Command & Control - level 3 ✍

Title: Memory analysis

Point: 30 Points

Level: Medium

Description: Berthier, the antivirus software didn't find anything. It's up to you now. Try to find the malware in the memory dump. The validation flag is the md5 checksum of the full path of the executable.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Solution:

Công cụ sử dụng: `Volatility`
Tiếp từ challenge **Command & Control - level 2**. Bây giờ nhiệm vụ của chúng ta là tìm malware trên bộ nhớ RAM

Sử dụng `Win7SP0x86` và liệt kê ra tất cả các tiến trình đang chạy. Sử dụng `pstree`:
`./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 pstree`
Output:

```
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x892ac2b8:wininit.exe                              456    396      3     77 2013-
01-12 16:38:14 UTC+0000
. 0x896294c0:services.exe                            560    456      6    205 2013-
01-12 16:38:16 UTC+0000
.. 0x89805420:svchost.exe                            832    560     19    435 2013-
01-12 16:38:23 UTC+0000
... 0x87c90d40:audiodg.exe                          1720    832      5    117 2013-
01-12 16:58:11 UTC+0000
.. 0x89852918:svchost.exe                            904    560     17    409 2013-
01-12 16:38:24 UTC+0000
... 0x87ad44d0:dwm.exe                              2496    904      5     77 2013-
01-12 16:40:25 UTC+0000
.. 0x898b2790:svchost.exe                           1172    560     15    475 2013-
01-12 16:38:27 UTC+0000
.. 0x89f3d2c0:svchost.exe                           3352    560      9    141 2013-
01-12 16:40:58 UTC+0000
.. 0x898fbb18:SearchIndexer.                        2900    560     13    636 2013-
01-12 16:40:38 UTC+0000
.. 0x8986b030:svchost.exe                            928    560     26    869 2013-
01-12 16:38:24 UTC+0000
```

```
.. 0x8a1d84e0:vmtoolsd.exe                1968    560      6    220 2013-
01-12 16:39:14 UTC+0000
.. 0x8962f030:svchost.exe                  692    560     10    353 2013-
01-12 16:38:21 UTC+0000
.. 0x898911a8:svchost.exe                 1084    560     10    257 2013-
01-12 16:38:26 UTC+0000
.. 0x898a7868:AvastSvc.exe                1220    560     66   1180 2013-
01-12 16:38:28 UTC+0000
.. 0x89f1d3e8:svchost.exe                 3624    560     14    348 2013-
01-12 16:41:22 UTC+0000
.. 0x9542a030:TPAutoConnSvc.              1612    560      9    135 2013-
01-12 16:39:23 UTC+0000
... 0x87ae2880:TPAutoConnect.             2568   1612      5    146 2013-
01-12 16:40:28 UTC+0000
.. 0x88cded40:sppsvc.exe                  1872    560      4    143 2013-
01-12 16:39:02 UTC+0000
.. 0x8a102748:svchost.exe                 1748    560     18    310 2013-
01-12 16:38:58 UTC+0000
.. 0x8a0f9c40:spoolsv.exe                 1712    560     14    338 2013-
01-12 16:38:58 UTC+0000
.. 0x9541c7e0:wlms.exe                     336    560      4     45 2013-
01-12 16:39:21 UTC+0000
.. 0x8a1f5030:VMUpgradeHelpe               448    560      4     89 2013-
01-12 16:39:21 UTC+0000
... 0x892ced40:winlogon.exe                500    448      3    111 2013-
01-12 16:38:14 UTC+0000
... 0x88d03a00:csrss.exe                   468    448     10    471 2013-
01-12 16:38:14 UTC+0000
.... 0x87c595b0:conhost.exe               3228    468      2     54 2013-
01-12 16:44:50 UTC+0000
.... 0x87a9c288:conhost.exe               2600    468      1     35 2013-
01-12 16:40:28 UTC+0000
.... 0x954826b0:conhost.exe               2168    468      2     49 2013-
01-12 16:55:50 UTC+0000
.. 0x87bd35b8:wmpnetwk.exe                3176    560      9    240 2013-
01-12 16:40:48 UTC+0000
.. 0x87ac0620:taskhost.exe                2352    560      8    149 2013-
01-12 16:40:24 UTC+0000
.. 0x897b5c20:svchost.exe                  764    560      7    263 2013-
01-12 16:38:23 UTC+0000
. 0x8962f7e8:lsm.exe                       584    456     10    142 2013-
01-12 16:38:16 UTC+0000
. 0x896427b8:lsass.exe                     576    456      6    566 2013-
01-12 16:38:16 UTC+0000
 0x8929fd40:csrss.exe                      404    396      9    469 2013-
01-12 16:38:14 UTC+0000
 0x87978b78:System                           4      0    103   3257 2013-
01-12 16:38:09 UTC+0000
. 0x88c3ed40:smss.exe                      308      4      2     29 2013-
01-12 16:38:09 UTC+0000
 0x87ac6030:explorer.exe                  2548   2484     24    766 2013-
01-12 16:40:27 UTC+0000
. 0x87b6b030:iexplore.exe                 2772   2548      2     74 2013-
01-12 16:40:34 UTC+0000
```

```
.. 0x89898030:cmd.exe                          1616   2772      2    101 2013-
01-12 16:55:49 UTC+0000
. 0x95495c18:taskmgr.exe                       1232   2548      6    116 2013-
01-12 16:42:29 UTC+0000
. 0x87bf7030:cmd.exe                           3152   2548      1     23 2013-
01-12 16:44:50 UTC+0000
.. 0x87cbfd40:winpmem-1.3.1.                   3144   3152      1     23 2013-
01-12 16:59:17 UTC+0000
. 0x898fe8c0:StikyNot.exe                      2744   2548      8    135 2013-
01-12 16:40:32 UTC+0000
. 0x87b784b0:AvastUI.exe                       2720   2548     14    220 2013-
01-12 16:40:31 UTC+0000
. 0x87b82438:VMwareTray.exe                    2660   2548      5     80 2013-
01-12 16:40:29 UTC+0000
. 0x87c6a2a0:swriter.exe                       3452   2548      1     19 2013-
01-12 16:41:01 UTC+0000
.. 0x87ba4030:soffice.exe                      3512   3452      1     28 2013-
01-12 16:41:03 UTC+0000
... 0x87b8ca58:soffice.bin                     3564   3512     12    400 2013-
01-12 16:41:05 UTC+0000
. 0x9549f678:iexplore.exe                      1136   2548     18    454 2013-
01-12 16:57:44 UTC+0000
.. 0x87d4d338:iexplore.exe                     3044   1136     37    937 2013-
01-12 16:57:46 UTC+0000
. 0x87aa9220:VMwareUser.exe                    2676   2548      8    190 2013-
01-12 16:40:30 UTC+0000
 0x95483d18:soffice.bin                        3556   3544      0 ------ 2013-
01-12 16:41:05 UTC+0000
```

