別紙１

仙台 CTF 2018 セキュリティ技術勉強会 実習

タイムライン解析による
マルウェア感染原因の特定

2018年9月8日

仙台 CTF 推進プロジェクト

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。

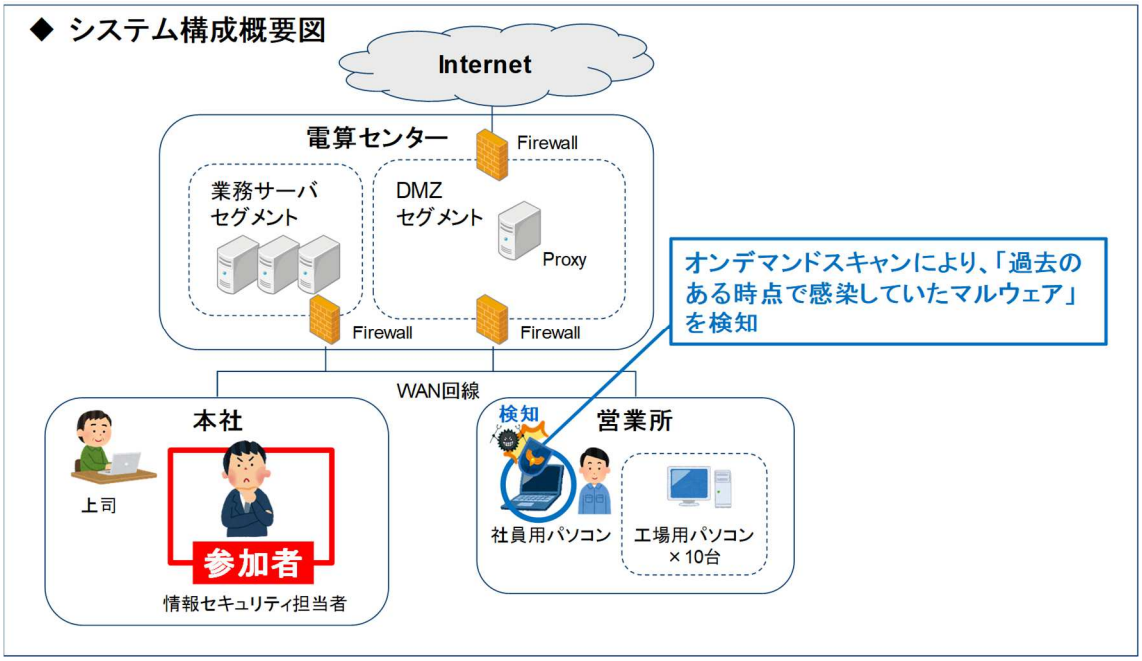
ある日、営業所の社員用パソコンのウイルス対策ソフトから、ウイルス検知アラートが通知されました。社員に電話連絡し状況を確認したところ、８月末から利用していなかった社員用パソコンを久しぶりに起動し、最新パターンファイルに更新のうえ手動でオンデマンドスキャンを実行したところ、「過去のある時点で感染していたマルウェア」を検知したようです。

感染パソコンから証拠保全したエビデンスを解析し、感染原因を特定してください。

◆ウイルス検知アラートの内容

検知日時	2018 年 9 月 8 日（土） 15:00
脅威名	BKDR_POISON.DS
検出ファイル名	C:¥Users¥user01¥Desktop¥rund11.exe
検査の種類	オンデマンドスキャン
処理結果	無視

