問題解説 Forensic

平成30年11月10日

仙台CTF推進プロジェクト
五十嵐 良一

Forensic01

問題1

検体を解析し、ダウンロード元URLを特定してください。

[検知したファイル]

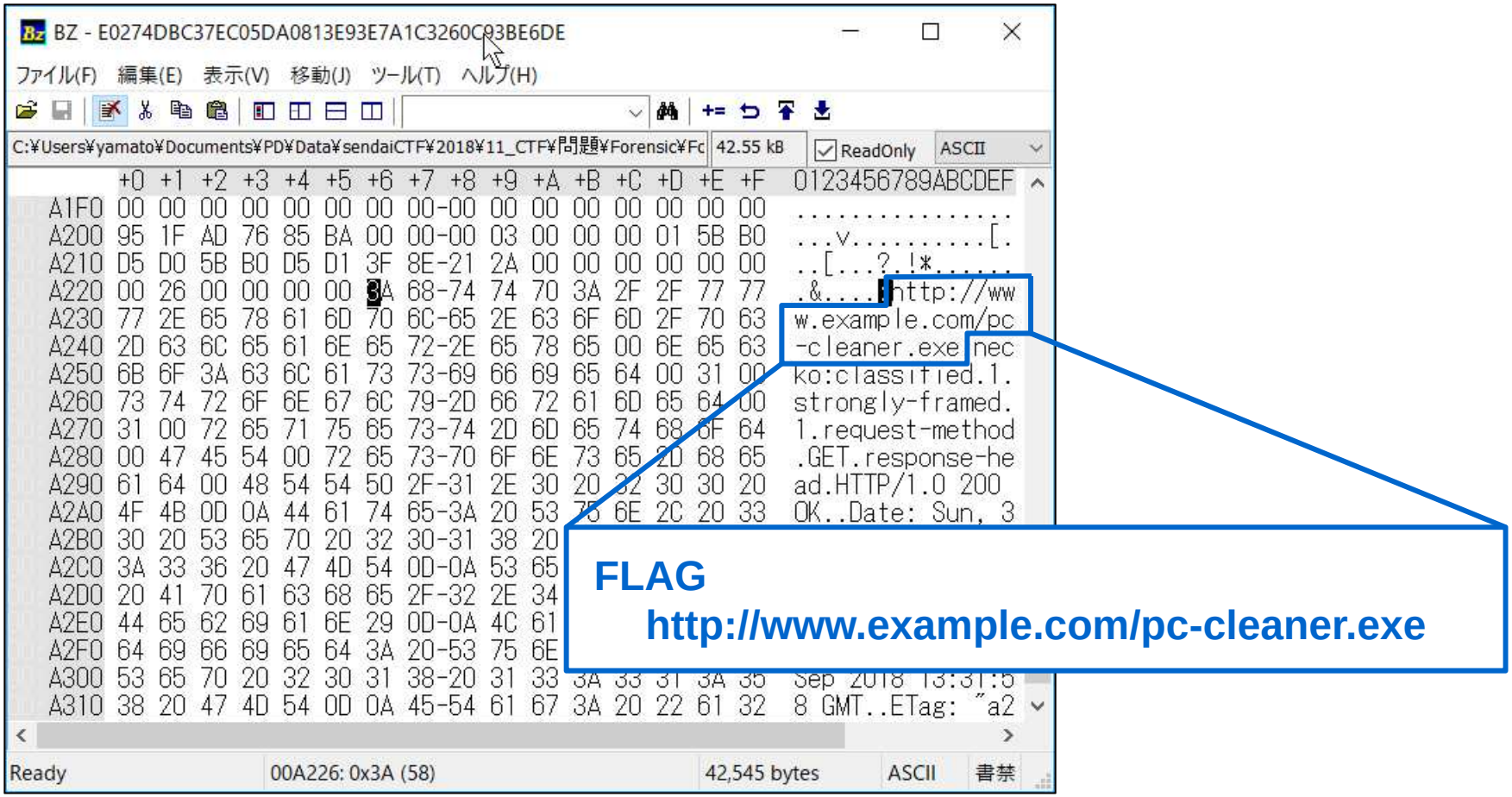
- **フォルダ名:**
  - C:¥Users¥user01¥AppData¥Local¥Mozilla¥Firefox¥Profiles¥o5j56hgo.default¥cache2¥entries
- **ファイル名:**
  - E0274DBC37EC05DA0813E93E7A1C3260C93BE6DE