Ở địa chỉ `0x87b6b030` có một tiến trình `iexplore.exe` nhưng mà nó lạ lắm,
tại `0x89898030`, `cmd.exe` đang được chạy như một process con của thằng kia, cái này làm mình nghi ngờ, đây là một dạng điển hình của backdoor luôn, chạy process rồi gắn cái shell vào để thực hiện mục đích gì đó theo ý hacker .
Xem thêm thông tin process với PID là `2772`. Sử dụng `cmdline`

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 cmdline -p 2772
```

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6
************************************************************************
iexplore.exe pid:   2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe
```

Vậy là rõ ràng rồi, process hệ thống nào mà lại chạy đường dẫn lạ đến “lộ thiên” vậy ??? Caught you, bitch !

Có thể check một tiến trình ứng dụng "Internet Explorer" bình thường được chạy bằng cách vào xem process có PID là `1136` (Đường dẫn mặc định là `C:\Program Files\Internet Explorer\iexplore.exe`):

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 cmdline -p 1136
```

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 cmdline -p 1136
Volatility Foundation Volatility Framework 2.6
************************************************************************
iexplore.exe pid:   1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
```

Bây giờ ta sẽ tính toán **md5 checksum** của đường dẫn để submit của `C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe`. Mình sử dụng [this site](#) để tính toán cho gọn

Hoặc sử dụng command này. `-n` để loại bỏ "ký tự xuống dòng" khi xuất ra và nhớ một trường hợp đặc biệt trên hệ thống **Unix **, `echo "\U"` sẽ không in ra gì cả (vì `\u` và `\U` là một dạng unicode specifier. Do đó, một mình `\U` sẽ bị xóa) sử dụng `echo -E "\\U"` để tiện sử dụng.

```
echo -n -E "C:\\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" | md5sum
```

FLag: **4997914963263943239 7b3a1df8cb43d**