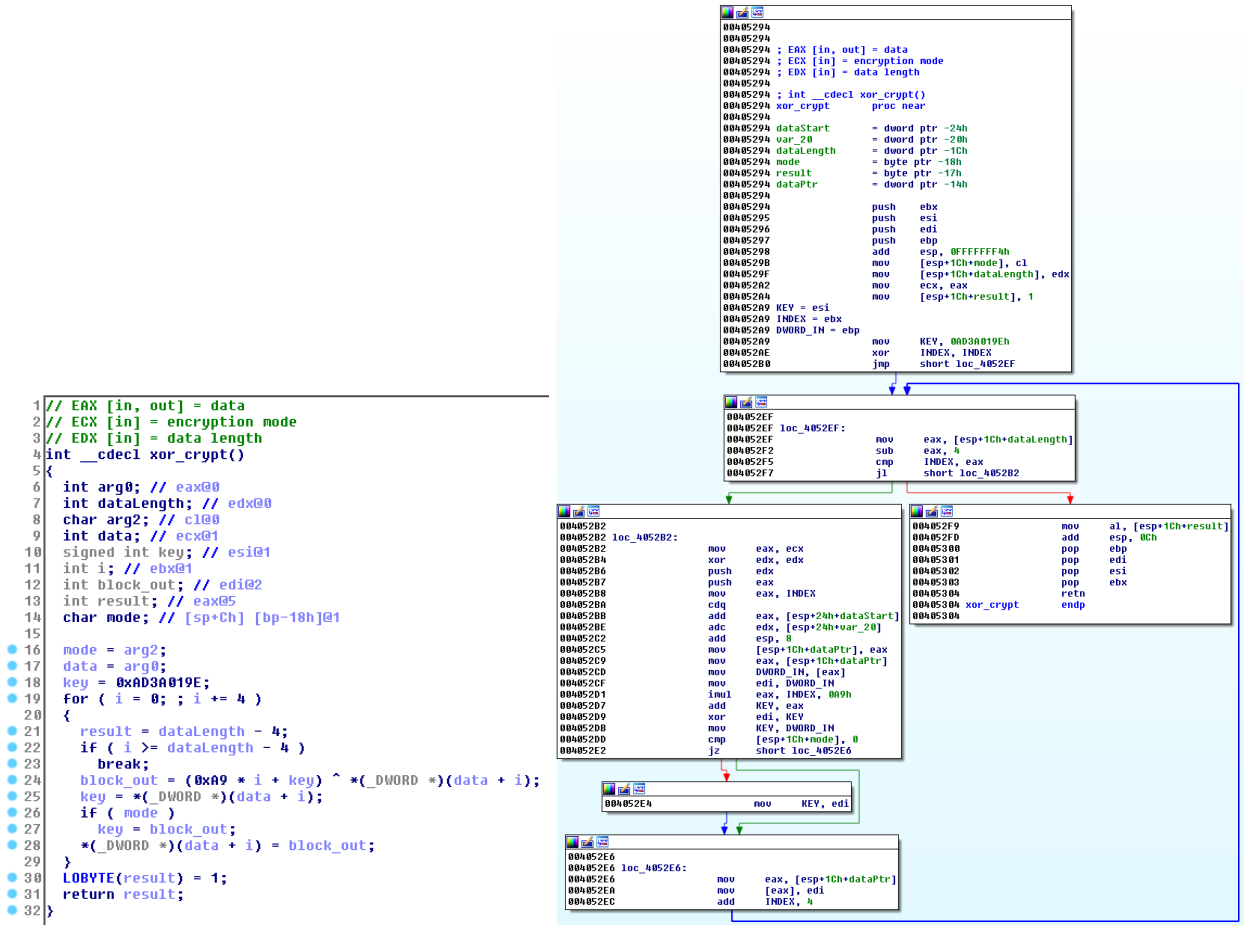


Рисунок 3 – У всіх останніх зразках встановлена нульова часова позначка компіляції

Шифрування та дешифрування

Шкідлива програма приховує власну діяльність від адміністраторів та аналітиків шляхом шифрування власних рядків, внутрішніх файлів, даних конфігурації та мережевого зв'язку. У той час як модуль `RC2FM` використовує декілька процедур шифрування, модифікованої DLL та модуль `RC2CL` використовують одну процедуру для всіх цілей, особливо для дешифрування інших модулів шкідливого програмного забезпечення, вбудованих в модифікований DLL.

