実習資料1

仙台 CTF セキュリティ技術勉強会 実習

「Volatility Framework」による メモリフォレンジック

平成29年11月12日

仙台 CTF 実行委員会

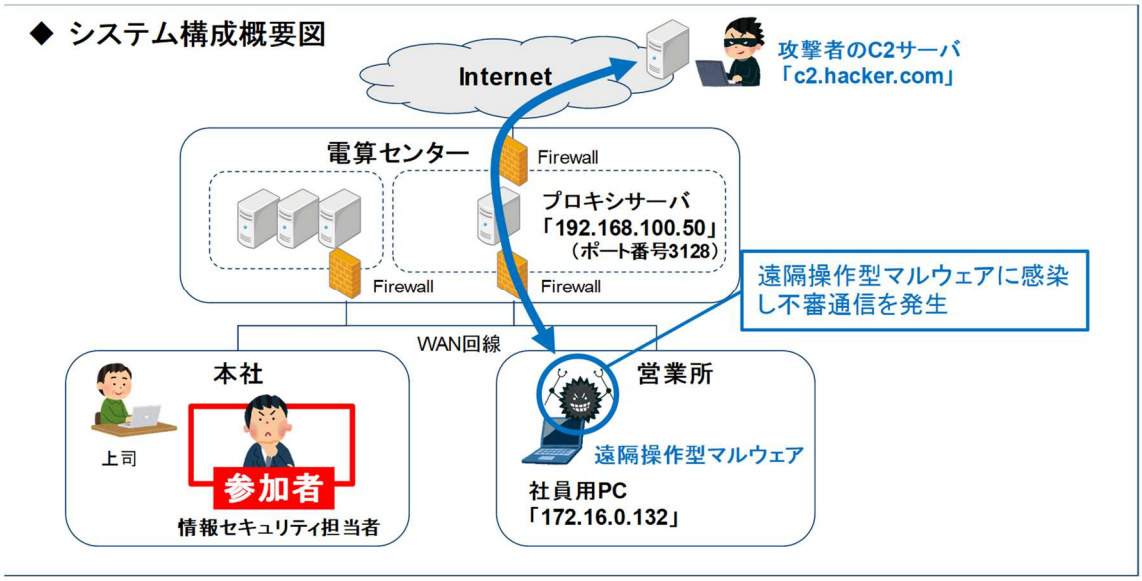
目次

本実習の概要

あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。

営業所の社員用 PC（以下、感染 PC）が遠隔操作型マルウェアに感染し、攻撃者の C2 サーバ※1「c2.hacker.com」と通信をしていることが判明しました。

感染 PC のメモリイメージを解析し、感染の原因となったプロセスの調査を実施してください。



［補足情報］

- インシデントを検知した日時は、2017 年 10 月 7 日（土）です。
- メモリイメージは、インシデント検知後、感染 PC の LAN ケーブルを抜線したうえで、調査用ツール「FTK Imager Lite」を起動し取得しました。
- 感染 PC の OS は、Windows7 SP0 32bit 版です。
- 社員用 PC とインターネットとの通信は、必ずプロキシサーバを経由するネットワーク構成となっています。

※1 C2 サーバ（Command & Control サーバ）：遠隔操作型マルウェアに指令を出すサーバ。

実習１　ネットワーク接続状況の確認

状 況 説 明

株式会社仙台シーテーエフでは、社員用 PC とインターネットとの通信は、必ずプロキシサーバを経由するネットワーク構成となっており、感染 PC のマルウェアは、インターネット上の C2 サーバと通信するために、プロキシサーバに接続しているはずです。

あなたは、感染 PC のメモリイメージを解析し、プロキシサーバと通信しているプロセスを確認することとしました

実 習 内 容

感染 PC のメモリイメージファイル「memdump.mem」を、Volatility Framework の「netscan」プラグインで解析し、プロキシサーバと通信している「Pid」（プロセス ID）を全て列挙してください。

［補足情報］

・感染 PC の OS は、「Windows7 SP0 32bit 版」です。

・プロキシサーバの IP アドレスは、「192.168.100.50」、ポート番号「3128」で稼働しています。

［実習用データ］

フォルダ： ¥Seminar¥Lab01¥

ファイル： memdump.mem

回答記入欄

プロキシサーバと通信しているプロセスの「Pid」

解説

Volatility Framework（以下、Volatility）の「netscan」プラグインを利用して、メモリイメージを解析します。

（補足）
- 解説では、Windows 版「Volatility 2.6 Windows Standalone Executable (x64)」を「C:¥work¥」にインストールしています。また、インストールしたファイル「volatiliey_2.6_win64_standalone.exe」の名前は「volat.exe」に変更しています。
  各自の環境に合わせて、コマンド名やフォルダ名を適宜読み替えてください。
- 解説におけるコマンド入力例では、参加者が入力する文字を「緑色」で記載してあります。