[フラグ]

- **検体「E0274DBC37EC05DA0813E93E7A1C3260C93BE6DE」のダウンロード元のURL(半角、小文字)**
  例:http://www.sendai-ctf.org/abc.exe

解説

- Firefoxは、一時ファイル（キャッシュ）としてダウンロードしたファイルの末尾に、HTTPリクエスト/レスポンスの情報を追記するため、バイナリエディタで問題ファイルを確認することで、ダウンロード元URLを特定することができます。



Forensic02

問題2

検知したファイルのダウンロード元URLは、有名なフリーソフト「PC-Cleaner」（注記：架空のフリーソフト）の公式サイトのようです。「PC-Cleaner」の公式サイトを確認したところ、不正アクセス被害に遭い、マルウェアが混入されたプログラム「PC-Cleaner.exe」が配布されたというお詫び文書が掲載されていました。

社員（以下user01という）に確認したところ、ダウンロードした「PC-Cleaner.exe」を実行したか記憶が定かではないが、もしも実行していたとしても、すぐに削除したはずだと証言しています。あなたは、user01のパソコンはマルウェアに感染している可能性が高いと考え、パソコンをネットワークから隔離したうえで、いくつかのファイルをエビデンスとして証拠保全しました。

user01のパソコンから証拠保全したエビデンスを解析し、「PC-Cleaner.exe」が実行された日時を特定してください。

[フラグ]

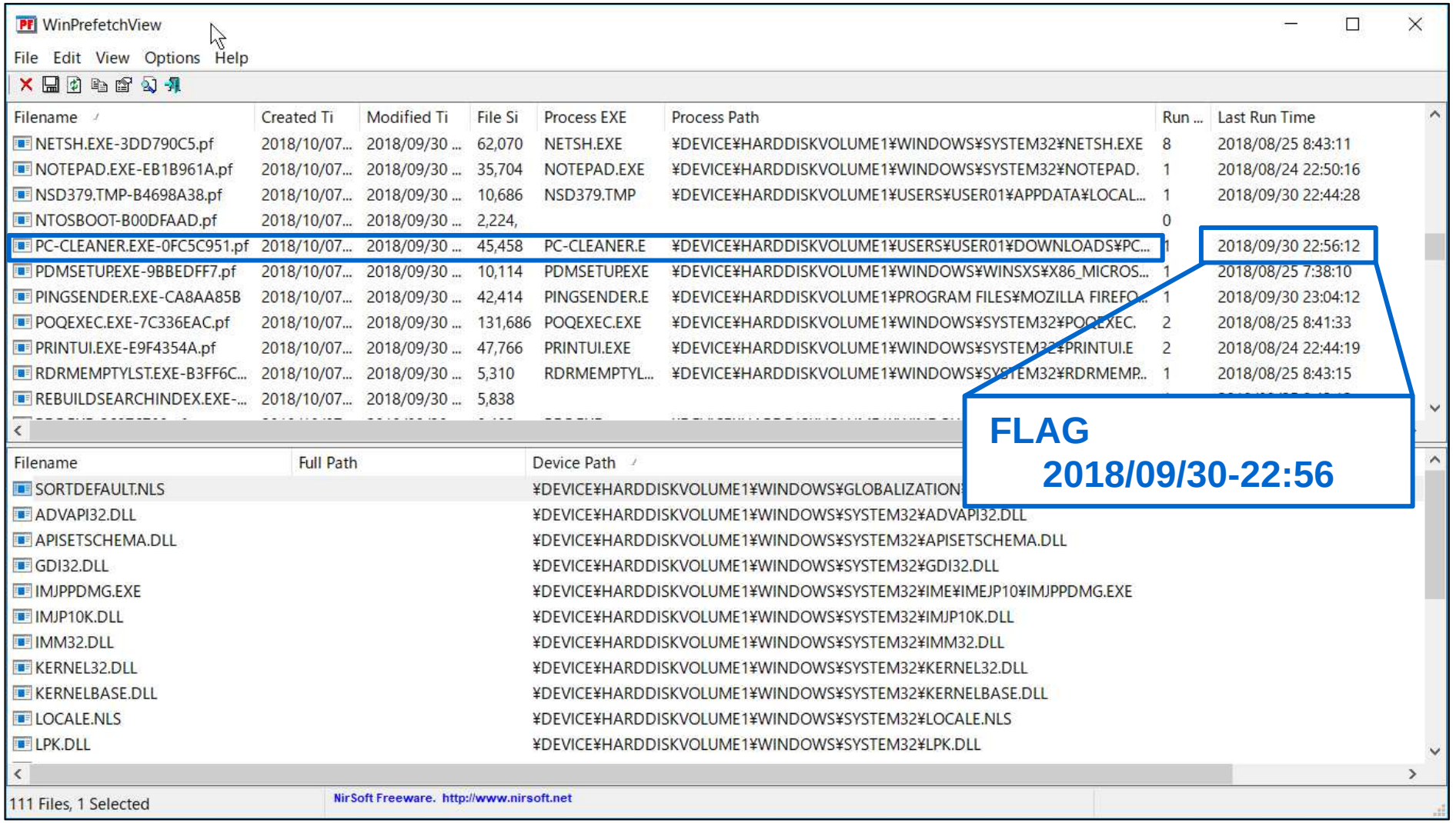
- フリーソフト「PC-Cleaner.exe」の実行日時（YYYY/MM/DD-hh:mm）（半角）
  例：2018/11/10-23:59