Скрипт, який здатний витягнути вбудовані модулі `RC2FM` та `RC2CL` з модифікованої DLL, використовуючи цю процедуру, доступний у [дослідженні ESET у сховищі GitHub](#).



```
// EAX [in, out] = data
// ECX [in] = encryption mode
// EDX [in] = data length
int __cdecl xor_crypt()
{
  int arg0; // eax@0
  int dataLength; // edx@0
  char arg2; // cl@0
  int data; // ecx@1
  signed int key; // esi@1
  int i; // ebx@1
  int block_out; // edi@2
  int result; // eax@5
  char mode; // [sp+Ch] [bp-18h]@1

  mode = arg2;
  data = arg0;
  key = 0xAD3A019E;
  for ( i = 0; ; i += 4 )
  {
    result = dataLength - 4;
    if ( i >= dataLength - 4 )
      break;
    block_out = (0xA9 * i + key) ^ *(_DWORD *)(data + i);
    key = *(_DWORD *)(data + i);
    if ( mode )
      key = block_out;
    *(_DWORD *)(data + i) = block_out;
  }
  LOBYTE(result) = 1;
  return result;
}
```

Рисунок 4 – Шифрування, що використовується у всіх зразках (декомпільовано та розібрано).

Модуль RC2FM

Перший, менший модуль `RC2FM` містить бекдор, що підтримує 15 команд, які виконуються на інфікованих комп'ютерах зловмисниками. Модуль призначений для внесення різних змін у систему, а також пропонує ряд шпигунських команд.

Параметр збору журналів реалізований, але назва файлу журналу не налаштовується у проаналізованому зразку. Це свідчить про те, що він використовувався лише під час розробки шкідливого програмного забезпечення.

Мережеве з'єднання

Модуль з'єднується з командними серверами (C&C), які закодовані у зразку, та можуть бути оновлені зловмисниками.

Більше того, модуль може з’єднуватися з командними серверами (C&C), навіть якщо на інфікованому комп'ютері налаштовано проксі. Якщо пряме з'єднання не виконується, модуль намагається підключитися до будь-якого з командних серверів за допомогою локально налаштованих проксі-серверів або проксі-серверів, налаштованих у різних браузерах (Firefox, Pale Moon та Opera).

Модуль може використовувати пошук нещодавно виконаних додатків і спеціально шукати виконувані файли портативних браузерів:

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

Якщо жертва використовує портативний браузер з налаштованим проксі-сервером, загроза може знаходити це в налаштуваннях користувача та використовувати проксі для з’єднання з командними серверами.

Фактична комунікація складається із серії запитів HTTP GET та POST, як показано на рисунку 5. Зашифрований запит включає в себе ідентифікатор ПК та часовий покажчик, а також інші дані. Варто зазначити, що модуль `RC2FM` використовує цілий ряд методів шифрування (варіанти простих процедур шифрування XOR), на відміну від інших частин InvisiMole.

