実習資料2

仙台 CTF セキュリティ技術勉強会 実習

「plaso/log2timeline」による タイムライン解析

平成29年11月12日

仙台 CTF 実行委員会

目次

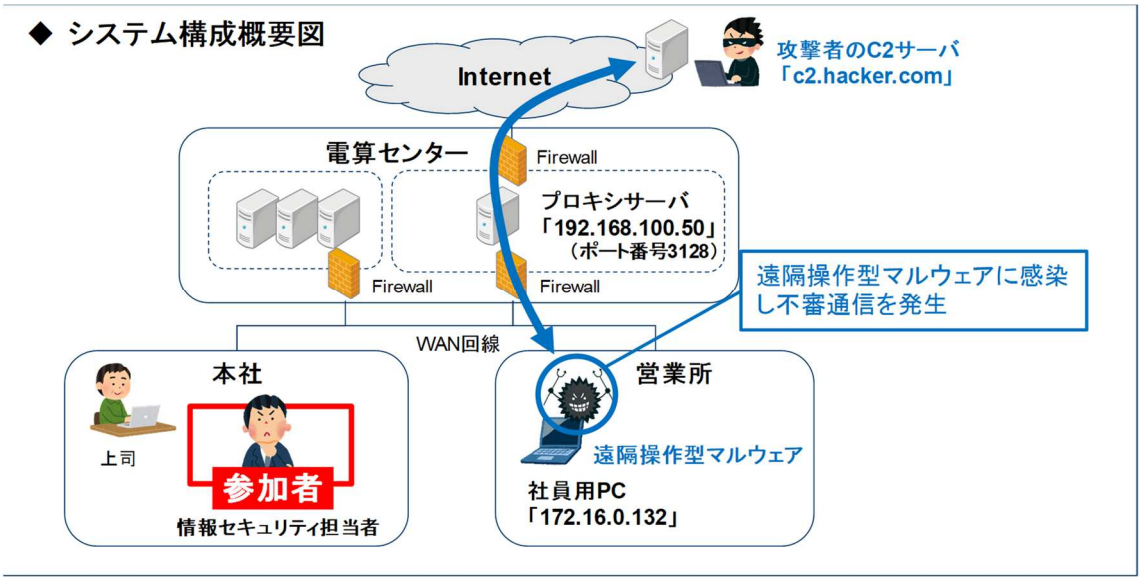
本実習の概要

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たところ、2017 年 10 月 7 日（土）11:51:23 に、不審ファイル「C:¥Users¥user01¥Desktop¥　　請求書¥svchost.exe」が起動し、C2 サーバと通信していたことが判明しました。

感染 PC のディスクイメージをタイムライン解析し、感染原因を特定してください。



［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。
- ディスクイメージは、インシデント検知後、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。
- 感染 PC は、メーラーソフトとして「Thunderbird」を利用しています。また、圧縮・解凍ソフトとして「Lhaplus」が標準設定でインストールされています。
- なお、実習用データは、ディスクイメージから実習に必要なデータのみ抽出した「模擬ディスクイメージ」です。ファイルシステムレベルで確認すると、一部、実習のシナリオと整合がとれない部分がありますので、ご了承ください。

※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　タイムライン解析

状況説明

感染 PC では、2017 年 10 月 7 日（土）11:51:23 に、不審ファイル「C:¥Users¥user01¥Desktop¥　　請求書¥svchost.exe」が起動しており、この時刻付近で、感染原因となった何かが起きた可能性があります。

あなたは、感染 PC のディスクイメージからタイムラインを作成し、次の視点で不審ファイルが起動した時刻付近の状況を調査することとしました。

① プロセス起動の痕跡や、プロセスが作成する一時ファイルなど、感染 PC の操作内容を推測できる手掛かりはないか。

② 「svchost.exe」のほかに、不審なファイルはないか。

実習内容

感染 PC のディスクイメージファイル「diskimage.dd」を、log2timeline の「filestat」パーサーで解析し、インシデントが発生した当日である「2017 年 10 月 7 日（土）0:00～24:00」のタイムラインを作成してください。

次に、作成したタイムラインから、不審ファイル「C:¥Users¥user01¥Desktop¥　　請求書¥svchost.exe」が起動した時刻である「2017 年 10 月 7 日（土）11:51:23」の直前 1 分間に注目し、次の2点を確認してください。