解説（1）

- Windowsには、アプリケーションの起動を高速化するための「Prefetch」と呼ばれる機能が搭載されており、アプリケーションが起動されると、「C:¥Windows¥Prefetch」に、Prefetchファイル（拡張子「.pf」で、アプリケーション名を含むファイル名）が作成されます。
- Prefetchファイルには、アプリケーションのフルパス、最終起動日時などが記録されているため、調査用ツール「WinPrefetchView」などを利用し、「PC-Cleaner.exe」の最終起動日時を確認することができます。

NirSoft WinPrefetchView　https://www.nirsoft.net/utils/win_prefetch_view.html

解説(2)


WinPrefetchView
File Edit View Options Help
Filename Created Ti Modified Ti File Si Process EXE Process Path Run ... Last Run Time
NETSH.EXE-3DD790C5.pf 2018/10/07... 2018/09/30 ... 62,070 NETSH.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥NETSH.EXE 8 2018/08/25 8:43:11
NOTEPAD.EXE-EB1B961A.pf 2018/10/07... 2018/09/30 ... 35,704 NOTEPAD.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥NOTEPAD. 1 2018/08/24 22:50:16
NSD379.TMP-B4698A38.pf 2018/10/07... 2018/09/30 ... 10,686 NSD379.TMP ¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥LOCAL... 1 2018/09/30 22:44:28
NTOSBOOT-B00DFAAD.pf 2018/10/07... 2018/09/30 ... 2,224, 0
PC-CLEANER.EXE-0FC5C951.pf 2018/10/07... 2018/09/30 ... 45,458 PC-CLEANER.E ¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥DOWNLOADS¥PC... 1 2018/09/30 22:56:12
PDMSETUP.EXE-9BBEDFF7.pf 2018/10/07... 2018/09/30 ... 10,114 PDMSETUP.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS... 1 2018/08/25 7:38:10
PINGSENDER.EXE-CA8AA85B 2018/10/07... 2018/09/30 ... 42,414 PINGSENDER.E ¥DEVICE¥HARDDISKVOLUME1¥PROGRAM FILES¥MOZILLA FIREFO... 1 2018/09/30 23:04:12
POQEXEC.EXE-7C336EAC.pf 2018/10/07... 2018/09/30 ... 131,686 POQEXEC.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥POQEXEC. 2 2018/08/25 8:41:33
PRINTUI.EXE-E9F4354A.pf 2018/10/07... 2018/09/30 ... 47,766 PRINTUI.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥PRINTUI.E 2 2018/08/24 22:44:19
RDRMEMPTYLST.EXE-B3FF6C... 2018/10/07... 2018/09/30 ... 5,310 RDRMEMPTYL... ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥RDRMEMP... 1 2018/08/25 8:43:15
REBUILDSEARCHINDEX.EXE-... 2018/10/07... 2018/09/30 ... 5,838
FLAG
2018/09/30-22:56
Filename Full Path Device Path
SORTDEFAULT.NLS ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥GLOBALIZATION
ADVAPI32.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVAPI32.DLL
APISETSCHEMA.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥APISETSCHEMA.DLL
GDI32.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥GDI32.DLL
IMJPPDMG.EXE ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥IME¥IMEJP10¥IMJPPDMG.EXE
IMJP10K.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥IMJP10K.DLL
IMM32.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥IMM32.DLL
KERNEL32.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥KERNEL32.DLL
KERNELBASE.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥KERNELBASE.DLL
LOCALE.NLS ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥LOCALE.NLS
LPK.DLL ¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥LPK.DLL
111 Files, 1 Selected
NirSoft Freeware. http://www.nirsoft.net