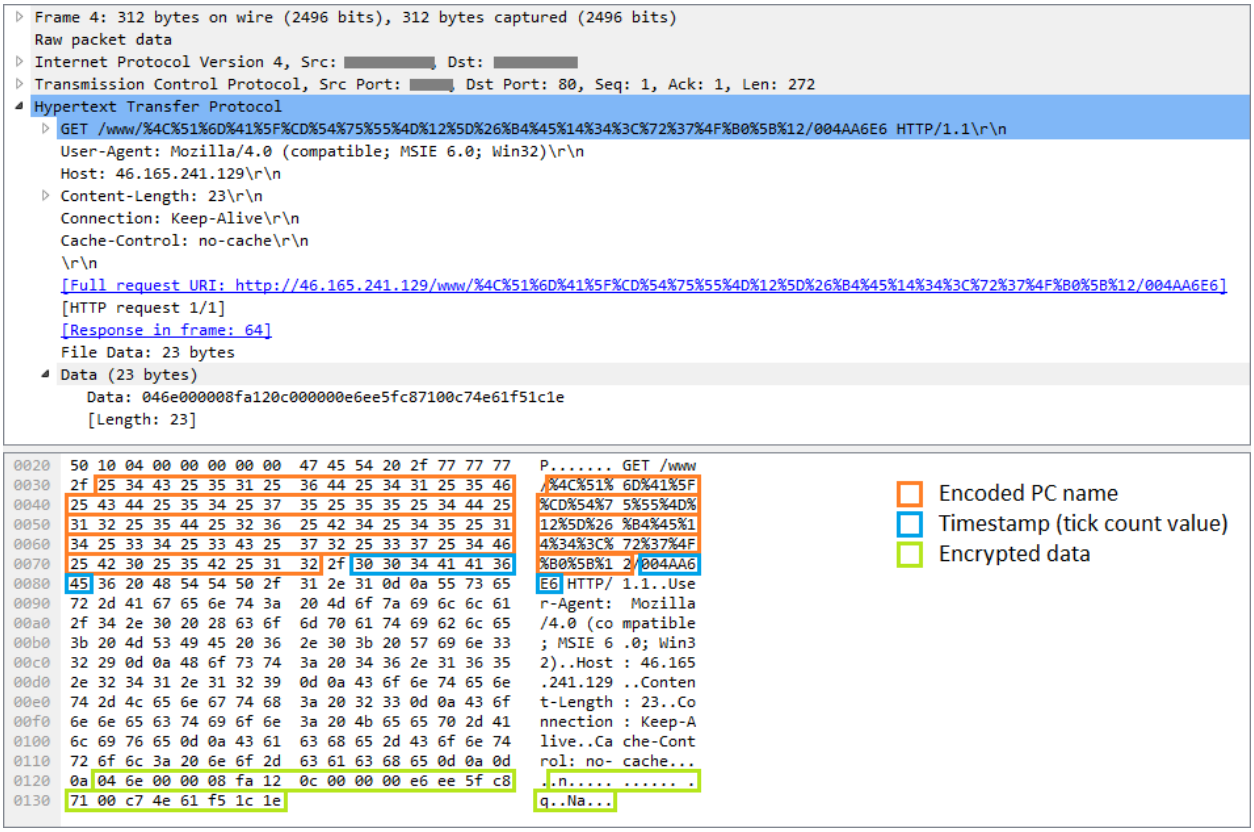


Рисунок 5 – Приклад запиту, надісланого командному серверу модулем `RC2FM`

Після успішної реєстрації жертви на командному сервері завантажуються додаткові дані, які інтерпретуються на локальному комп'ютері як команди бекдора.

Можливості

`RC2FM` підтримує команди для відображення основної системної інформації та виконання простих змін у системі, а також включає в себе кілька шпигунських функцій. Модуль здатний дистанційно активувати мікрофон на зараженому комп'ютері та захоплювати звук за запитом зловмисників. Аудіозаписи кодуються у формат MP3 за допомогою легітимної `lame.dll` бібліотеки, яка завантажується та використовується шкідливим програмним забезпеченням.

Іншим способом, за допомогою якого шкідлива програма може отримувати доступ до конфіденційних даних жертви, є можливість робити знімки екрану, що є ще однією командою бекдора.

Шкідливе ПЗ також відстежує всі фіксовані та змінні диски в локальній системі. Кожного разу, коли вставляється новий диск, шкідлива програма створює список всіх файлів на диску і зберігає його в зашифрованому вигляді у файлі.

Усі зібрані дані можуть бути відправлені зловмисникам, коли така команда буде надана.

Команди бекдора

Підтримується п'ятнадцять команд, які зазначено нижче. Функцію інтерпретатора бекдора візуалізовано на рисунку 6.

Команди ID	Опис команди
0	Зберегти інформацію про пов'язані диски, список файлів у папці, список мережевих ресурсів
2	Створювати, переміщувати, перейменовувати, виконувати або видаляти файли, видаляти каталог, використовуючи певний шлях
4	Відкрити файл, встановлювати вказівник на початок файлу
5	Закрити раніше відкритий файл
6	Записати дані у раніше відкритий файл
7	Змінити час файлу / видалити файл
8	Відкрити файл, встановити вказівник файлу на кінець файлу
10	Модифікувати час файлу / видалити файл
12	Шукати файл за маскою файлу у певному каталозі
13	Зробити знімок екрану
14	Завантажувати або змінювати файли з внутрішніми даними
15	Записувати звук за допомогою аудіопристроїв, зберегти доступні пристрої, надсилати записи, змінити конфігурацію
16	Перевіряти, чи певний файл наразі відкритий
17	Оновити перелік командних серверів (C&C)
19	Створювати, встановлювати, копіювати, підраховувати або видаляти певні ключі реєстру або значення