① 「svchost.exe」以外の不審なプログラム（.exe）のファイル名

② 利用者が操作していた可能性があるプログラム名

また、上記の確認結果を踏まえ、感染原因を推測してください。

［実習用データ］

フォルダ：　¥Seminar¥Lab02¥

ファイル：　diskimage.dd

回答記入欄

① 不審なプログラムのファイル名（svchost.exe 以外のもの）

② 利用者が操作していた可能性があるプログラム名

［感染原因の推測］

実習1の解説

plaso(log2timeline)の「filestat」パーサーを利用して、ディスクイメージを解析します。

（補足）
- 解説では、Windows 版「plaso ver.1.5.1」を「C:¥work¥」にインストールしています。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「diskimage.dd」を、plaso 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、plaso 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. log2timeline の「filestat」パーサーを実行し、plaso storage（解析のための中間ファイル。実行例では、「db.plaso」というファイル名）を作成します。
   コマンド実行により、中間ファイル「db.plaso」が作成されます。

```
C:¥work>log2timeline --parsers filestat  db.plaso  diskimage.dd
Checking availability and versions of dependencies.
[OK]


Source path     : C:¥work¥diskimage.dd
Source type     : storage media image

Processing started.
2017-10-15 21:11:17,216 [INFO] (MainProcess) PID:6704 <engine> Preprocessing detecte
d platform: Unknown
2017-10-15 21:11:17,216 [INFO] (MainProcess) PID:6704 <extraction_frontend> Setting
timezone to: UTC
Worker_00 (PID: 8528) - events produced: 204 - file: TSK:/Users/user01/AppData/Local
/VirtualStore - running: True
（以下略）
```

4. psort コマンドにより、中間ファイル「db.plaso」からタイムライン（実行例では、timeline.txt）を作成します。

期間を指定せずにタイムラインを作成すると、出力が膨大な量になるため、インシデントが発生した「2017 年 10 月 7 日 0:00～24:00」の期間のタイムラインのみ抽出します。

なお、期間の指定は、UTC（協定世界時）で指定する必要があります。UTC は、「日本時間 － 9 時間」で計算します。

```
C:¥work>psort -z Japan  -o tln  -w timeline.txt  db.plaso  "date < '2017-10
-07 15:00:00' and date > '2017-10-06 15:00:00'"

Processing completed.

********************************** Counter **********************************
 Events filtered : 3450
Events processed : 2646
-----------------------------------------------------------------------------

C:¥work>
```

5. 作成されたタイムライン「timeline.txt」をテキストエディタなどで検索し、「svchost.exe」のほかに、拡張子が「.exe」のファイルがあるか確認します。

確認の結果、11:51:18 に「/Users/user01/Desktop/　　請求書/請求書.exe」という不審なプログラムが作成されていることが分かります。

「timeline.txt」の抜粋（見やすくするために一部加工してあります）

```
11:51:18; atime;   TSK:/Users/user01/Desktop  Type: directory
11:51:18; crtime;  TSK:/Users/user01/Desktop/      請求書  Type: directory
11:51:18; ctime;   TSK:/Users/user01/Desktop  Type: directory
11:51:18; mtime;   TSK:/Users/user01/Desktop  Type: directory
11:51:18; atime;   TSK:/Users/user01/Desktop/      請求書/請求書.exe  Type: file
11:51:18; crtime;  TSK:/Users/user01/Desktop/      請求書/請求書.exe  Type: file
11:51:19; atime;   TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json  Type: file
11:51:19; crtime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json  Type: file
11:51:19; ctime;   TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json  Type: file
11:51:19; mtime;   TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json  Type: file
11:51:21; ctime;   TSK:/Windows/Prefetch/LHAPLUS.EXE-537CE22B.pf  Type: file
11:51:21; mtime;   TSK:/Windows/Prefetch/LHAPLUS.EXE-537CE22B.pf  Type: file
11:51:23; atime;   TSK:/Users/user01/Desktop/      請求書  Type: directory
11:51:23; atime;   TSK:/Users/user01/Desktop/      請求書/svchost.exe  Type: file
11:51:23; crtime;  TSK:/Users/user01/Desktop/      請求書/svchost.exe  Type: file
11:51:23; ctime;   TSK:/Users/user01/Desktop/      請求書  Type: directory
11:51:23; ctime;   TSK:/Users/user01/Desktop/      請求書/svchost.exe  Type: file
11:51:23; mtime;   TSK:/Users/user01/Desktop/      請求書  Type: directory
11:51:23; mtime;   TSK:/Users/user01/Desktop/      請求書/svchost.exe  Type: file
```