◆ システム構成概要図



［補足情報］

・ 実習データの都合上、実際には社員パソコンは、8 月 25 日（土）以降は起動していません。また、ウイルス対策ソフトも未導入です。

・ 社員パソコンの OS は、Windows7 Enterprise 32bit 版です。

実習1　タイムライン解析

実習内容

感染パソコンから証拠保全したエビデンスをタイムライン解析し、次の点を確認してください。

① 不審なプログラム「rund11.exe」が作成および起動された日時
（年月日　時分まで特定）

② 「rundll11.exe」の起動直前の社員が操作していた内容の推測
（USB メモリへのファイルコピー、ウェブサイト閲覧、メール閲覧のいずれかを選択）

③ 感染に利用された脆弱性攻撃コードのファイル名
（タイムラインで怪しいと思ったファイルの内容を、テキストエディタ等で確認）

④ 上記③で特定した脆弱性攻撃コードのダウンロード元 URL

［実習用データ］

実習用仮想マシンに格納してあります。

フォルダ　：　/var/samba/public/lab/

（補足）危険なファイルは無害化したうえで格納してありますが、一部のファイルはウイルス対策ソフトで検知される可能性があります。

回答記入欄

① 不審なプログラム「rund11.exe」が作成および起動された日時
（年月日　時分まで特定）

② 「rundll11.exe」の起動直前の社員が操作していた内容の推測
（USB メモリへのファイルコピー、ウェブサイト閲覧、メール閲覧のいずれかを選択）

③ 感染に利用された脆弱性攻撃コードのファイル名
（タイムラインで怪しいと思ったファイルの内容を、テキストエディタ等で確認）

④ 上記③で特定した脆弱性攻撃コードのダウンロード元 URL

実習1の解説

最初に、NTFS の「MFT」からファイルシステムのタイムラインを作成します。

1. 実習用仮想マシンを起動します。
2. コマンドプロンプト（MATE 端末）を起動し、実習用データが格納されているフォルダに移動します。

```
caine@caine:~$ cd /var/samba/public/lab/
caine@caine:/var/samba/public/lab$
```

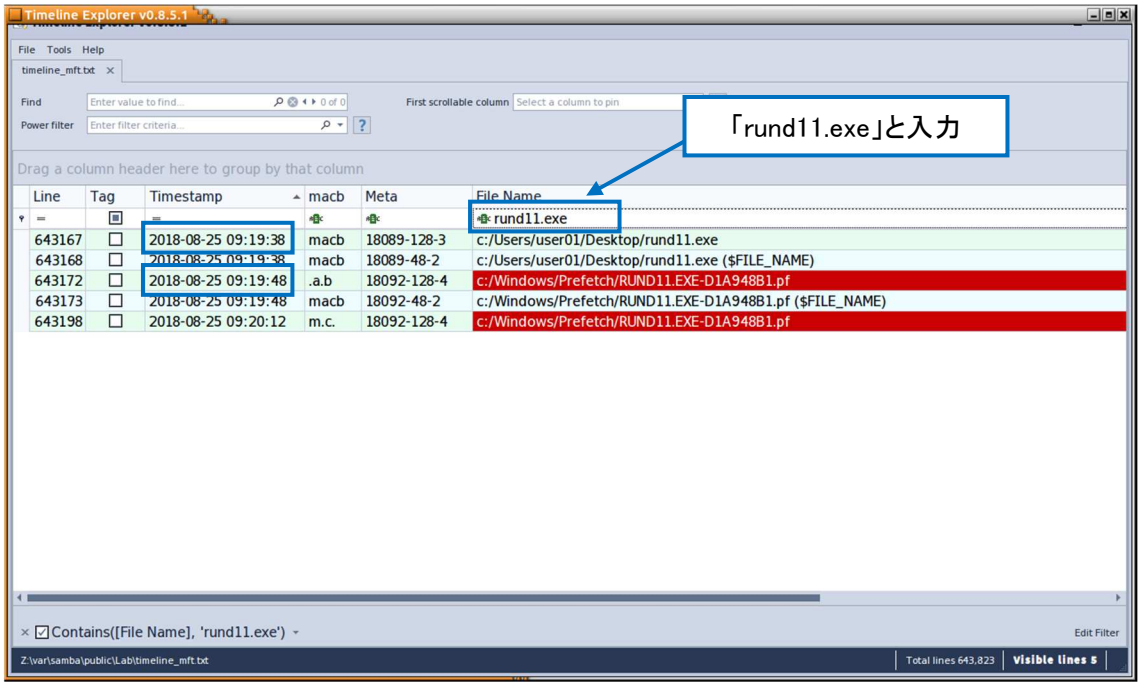
3. mftecmd コマンドを実行し、「MFT」から body 形式の中間ファイルを作成します。
   なお、作成されるファイ名は「YYYYMMDDhhmmss_MFTECmd_Output.body」という名前となります。（YYYYMMDDhhmmss は、コマンドを実行した時刻となります。）

```
caine@caine:/var/samba/public/lab$ mftecmd -f MFT --body . --bdl C
0014:err:xrandr:xrandr12_get_current_mode Unknown mode, returning default.
MFTECmd version 0.2.9.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f MFT --body . --bdl C

0038:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733
0038:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733

Processed 'MFT' in 8.6680 seconds

Bodyfile output will be saved to '.¥20180826050356_MFTECmd_Output.body'
（以下略）
caine@caine:/var/samba/public/lab$
```