Forensic03

問題3

調査により、社員（以下、user01という）のパソコンは、マルウェアが混入したフリーソフトを実行していたことが確認されました。

フリーソフト「PC-Cleaner」（注記：架空のフリーソフト）に混入したマルウェアについて、セキュリティ研究者のブログなどで情報収集したところ、ダウンローダーという種類のマルウェアであり、他のマルウェア（以下、マルウェアBという）をダウンロードする機能を有しているようです。

マルウェアBは、実行されると、パソコンのあるフォルダに自身をコピーするとともに、パソコンのログオン時に自動的に実行されるようレジストリを改変するようです。

あなたは、user01のパソコンに潜伏しているマルウェアBの検体をウイルス対策ソフトの開発元に送付し、パターンファイルの作成を依頼する必要があると考えました。

user01のパソコンから証拠保全したエビデンスを解析し、マルウェアBのフルパスを特定してください。

[フラグ]

- マルウェアBのフルパス（半角）
  例：C:¥Windows¥abc.exe

解説(1)

- **$MFTを「MFTECmd」および「mactime」でタイムライン解析し、フリーソフト「PC-Cleaner」が実行された日時で2018/09/30-22:56」の直後に、不審なファイルが作成されていないか確認します。**

```
C:¥work>mftecmd -f $MFT --body . --bdl C
MFTECmd version 0.3.0.0

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

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

Warning: Administrator privileges not found!


Processed '$MFT' in 3.9603 seconds

Bodyfile output will be saved to '.¥20181007233902_MFTECmd_Output.body'

C:¥work>mactime -z Japan -b 20181007233902_MFTECmd_Output.body -m -d > timeline_mft.txt

C:¥work>
```