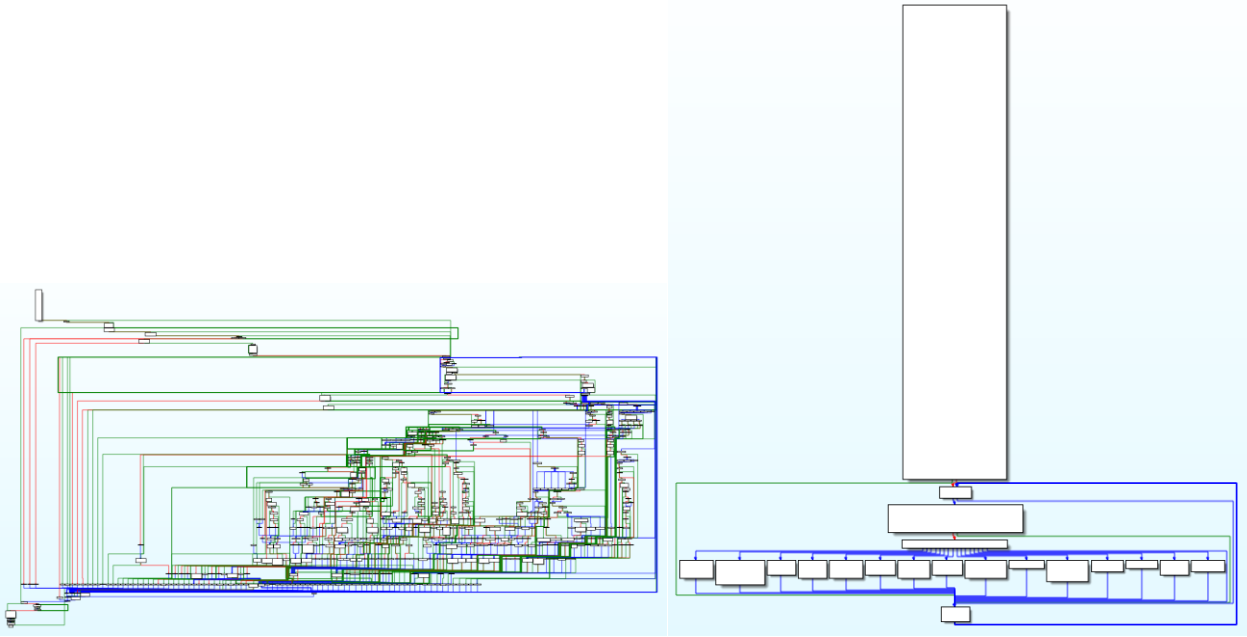


Рисунок 6 – Функції інтерпретатора бекдора (оригінал і після аналізу змінено за допомогою Group Nodes функціональності IDA Pro для кращої читабельності).

Модуль RC2CL

Модуль RC2CL також є бекдором з широкими можливостями шпигування. Він запускається за допомогою модифікованої DLL разом з модулем RC2FM. Цей модуль є більш складним та пропонує функції для збору якнайбільшої кількості даних про інфікований комп'ютер, а не для внесення змін в систему.

Цікаво, що в модулі RC2CL є опція вимкнення функціоналу бекдора та увімкнення фунціоналу проксі-сервера. У цьому випадку шкідливе програмне забезпечення вимикає брандмауер і створює сервер, який пересилає з'єднання між клієнтом і командним сервером або між двома клієнтами.

Мережеві з’єднання

Шкідливе програмне забезпечення з’єднується з командними серверами через сокет TCP. Повідомлення, відправлені від клієнта, імітують протокол HTTP (зверніть увагу на неправильний оператор «HIDE» HTTP в прикладі на рисунку 7).

Запити містять ідентифікатор інфікованого комп’ютера, тип запиту та зашифровані дані, що надсилаються зловмисникам, тобто результати команд бекдора або звернення за додатковими інструкціями.