6. 引き続き、タイムライン「timeline.txt」をテキストエディタなどで確認します。
拡張子「.pf」のファイルは Prefetch ファイルと呼ばれるもので、プログラム起動のおよそ 10 秒後に自動的に作成されるものです。
確認の結果、メールソフト「Thunderbird.exe」、および圧縮・解凍用ソフト「Lhaplus.exe」の Prefetch ファイルが更新されており、起動したことが分かります。また、「Thunderbird」の一時ファイルと思われるファイルも複数作成されていることが分かります。
このことから、インシデント発生の直前、利用者は、メールソフトを利用し、その後に圧縮・解凍ソフトを利用した可能性があると推測できます。

「timeline.txt」の抜粋（見やすくするために一部加工してあります）

```
11:50:36; ctime;  TSK:/Windows/Prefetch/THUNDERBIRD.EXE-EDED9AF7.pf Type: file
11:50:36; mtime;  TSK:/Windows/Prefetch/THUNDERBIRD.EXE-EDED9AF7.pf Type: file
11:51:02; atime;  TSK:/Users/user01/AppData/Local/Thunderbird/Profiles/omwzc6fd.default/cache2/entries/8E387515A7A123BA8B378492B5B
                  678044C774031 Type: file
11:51:02; crtime; TSK:/Users/user01/AppData/Local/Thunderbird/Profiles/omwzc6fd.default/cache2/entries/8E387515A7A123BA8B378492B5B
                  678044C774031 Type: file
11:51:05; ctime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/Mail/mail.localdomain.invalid/Inbox Type: file
11:51:05; mtime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/Mail/mail.localdomain.invalid/Inbox Type: file
11:51:10; ctime;  TSK:/Users/user01/AppData/Local/Thunderbird/Profiles/omwzc6fd.default/cache2/entries/8E387515A7A123BA8B378492B5B
                  678044C774031 Type: file
11:51:10; mtime;  TSK:/Users/user01/AppData/Local/Thunderbird/Profiles/omwzc6fd.default/cache2/entries/8E387515A7A123BA8B378492B5B
                  678044C774031 Type: file
11:51:10; atime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/addons.json Type: file
11:51:10; crtime; TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/addons.json Type: file
11:51:10; ctime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/addons.json Type: file
11:51:10; mtime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/addons.json Type: file
11:51:18; atime;  TSK:/Users/user01/Desktop Type: directory
11:51:18; crtime; TSK:/Users/user01/Desktop/        請求書 Type: directory
11:51:18; ctime;  TSK:/Users/user01/Desktop Type: directory
11:51:18; mtime;  TSK:/Users/user01/Desktop Type: directory
11:51:18; atime;  TSK:/Users/user01/Desktop/        請求書/請求書.exe Type: file
11:51:18; crtime; TSK:/Users/user01/Desktop/        請求書/請求書.exe Type: file
11:51:19; atime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json Type: file
11:51:19; crtime; TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json Type: file
11:51:19; ctime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json Type: file
11:51:19; mtime;  TSK:/Users/user01/AppData/Roaming/Thunderbird/Profiles/omwzc6fd.default/downloads.json Type: file
11:51:21; ctime;  TSK:/Windows/Prefetch/LHAPLUS.EXE-537CE22B.pf Type: file
11:51:21; mtime;  TSK:/Windows/Prefetch/LHAPLUS.EXE-537CE22B.pf Type: file
11:51:23; atime;  TSK:/Users/user01/Desktop/        請求書 Type: directory
11:51:23; atime;  TSK:/Users/user01/Desktop/        請求書/svchost.exe Type: file
11:51:23; crtime; TSK:/Users/user01/Desktop/        請求書/svchost.exe Type: file
11:51:23; ctime;  TSK:/Users/user01/Desktop/        請求書 Type: directory
11:51:23; ctime;  TSK:/Users/user01/Desktop/        請求書/svchost.exe Type: file
11:51:23; mtime;  TSK:/Users/user01/Desktop/        請求書 Type: directory
11:51:23; mtime;  TSK:/Users/user01/Desktop/        請求書/svchost.exe Type: file
```

7. 引き続き、タイムライン「timeline.txt」をテキストエディタなどで確認します。
確認の結果、11:51:33 に、「請求書.exe」の Prefetch ファイルが作成されていることから、「請求書.exe」、「svchost.exe」は、ファイル作成日時の 10 秒前である 11:51:23 に実行されたと考えられます。