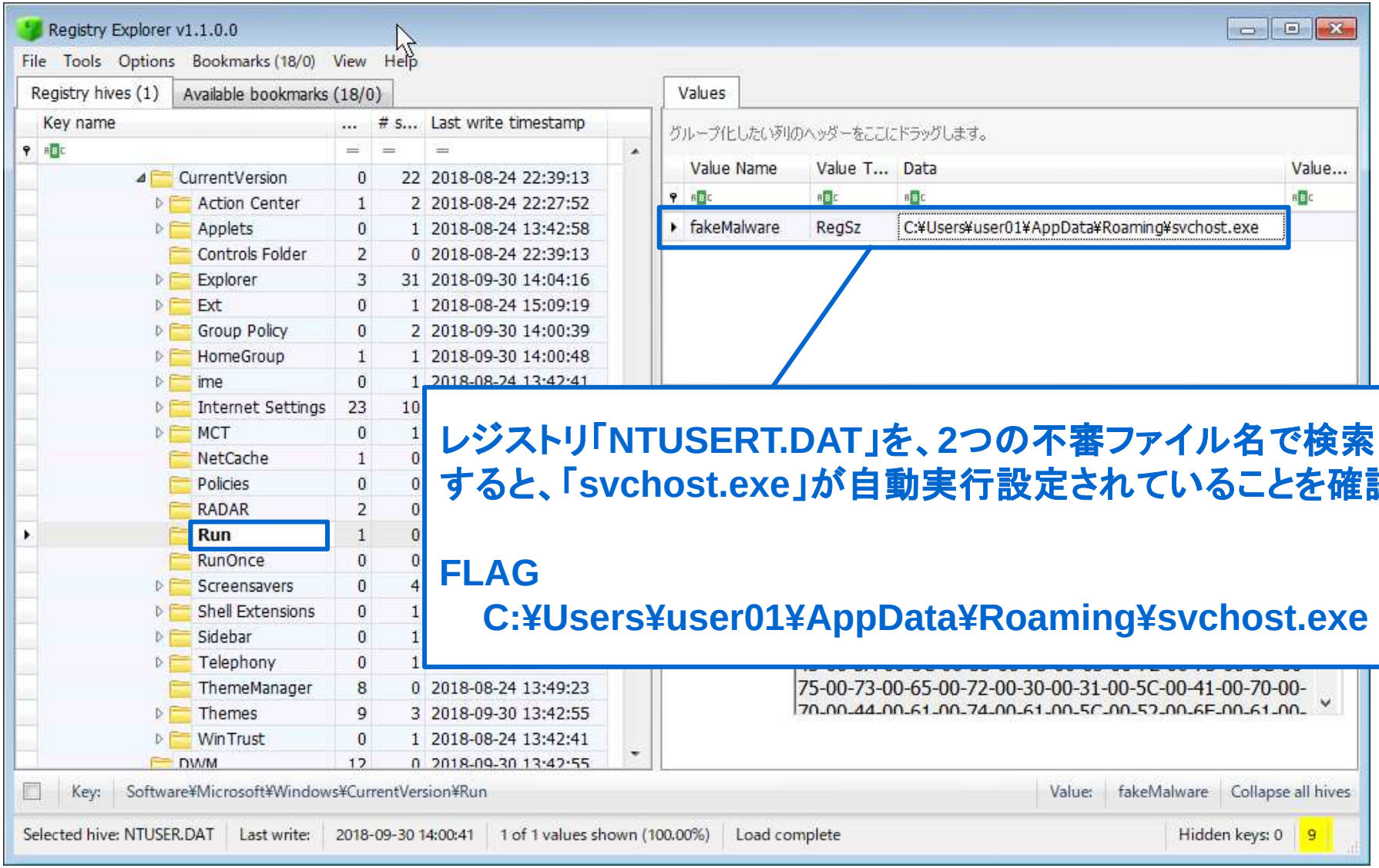
MFTECmd	https://github.com/EricZimmerman/MFTECmd/releases
mactime	https://www.sleuthkit.org/ （The Sleuth Kitに同梱）

解説(2)