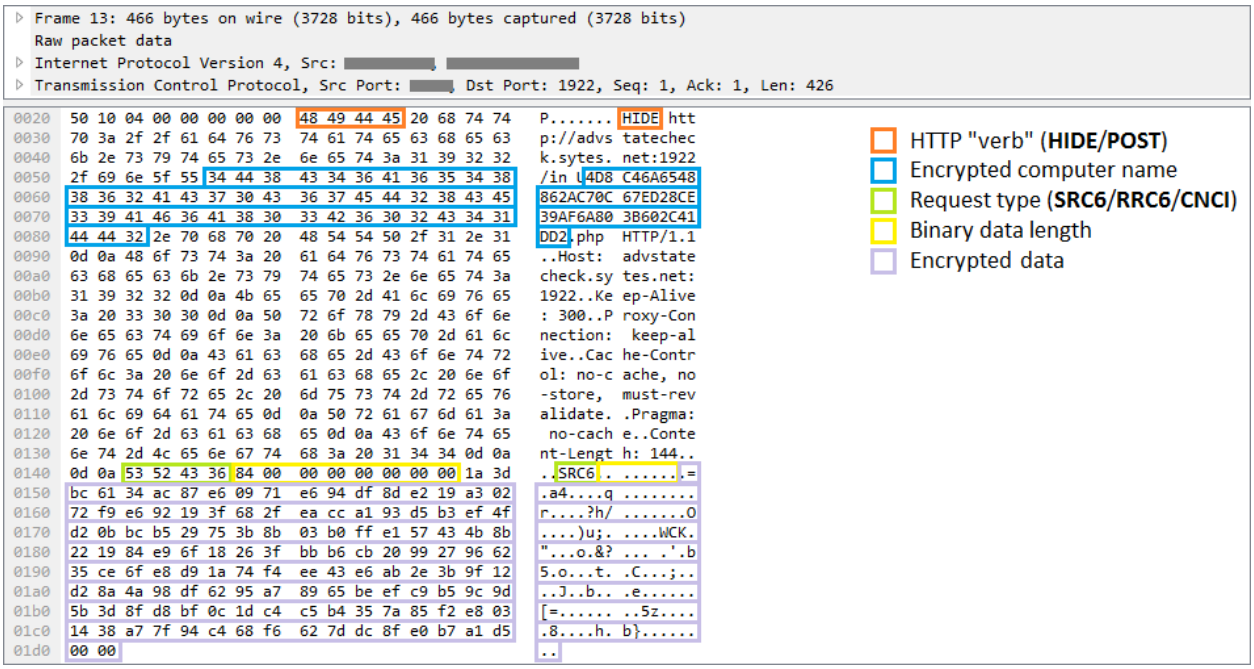


Рисунок 7 – Приклад запиту, відправленого на командний сервер за допомогою модуля RC2CL

Можливості

Залежно від отриманих команд бекдор може виконувати різні дії на інфікованому комп'ютері. Поширені бекдори часто підтримують такі команди, як операції з файловою системою, виконання

файлів, маніпулювання ключами реєстру або активація віддаленого командного рядка. Це шпигунське програмне забезпечення підтримує всі ці інструкції та багато іншого, його 84 команди надають зловмисникам все, що потрібно для пильного спостереження за жертвою.

Шкідлива програма може перевіряти інфікований комп'ютер та надавати різні дані – від системної інформації, такої як список активних процесів, запущених служб, завантажених драйверів або доступних дисків, до інформації про мережу, включаючи таблицю перенаправлення IP та швидкість підключення до мережі Інтернет.

Шкідливе програмне забезпечення InvisiMole здатне сканувати доступні бездротові мережі в інфікованій системі. Воно записує таку інформацію, як ідентифікатор служби та MAC-адресу видимих точок доступу WiFi. Потім ці дані можуть бути об'єднані з публічними базами даних, дозволяючи злочинцям відслідковувати географічне розташування жертви.

Інші команди можуть надавати інформацію про користувачів інфікованого комп'ютера, інформацію про їхні облікові записи та попередні сеанси.

Особливий інтерес становить програмне забезпечення, встановлене на інфікованому комп'ютері. Які програми встановлені в системі? Які з них виконуються автоматично з кожним запуском системи або входом користувача? Які програми використовуються певним користувачем? Якщо зловмисники зацікавлені, ці цінні дані можна отримати за допомогою лише однієї команди.

Шкідливе програмне забезпечення може шукати нещодавно використані документи або інші файли. Воно здатне відстежувати певні каталоги та змінні пристрої, повідомляти про будь-які зміни та вилучати файли відповідно до вибору зловмисників.

Шкідлива програма може включати або відключати User Account Control (UAC) або навіть обходити UAC і працювати з файлами в захищених директоріях без права адміністратора (детальніше на сторінці https://wikileaks.org/ciav7p1/cms/page_3375231.html). Оскільки шкідливе програмне забезпечення запускається в процесі `explorer.exe`, який стартує автоматично, він може створювати COM-об'єкт з підвищеними правами і використовувати його для видалення або переміщення файлів у місцях, які вимагають прав адміністратора.