4. mactime コマンドにより、中間ファイル「（時刻）_MFTECmd_Output.body」からタイムラインを作成します。（以下の実行例の body ファイル名は、適宜読み替えてください。）

```
caine@caine:/var/samba/public/lab$ mactime -b 20180826050356_MFTECmd_Output.body -z Japan -m -d > timeline_mft.txt
caine@caine:/var/samba/public/lab$
```

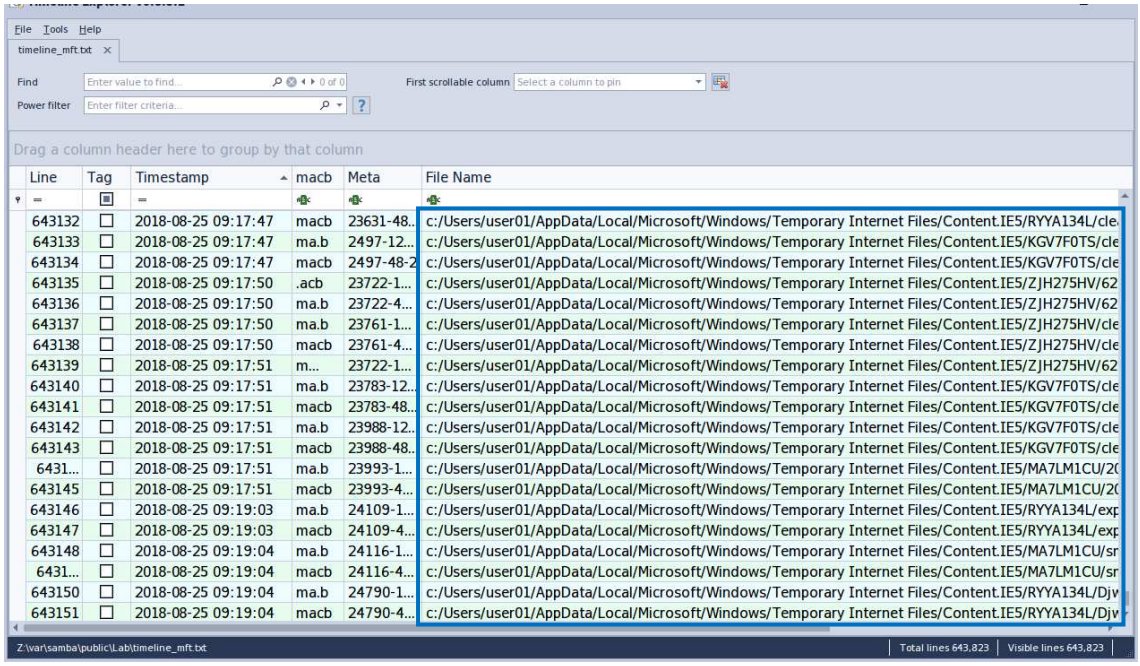
5. 実習用仮想マシンのメニュー（画面左下の赤丸アイコン）から「Windows Forensics Tools」-「Timeline Explorer」を起動します。
6. 「Timeline Explorer」で、前述の手順で作成したタイムライン（実行例では、timeline_mft.txt）を開きます。
7. 「Timeline Explorer」の「File Name」列を「rund11.exe」をフィルタします。
（アルファベット小文字の「l」（エル）ではなく、数字の「1」（イチ）なので注意）