Line	...	Timestamp	macb	Meta	File Name	File Size
640191		2018-09-30 22:55:33	macb	46208-128-1	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/cache2/entries/18CE467B00ED7B507CC72681EDCE...	101
640192		2018-09-30 22:55:33	macb	46208-48-2	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/cache2/entries/18CE467B00ED7B507CC72681EDCE...	101
640193		2018-09-30 22:55:40	m...	1719-128-4	c:/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf	11960
640194		2018-09-30 22:55:41	m...	1757-128-4	c:/Windows/Prefetch/SEARCHFILTERHOST.EXE-AA7A1FDD.pf	18804
640195		2018-09-30 22:56:09	m...	11727-128-4	c:/Windows/Prefetch/DLLHOST.EXE-71214090.pf	64754
640196		2018-09-30 22:56:12	mac.	18339-144-0	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L	0
640197		2018-09-30 22:56:12	ma.b	18467-128-4	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/lupin[1].jpg	37888
640198		2018-09-30 22:56:12	macb	18467-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/lupin[1].jpg ($FILE_NAME)	37888
640199		2018-09-30 22:56:12	macb	46113-128-3	c:/Users/user01/AppData/Local/Temp/a.exe	37888
640200		2018-09-30 22:56:12	macb	46113-48-2	c:/Users/user01/AppData/Local/Temp/a.exe ($FILE_NAME)	37888
640201		2018-09-30 22:56:12	m.c.	46222-128-1	c:/Users/user01/AppData/Roaming/svchost.exe	37888
640202		2018-09-30 22:56:19	m...	11787-128-4	c:/Windows/Prefetch/RUNDLL32.EXE-AFD98684.pf	18692
640203		2018-09-30 22:56:22	ma.b	18482-128-4	c:/Windows/Prefetch/PC-CLEANER.EXE-0FC5C951.pf	45458
640204		2018-09-30 22:56:22	macb	18482-48-2	c:/Windows/Prefetch/PC-CLEANER.EXE-0FC5C951.pf ($FILE_NAME)	45458
640205		2018-09-30 22:56:22	ma.b	46183-128-4	c:/Windows/Prefetch/A.EXE-E042BB59.pf	28550
640206		2018-09-30 22:56:22	macb	46183-48-2	c:/Windows/Prefetch/A.EXE-E042BB59.pf ($FILE_NAME)	28550
640207		2018-09-30 22:				0
640208		2018-09-30 22:			==.ico	1086
640209		2018-09-30 22:			==.ico ($FI...	1086
640210		2018-09-30 22:				0
640211		2018-09-30 22:				25944
640212		2018-09-30 22:			tions-ms	19362
640213		2018-09-30 22:			tions-ms (...	19362
640214		2018-09-30 22:			==.ico	2989
640215		2018-09-30 22:56:24	macb	46209-48-2	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/jumpListCache/MW3sU0k0_hvs1i7XbP1NKQ==.ico ($FI...	2989
640216		2018-09-30 22:56:29	m...	44475-128-4	c:/Windows/Prefetch/AUDIODG.EXE-D0D776AC.pf	30650
640217		2018-09-30 22:56:45	m.c.	45891-128-4	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/cache2/entries/8C8ED651EE3EA7170F1F56FA86C40...	51953

2つの不審ファイルを発見
C:/Users/user01/AppData/Local/Temp/a.exe
C:/Users/user01/AppData/Roaming/svchost.exe

解説(3)



レジストリ「NTUSERT.DAT」を、2つの不審ファイル名で検索すると、「svchost.exe」が自動実行設定されていることを確認

FLAG

C:¥Users¥user01¥AppData¥Roaming¥svchost.exe

Forensic04

問題4

感染していたマルウェアの挙動について情報収集したところ、以下のようなキーロガー機能を有していることが判明しました。

[キーロガー機能の動作]

(1) 利用者が入力した、オンラインバンキング等のユーザーIDとパスワードを「C:¥Users¥【ユーザー名】¥AppData¥keylogger.txt」に記録する。

(2) 「keylogger.txt」の内容を、C2サーバに送信する。

(3) 「keylogger.txt」の内容を、0バイトの文字列で上書き保存することにより消去する。

感染したパソコンを確認したところ「keylogger.txt」が発見されたため、何らかのユーザーIDとパスワードが情報流出した可能性があると考えられます。

あなたは、感染したパソコンディスクイメージを解析し、消去されたデータ(＝情報流出したデータ)の復元を試みることにしました。

感染したパソコンの模擬ディスクイメージを解析し、情報流出した「パスワード」を特定してください。

[フラグ]