Шкідлива програма також може дистанційно активувати веб-камеру та мікрофон жертви та шпигувати за жертвою шляхом зйомки та звукозапису. Діяльність екрана може контролюватися за допомогою знімків екрана. Зокрема шкідлива програма здатна робити знімки екрану не тільки всього дисплею, але й кожного вікна, що допомагає злочинцям отримувати більше інформації, навіть якщо вікна перекриваються.

Крім того, одна з команд бекдора використовується для заміни вмісту драйверів з такими іменами:

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

Спеціалісти ESET не зафіксували, як зловмисники використовують цю команду, але можна припустити, що це потрібно для досягнення додаткової стійкості на 32-бітних системах.

Хоча бекдор здатний втрутитися в систему (наприклад, вийти з профілю користувача, завершити процес або вимкнути систему), він, в основному, здійснює пасивні операції. Коли це можливо, він намагається приховати свою діяльність.

Наприклад, шкідливі програми збирають інформацію в цікавих місцях системи, читають останні документи або навіть модифікують деякі файли. Це залишає сліди в системі і може викликати підозру жертви, оскільки час останнього доступу або зміни файлів змінюється з кожною такою діяльністю. Щоб запобігти цьому, шкідливе програмне забезпечення завжди відновлює вихідний час доступу до файлів або модифікації, щоб користувач не здогадувався про операції зловмисників.

Іншим приклад того, як автори шкідливого програмного забезпечення намагаються діяти таємно, є спосіб обробки слідів, залишених на диску. Шкідлива програма збирає велику кількість конфіденційних даних, які тимчасово зберігаються у файлах та видаляються після успішного завантаження на командні сервери. Проте навіть видалені файли можуть бути відновлені досвідченим системним адміністратором, що може допомогти подальшому розслідуванню атаки після того, як жертва дізналася про неї. Це можливо завдяки тому, що деякі дані все ще зберігаються на диску навіть після видалення файлу. Щоб запобігти цьому, шкідливе програмне забезпечення має можливість безпечно видаляти всі файли, а це означає, що воно спочатку перезаписує дані у файлі нульовими або випадковими байтами, а тільки потім файл видаляється.

Внутрішнє сховище

Конфігурація бекдора та зібрані дані зберігаються в одному з двох місць — робочому каталозі та робочих ключах реєстру. Значна частина команд бекдорів призначена для управління місцями зберігання та їхнім контентом.

Розташування робочого каталогу визначається інструкціями віддаленого сервера. Цей каталог використовується як тимчасове сховище для файлів, що містять зібрані дані про інфікований комп'ютер. Такі файли мають спільну назву, алгоритм шифрування та структуру. Вони шифруються за допомогою простого варіанта шифру XOR, який використовується для компонентів шкідливого програмного забезпечення. Тип файлу може бути виведено з 4-байтних контрольних послідовностей, розміщених на початку файлів.

Крім того, що є сховищем для зібраних даних, робочий каталог також є домом для легітимної програми WinRAR. Вона встановлюється шкідливим програмним забезпеченням і використовується зловмисниками для стиснення даних, які слід відфільтрувати.

Робочі ключі реєстру зберігають дані конфігурації, а також список файлів у робочому каталозі. Дані упаковуються за допомогою процедури Zlib і шифруються тим самим шифром, що й внутрішні файли.

Структура робочого каталогу

Назва підкаталогу	Назва файлу	Контрольні послідовності	Вміст файлу
\	~mrc_%random%.tmp	932101DA	Audio records
\	~src_%random%.tmp	958901DA	Audio records
\	~wbc_%random%.tmp	938901DA	Webcam photos
sc\	~sc%random%.tmp	DFE43A08	Screenshots
~zlp\	zdf_%variable%.data	B1CBF218	Zlib packages
~lcf\	tfl_%random%	C0AFF208	Internal data
fl_%timestamp%\strcn%num%\	fdata.dat	A1CAF108	Data from removable drives
fl_%timestamp%\strcn%num%\	index.dat	BAAB0019	Data from removable drives
Winrar\	comment.txt	-	WinRAR component
Winrar\	descript.ion	-	WinRAR component
Winrar\	Default.SFX	-	WinRAR component
Winrar\	WinRAR.exe	-	WinRAR component
Winrar\	main.ico	-	WinRAR component

Команди бекдора

Бекдор забезпечує понад вісімдесят команд, які використовують робочий каталог і ключі реєстру для зберігання їх проміжних результатів та даних конфігурації.