8. 上記の結果より、不審ファイル「rund11.exe」の作成日時は「2018-08-25 09:19:38」であることが確認できます。また、不審ファイルの実行日時は、Prefetch ファイル(RUND11.EXE-D1A948B1.pf)の作成日時（「macb」列の「b」のタイムスタンプ）から、「2018-08-25 09:19:48」であることが確認できます。

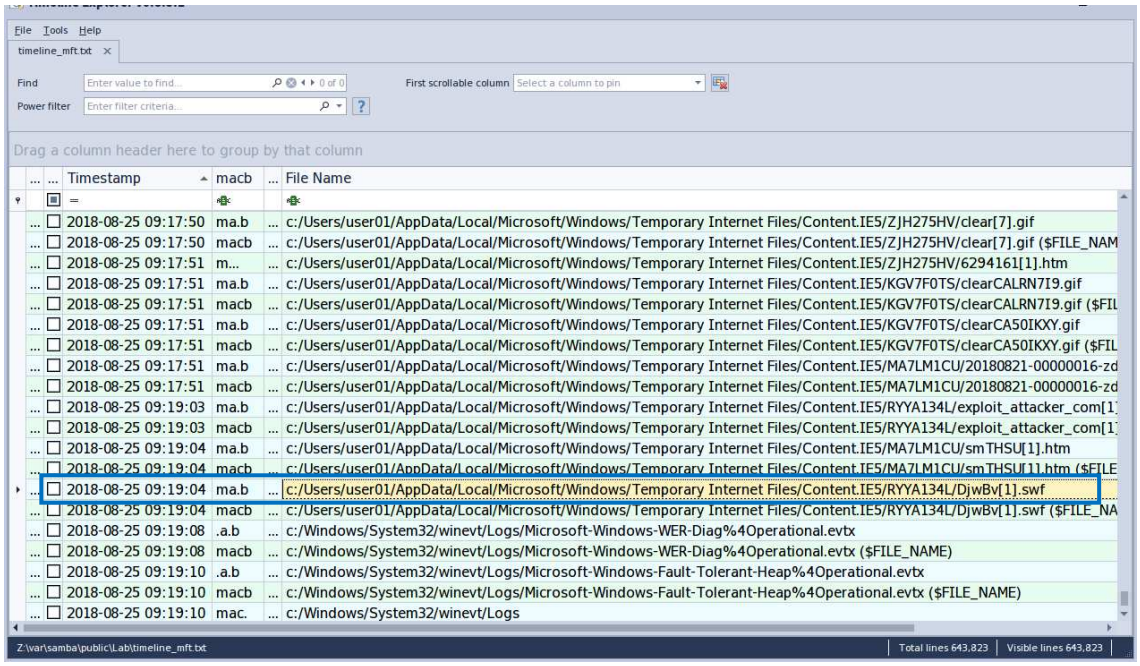
［問題①の答え］ 2018 年 08 月 25（土） 09:19

9. 不審ファイル「rundll11.exe」が作成された「2018-08-25 09:19:38」からタイムラインを遡ってみると、Internet Explorer の一時フォルダに多数のファイルが作成されていることが確認できます。このことから、社員は感染直前にウェブサイトを閲覧していたと推測できます。