「timeline.txt」の抜粋 （見やすくするために一部加工してあります）

```
11:51:28; ctime;   TSK:/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf Type: file
11:51:28; mtime;   TSK:/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf Type: file
11:51:28; ctime;   TSK:/Windows/Prefetch/SEARCHFILTERHOST.EXE-AA7A1FDD.pf Type: file
11:51:28; mtime;   TSK:/Windows/Prefetch/SEARCHFILTERHOST.EXE-AA7A1FDD.pf Type: file
11:51:28; ctime;   TSK:/Windows/Prefetch/EXPLORER.EXE-7A3328DA.pf Type: file
11:51:28; mtime;   TSK:/Windows/Prefetch/EXPLORER.EXE-7A3328DA.pf Type: file
11:51:33; atime;   TSK:/Windows/Prefetch/請求書.EXE-B5754C28.pf Type: file
11:51:33; crtime;  TSK:/Windows/Prefetch/請求書.EXE-B5754C28.pf Type: file
11:51:33; ctime;   TSK:/Windows/Prefetch/請求書.EXE-B5754C28.pf Type: file
11:51:33; mtime;   TSK:/Windows/Prefetch/請求書.EXE-B5754C28.pf Type: file

11:51:33; atime;   TSK:/Windows/Prefetch/SVCHOST.EXE-BA96A7BE.pf Type: file
11:51:33; crtime;  TSK:/Windows/Prefetch/SVCHOST.EXE-BA96A7BE.pf Type: file
11:51:33; ctime;   TSK:/Windows/Prefetch/SVCHOST.EXE-BA96A7BE.pf Type: file
11:51:33; mtime;   TSK:/Windows/Prefetch/SVCHOST.EXE-BA96A7BE.pf Type: file
```

8. ここまでの調査結果を時系列に整理してみます。

日時	発生した事象
2017 年 10 月 7 日 11:50:26	メールソフト「Thunderbird.exe」が起動した。 ［根拠］ Prefetch ファイルは、プログラム起動のおよそ 10 秒後に作成・更新されることから、「/Windows/Prefetch/THUNDERBIRD.EXE-EDED9AF7.pf」の作成日時である「2017 年 10 月 7 日 11:50:36」の 10 秒前にプログラムが起動したものと考えられる。
11:51:02	メールソフト「Thunderbird」を利用していた。 ［根拠］ 「Thunderbird」のキャッシュファイルなどが格納されているフォルダ「/Users/user01/AppData/Roaming/Thunderbird/」内のファイルが作成・更新されていることから、「Thunderbird」を利用していたものと考えられる。
11:51:11	圧縮・解凍ソフト「Lhaplus」が起動した。 ［根拠］ Prefetch ファイル「/Windows/Prefetch/LHAPLUS.EXE-537CE22B.pf」の作成日時である「2017 年 10 月 7 日 11:51:21」の 10 秒前にプログラムが起動したものと考えられる。

11:51:18	Lhaplus により圧縮ファイルが解凍され、「/Users/user01/Desktop/　　請求書/請求書.exe」が作成された。 ［根拠］ Lhaplus は、ZIP などの圧縮ファイルを開くと、デスクトップに圧縮ファイルと同名のフォルダを作成し、展開する。 タイムラインでは、Lhaplus の起動直後に、デスクトップにフォルダとファイルが作成されていることから、圧縮ファイルが展開されたものと考えられる。
11:51:23	不審ファイル「請求書.exe」が実行され、その直後に C2 サーバと通信していた「svchost.exe」が実行されている。 このことから、「請求書.exe」はダウンローダーなどであり、「svchost.exe」を作成・実行した可能性があると考えられる。

9. タイムライン解析の結果を踏まえ、感染原因として、次の可能性を考えることができます。
   - 利用者が、不審メールに添付ファイルされていた圧縮ファイルを開封したことで、Lhaplus がデスクトップにフォルダ「請求書」を作成し、圧縮ファイルを解凍した。
   - 利用者が「請求書」に格納されていた「請求書.exe」を実行した。
   - 「請求書.exe」は、ダウンロードなどであり、同フォルダに遠隔操作型マルウェア「svchost.exe」を作成・実行した。

   なお、タイムラインからは、本当に「不審メール」を受信していたのかは断定できません。今後、感染 PC のメールファイルやメールサーバのログの確認、利用者への聞き取り調査などを行う必要があります。

回答例

① 不審なプログラムのファイル名（svchost.exe 以外のもの）

/Users/user01/Desktop/　　請求書/請求書.exe

② 利用者が操作していた可能性があるプログラム名

Thunderbird.exe、 Lhaplus.exe

［感染原因の推測］

利用者が不審メールの添付ファイル「請求書.exe」を開封したことにより感染した。