Приблизно третина команд присвячена читанню та оновленню даних конфігурації, що зберігаються в реєстрі. Решта команд наведено нижче.

Команда ID (s)	Опис команди
4	Занести до списку інформацію про файли в каталозі
6	Завантажити файл
20	Занести до списку інформацію про активні процеси
22	Зупинити процес за ID
24	Виконати файл
26	Видалити файл
28	Отримати таблицю перенаправлення IP
30	Записати дані до файлу
31	Сон
38	Занести до списку інформацію про облікові записи
40	Занести до списку інформацію про сервіси в системі
42	Занести до списку інформацію про завантажені драйвери

43	Зібрати базову системну інформацію (назва комп’ютера, версія ОС, статус пам’яті, місцевий час, інформація про диски, інформація про конфігурацію проксі, DEP політику системи та процесів...)
44	Занести до списку інстальоване програмне забезпечення
46	Занести до списку локальних користувачів та інформацію про сеанс
48	Занести до списку додатки, до яких мають доступ користувачі
52	Створити структуру каталогу
78	Створити віддалений командний процесор
81	Виконати команду через віддалений командний рядок
91	Увімкнути/вимкнути UAC
93	Вихід з профілю користувача/вимкнення/перезавантаження системи
101	Моніторинг та запис змін у певних каталогах
103	Видалити каталоги
109	Увімкнути/вимкнути/перевести монітор у режимі очікування
120	Зробити знімки екрану/активних вікон
126	Зробити знімки екрану/активних вікон + оновити дані конфігурації
130	Занести до списку інформацію про ресурси на невстановлених пристроях
132	Перейменувати/перемістити файл, змінити час створення/доступу/запису файлу до заданих значень
134	Занести до списку інформацію про нещодавно відкриті файли
152	Від'єднати (раніше з'єднані) віддалені пристрої
155	Створити/видалити ключ реєстру, встановити/видалити значення параметра реєстру або порахувати значення/ключі/дані реєстру
159, 161	Вимкнути маршрутизацію/брандмауер, створити проксі-сервер на вказаному порту
172	Неодноразово відображати діалогове вікно із запитом на перезавантаження комп'ютера
175	Обхід UAC для управління файлом
177	Створити та записати файл, встановити час створення/доступу/зміни
181	Видалити всі точки відновлення системи
183	Завантажити компоненти WinRAR
185	Додати файли до захищеного паролем архіву (12KsNh92Dwd)
187	Розшифрувати, розпакувати та завантажувати DLL, завантажувати виконувані файли з його ресурсів RC2CL, RC2FM
189	Створити точку відновлення системи
191	Видобути файли з захищеного паролем архіву (12KsNh92Dwd)
193	Модифікувати зашифрований файл
195	Перезавантажуватися після завершення первинного процесу
197	Надіслати 198 байт даних, закодованих у зразку
199	Перейменувати/перемістити файл
206	Розшифрувати, розпакувати та завантажити DLL, завантажити виконувані файли RC2CL, RC2FM з його ресурсів
211	Завантажити зібрану інформацію (знімки екрана, аудіозаписи тощо)
213	Занести до списку інформацію про активні вікна
218	API для запису вхідних аудіопристроїв
220	API для виконання фотографій за допомогою веб-камери

224	Занести до списку файли, що запускають разом з стартом системи
226	Занести до списку інформацію про доступні бездротові мережі (MAC-адреса, SSID, інтервал маяку)
228	Завантажити пакет Zlib