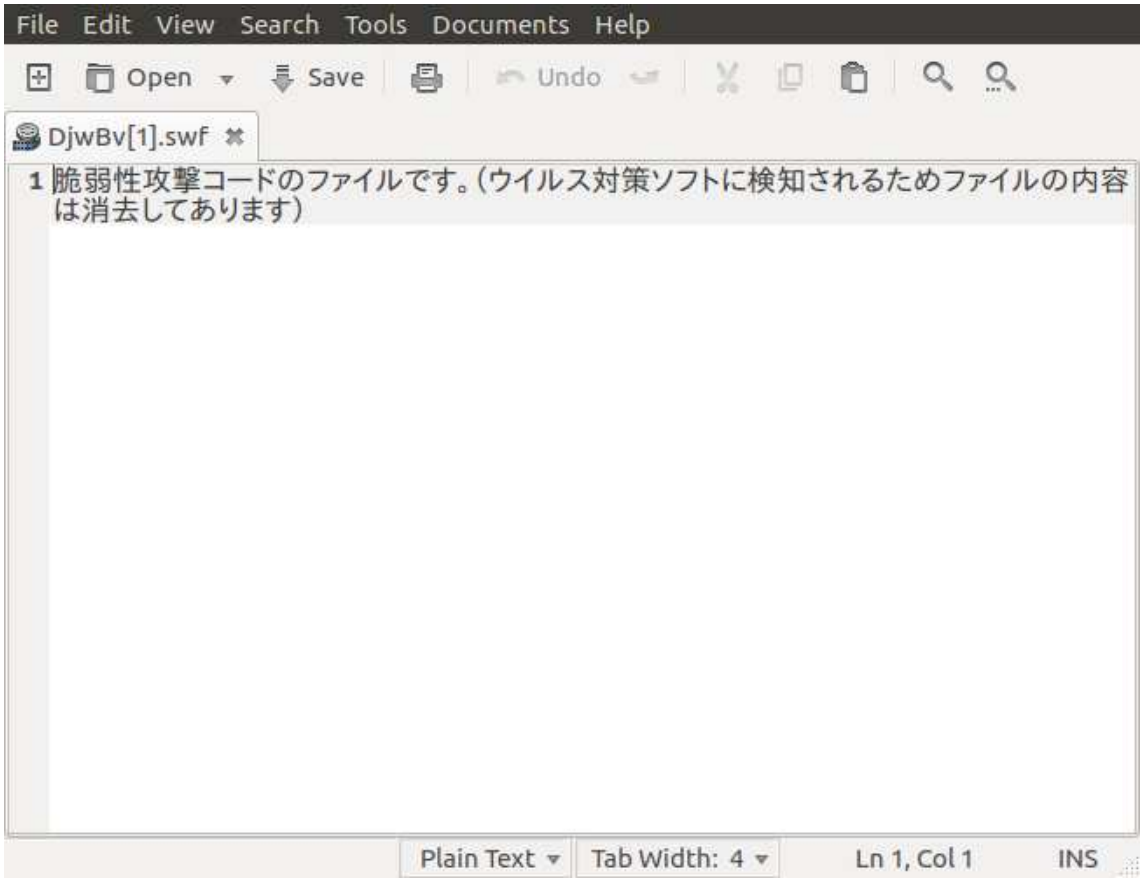


［問題②の答え］ ウェブサイト閲覧

10. 不審ファイル「rundll11.exe」が作成される直前、ブラウザの一時ファイルに Flash ファイル「DjwBv[1].swf」が書き込まれています。脆弱性攻撃に悪用されやすいファイルであるため、Virus Total などでウイルスチェックしてみたいところですが、実習では、ファイルの内容を削除してあるため、ヒントに従い、テキストエディタで内容を確認してみます。



11. 実習用仮想マシンのメニュー（画面左下の赤丸アイコン）から「アクセサリ」-「Pluma Text Editor」を起動し、「/var/samba/public/lab/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/DjwBv[1].swf」を開いてみます。