1. 実習用データ「memdump.exe」を、Volatility をインストールしたフォルダ（C:¥work）にコピーします。

2. コマンドプロンプトを起動し、Volatility をインストールしたフォルダに移動します。

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥Users¥ctf>cd ¥work

C:¥work>
```

3. Volatility での解析にあたり、「OS プロファイル名」を指定する必要があるため、Volatility の「--info」オプションを実行し、Volatility が対応している OS プロファイル名を確認します。
   コマンド実行の結果、問題データである Windows7 SP0 32bit 版の OS プロファイル名は、「WinSP0x86」であることが分かります。

```
C:¥work>volat --info
Volatility Foundation Volatility Framework 2.6

Profiles
--------
VistaSP0x64             - A Profile for Windows Vista SP0 x64
VistaSP0x86             - A Profile for Windows Vista SP0 x86
（中略）
Win7SP0x86              - A Profile for Windows 7 SP0 x86
（以下略）
```

4. Volatility の「netscan」プラグインを実行し、ネットワーク接続状況を解析します。
コマンド実行の結果、Pid 3012（Thunderbird）、Pid 2184（svchost.exe）、Pid 1124（svchost.exe）が、プロキシサーバ（192.168.100.50:3128）に接続していることが分かります。

```
C:¥work>volat --tz=Japan --profile=Win7SP0x86 -f memdump.mem netscan

Volatility Foundation Volatility Framework 2.6
Offset(P)   Proto  Local Address       Foreign Address      State        Pid   Owner          Crea
ted
0x23c90b70  TCPv4  0.0.0.0:49154       0.0.0.0:0            LISTENING    936   svchost.exe
（中略）

0x3e162b48  TCPv4  172.16.0.132:49839  192.168.100.50:3128  CLOSED       3012  thunderbird.ex

0x3eaebbb8  TCPv4  0.0.0.0:49154       0.0.0.0:0            LISTENING    936   svchost.exe
0x3eaebbb8  TCPv6  :::49154            :::0                 LISTENING    936   svchost.exe
0x3ea2c008  TCPv4  127.0.0.1:49836     127.0.0.1:49835      ESTABLISHED  3012  thunderbird.ex
0x3f7f9d60  UDPv4  127.0.0.1:57064     *:*                               4044  iexplore.exe    201
7-10-07 11:37:29 JST+0900

0x3fa3fdf8  TCPv4  172.16.0.132:49851  192.168.100.50:3128  CLOSED       3012  thunderbird.ex
0x3fa8f568  TCPv4  172.16.0.132:49850  192.168.100.50:3128  ESTABLISHED  2184  svchost.exe

0x3fc513e0  UDPv4  127.0.0.1:1900      *:*                               1772  svchost.exe     201
7-10-07 11:58:08 JST+0900
0x3fc98330  UDPv4  127.0.0.1:57063     *:*                               3968  iexplore.exe    201
7-10-07 11:37:23 JST+0900

0x3fd53df8  TCPv4  172.16.0.132:49858  192.168.100.50:3128  ESTABLISHED  1124  svchost.exe
0x3fd95df8  TCPv4  172.16.0.132:49840  192.168.100.50:3128  CLOSED       3012  thunderbird.ex

0x3fd989f8  TCPv4  127.0.0.1:49835     127.0.0.1:49836      ESTABLISHED  3012  thunderbird.ex
```

回答例

プロキシサーバと通信しているプロセスの「Pid」 3012、 2184、 1124

実習2　不審プロセスの確認

状 況 説 明

3つのプロセスがインターネットと通信していることが分かりました。

あなたは、どれがマルウェアのプロセスなのか特定するため、次の視点で各プロセスを調査することとしました。

① 親子関係が不自然なプロセスはないか。

② C2 サーバのホスト名である「c2.hacker.com」の文字列を含むプロセスはないか。

③ イメージパス（実行ファイルのフルパス名）が不自然なプロセスはないか。

実 習 内 容

感染 PC のメモリイメージファイル「memdump.mem」を、Volatility Framework の「pstree」プラグイン、「yarascan」プラグイン、および「dlllist」プラグインで解析し、マルウェアの可能性が高い「プロセス名」、「Pid」、および「イメージパス」を特定してください。

［実習用データ］

実習1と同じデータを利用します。

回答記入蘭

プロセス名：

Pid：

イメージパス：

解説

Volatility Framework（以下、Volatility）の「pstree」プラグイン、「yarascan」プラグイン、「dlllist」プラグインを利用して、メモリイメージを解析します。

1. コマンドプロンプトを起動し、Volatility をインストールしたフォルダに移動します。
   なお、同フォルダには、問題データ「memdump.mem」がコピーされているものとします。

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥Users¥ctf>cd ¥work

C:¥work>
```