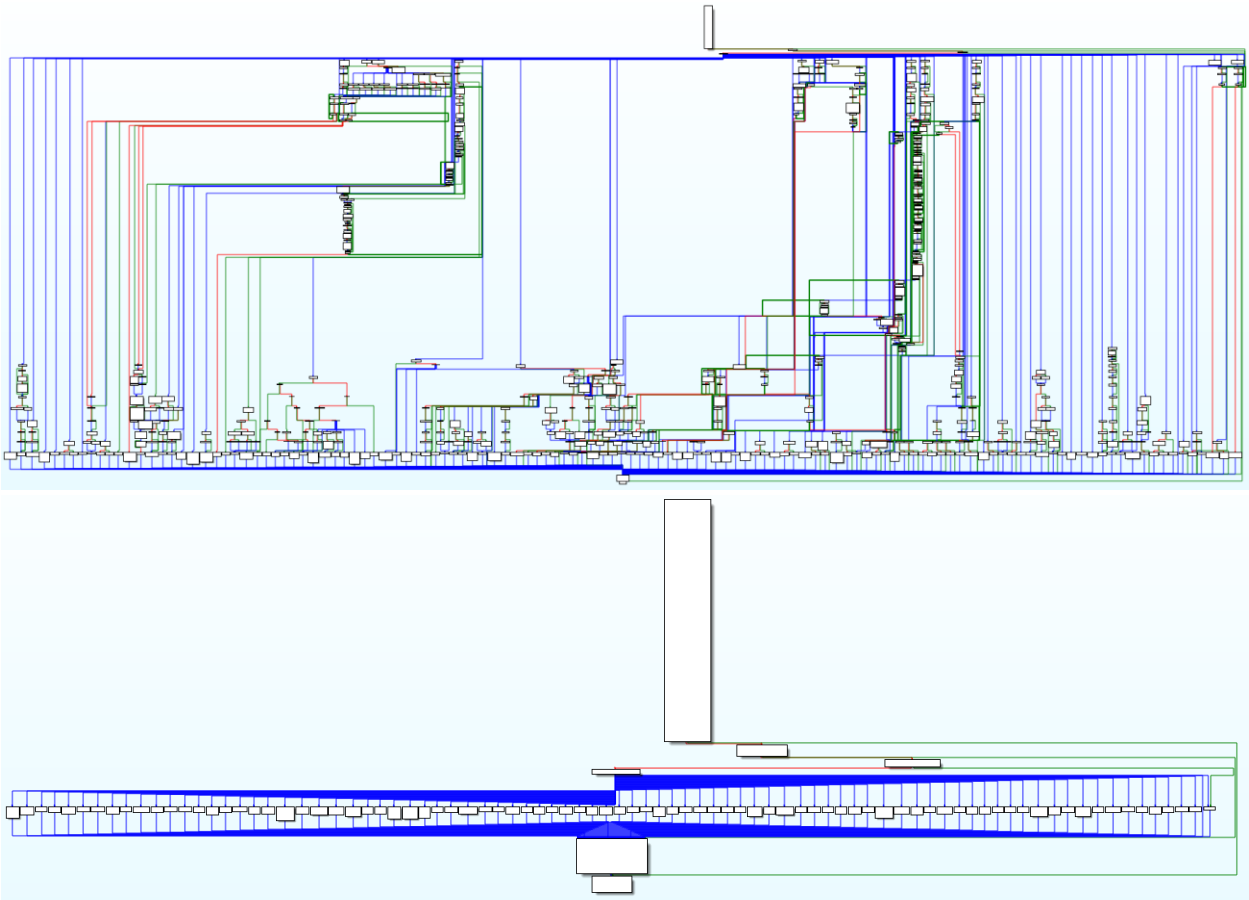


Рисунок 8 – Функції інтерпретатора бекдора (оригінал і після аналізу, змінені за допомогою Group Nodes функціоналу IDA Pro для більш зручного читання).

Висновок

InvisiMole – це добре оснащене шпигунське програмне забезпечення, можливості якого, безумовно, можуть конкурувати з іншими шпигунськими інструментами в реальному середовищі.

Можна тільки здогадуватися, чому автори вирішили використовувати два модулі з перекриваючими можливостями. Можна припустити, що менший модуль, `RC2FM`, використовується як початковий розвідувальний інструмент, тоді як більший модуль `RC2CL` працює тільки на цілях, які становлять інтерес. Однак це не так – обидва модулі запускаються одночасно. Ще одне пояснення полягає в тому, що модулі, можливо, були створені різними авторами, а потім об'єднані разом, щоб забезпечити більш складний функціонал.

Шкідлива програма використовує лише кілька методів для уникнення виявлення та аналізу, проте, завдяки розгортанню на дуже малу кількість високопрофільних цілей вона залишалася невиявленою щонайменше п'ять років.

Ідентифікатори інфікування (IoC)

Назви виявлень 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

SHA-1 хеші

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

Ім’я домену командних серверів (C&C)

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

IP-адреси командних серверів (C&C)

Active period	IP address
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

Ключі реєстру

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"
```

Файли та 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_%variable%.data
~lcf\tfl_%random%
```