このファイルは、脆弱性攻撃コードだったようです。

［問題③の答え］ DjwBv[1].swf

12. 脆弱性攻撃コードのダウンロード URL を特定するため、ブラウザの閲覧履歴などもタイムライン解析してみます。

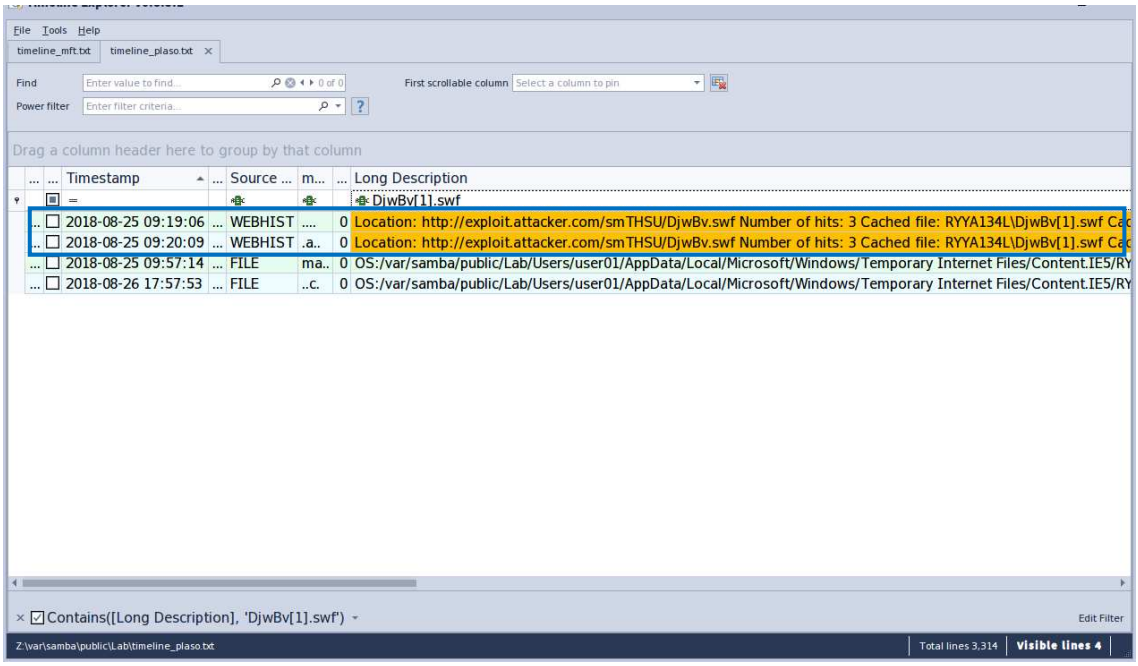
13. コマンドプロンプトで log2timeline コマンドを実行し、「Users」フォルダに格納されているエビデンスから、plaso storage 形式の中間ファイル（実行例では、「db.plaso」）を作成します。

```
caine@caine:/var/samba/public/lab$ log2timeline.py db.plaso Users/
plaso - log2timeline version 20171020

Source path     : /var/samba/public/Lab02/Users
Source type     : directory

Tasks:          Queued  Processing      To merge        Abandoned       Total
                0       0               0               0               536
（中略略）
Processing completed.

caine@caine:/var/samba/public/lab$
```

14. psort コマンドにより、前述の手順で作成した「db.plaso」からタイムラインを作成します。

```
caine@caine:/var/samba/public/lab$ psort.py -z Japan -o l2tcsv -w timeline_pl
aso.txt db.plaso
caine@caine:/var/samba/public/lab$
```

15. 「Timeline Explorer」で、前述の手順で作成したタイムライン（実行例では、timeline_plaso.txt）を開き、脆弱性攻撃コードのファイル名「DjwBv[1].swf」でフィルタをかけます。



16.「DjwBv[1].swf」のダウンロード元 URL は「http://exploit.attacker.com/smTHSU/DjwBv.swf」であることが確認できます。

［問題④の答え］ http://exploit.attacker.com/smTHSU/DjwBv.swf

以上で演習は終了です。お疲れさまでした。

回答例

① 不審なプログラム「rund11.exe」が作成および起動された日時
（年月日 時分まで特定）
2018 年 08 月 25（土） 09:19

② 「rundll11.exe」の起動直前の社員が操作していた内容の推測
（USB メモリへのファイルコピー、ウェブサイト閲覧、メール閲覧のいずれかを選択）
ウェブサイト閲覧

③ 感染に利用された脆弱性攻撃コードのファイル名
（タイムラインで怪しいと思ったファイルの内容を、テキストエディタ等で確認）
DjwBv[1].swf

④ 上記③で特定した脆弱性攻撃コードのダウンロード元 URL
http://exploit.attacker.com/smTHSU/DjwBv.swf