2. Volatility の「pstree」プラグインを実行し、プロセスの親子関係を確認します。
   一般的な「svchost.exe」は、「services.exe」から起動されますが、Pid 2184（svchost.exe）は直接起動されています。Pid 2184 は、プロキシサーバと通信しているプロセスであることから、マルウェアの可能性が疑われます。

```
C:¥WORK>volat.exe --tz=Japan --profile=Win7SP0x86 -f memdump.mem pstree
Volatility Foundation Volatility Framework 2.6
Name                          Pid   PPid   Thds   Hnds Time
----------------------------- ------ ------ ------ ------ ----
 0x871b3c88:wininit.exe         400    332      3     76 2017-10-07 11:30:45 JST+0900
. 0x87315908:lsm.exe            516    400      9    143 2017-10-07 11:30:45 JST+0900
. 0x878076b8:services.exe       500    400      8    206 2017-10-07 11:30:45 JST+0900
.. 0x87567760:svchost.exe      1048    500     12    538 2017-10-07 11:30:46 JST+0900
.. 0x874c93b8:svchost.exe       772    500     15    407 2017-10-07 11:30:45 JST+0900
（中略）
.. 0x87577bb8:svchost.exe      1124    500     19    490 2017-10-07 11:30:46 JST+0900
（中略）
 0x86032030:explorer.exe       3376   3340     30    899 2017-10-07 11:36:29 JST+0900
. 0x87658030:iexplore.exe      3968   3376     15    621 2017-10-07 11:37:22 JST+0900
.. 0x8586c5b0:iexplore.exe     4044   3968     22    653 2017-10-07 11:37:23 JST+0900
. 0x87817418:FTK Imager.exe    3632   3376     17    376 2017-10-07 11:58:45 JST+0900
. 0x85873310:vmtoolsd.exe      3480   3376      7    186 2017-10-07 11:36:30 JST+0900
. 0x859e1280:thunderbird.ex    3012   3376     42    657 2017-10-07 11:50:26 JST+0900
（中略）
0x85a4fc78 svchost.exe         2184   1140      5    307 2017-10-07 11:51:23 JST+0900
 0x86ad9d40:csrss.exe           408    392     10    284 2017-10-07 11:30:45 JST+0900
 0x87255b10:winlogon.exe        456    392      5    120 2017-10-07 11:30:45 JST+0900
```

3. Volatility の「yarascan」プラグインを実行し、C2 サーバのホスト名である文字列「c2.hacker.com」を含むプロセスを検索します。
コマンド実行の結果、Pid 2184 のなかでのみ、C2 サーバのホスト名が発見されたため、Pid 2184 がマルウェアである疑いがますます深まります。

```
C:¥WORK>volat.exe --profile=Win7SP0x86 -f memdump.mem yarascan --yara-rules="c2.hacker.com"

Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process svchost.exe Pid 2184
0x0040169f  63 32 2e 68 61 63 6b 65 72 2e 63 6f 6d 00 bb 01   c2.hacker.com...
0x004016af  8c 01 04 00 00 00 00 00 c1 02 04 00 ff ff ff ff   ................
（中略）
0x0040178f  0c c6 00 00 52 ff 75 0c ff 97 a9 00 00 00 59 58   ....R.u.......YX
Rule: r1
Owner: Process svchost.exe Pid 2184
0x001d9060  63 32 2e 68 61 63 6b 65 72 2e 63 6f 6d 00 00 00   c2.hacker.com...
0x001d9070  c8 9d 30 5d 00 00 00 80 e2 00 82 76 99 ad de 99   ..0].......v....
（後略）
```

4. Volatility の「dlllist」プラグインを実行し、Pid 2184 のイメージパスを確認します。
コマンド実行の結果、Pid 2184（svchost.exe）は、デスクトップから起動されていることが分かります。
正常な「svchost.exe」のパスは、「C:¥Windows¥System32」であるため、デスクトップに保管されている「svchost.exe」は、マルウェアの可能性が高いと判断できます。

```
C:¥WORK>volat --tz=Japan --profile=Win7SP0x86 -f memdump.mem dlllist -p 2184
Volatility Foundation Volatility Framework 2.6
************************************************************************
svchost.exe pid:   2184
Command line : svchost.exe

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000     0x1800     0xffff C:¥Users¥user01¥Desktop¥　　請求書¥svchost.exe
（以下略）
```

回答例

プロセス名： svchost.exe、 Pid: 2184
イメージパス：C:¥Users¥user01¥Desktop¥　　請求書¥svchost.exe