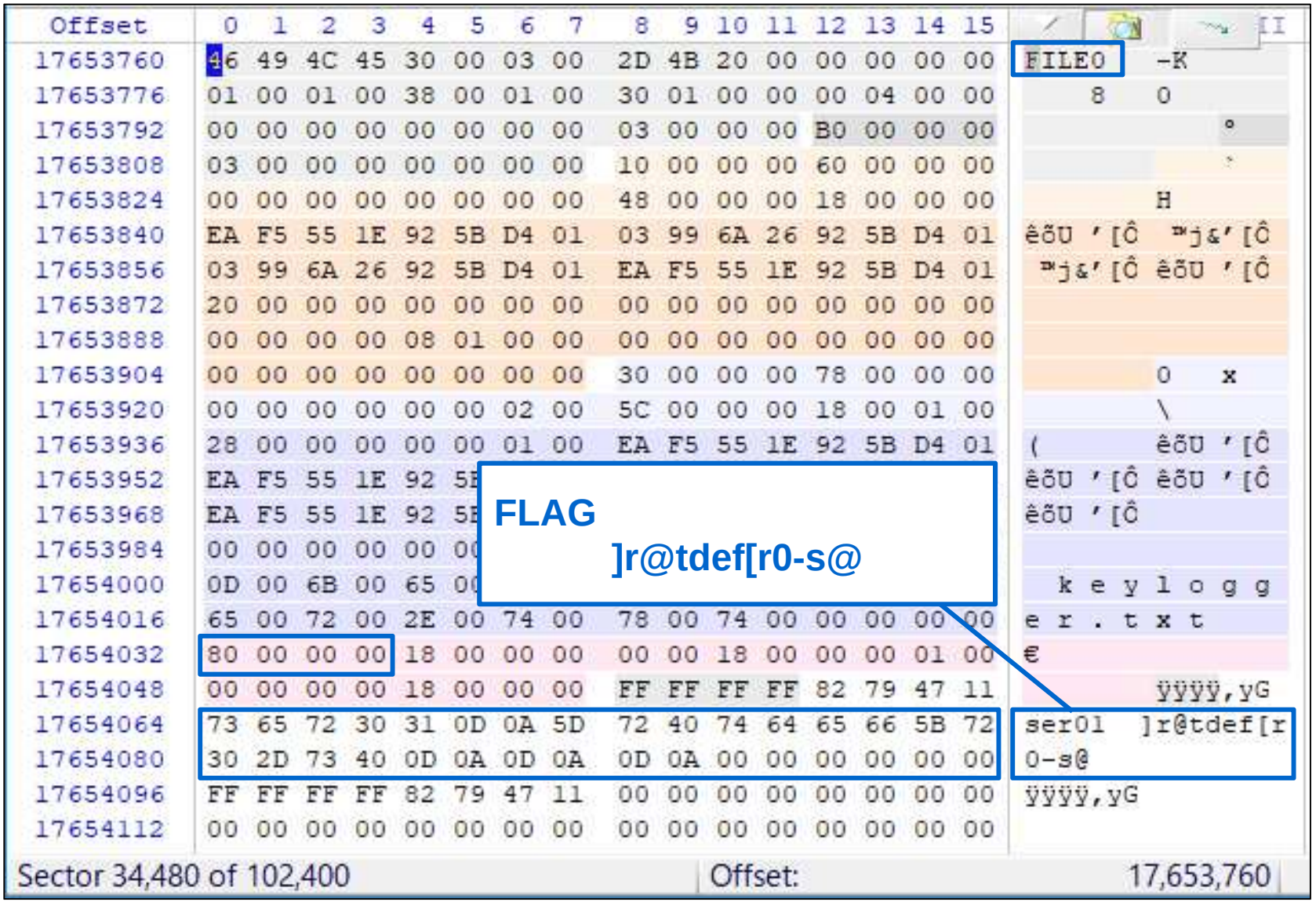
- **「keylogger.txt」に記録されていたパスワードと思われる文字列(半角)**
  例:1qaz2wsx3edc

解説（1）

- 問題ファイルのディスクイメージのファイルシステムは、NTFSです。
- NTFSは、ファイル名やタイムスタンプなどの属性情報「$MFT」のFILEレコード記録します。また、ファイルに記録されるデータのサイズが小さい場合、FILEレコードにデータが保存されます。
- また、FILEレコードに保存されたデータは、元データよりも小さなデータで上書き保存された場合、FILEレコードに古いデータの残骸が残るという特性があります。

- 従って、ディスクイメージをバイナリエディタなどで開き、ファイルシステムを目視確認することで、「keylogger.txt」の古いデータの残骸を確認することができます。

解説(2)



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17653760	46	49	4C	45	30	00	03	00	2D	4B	20	00	00	00	00	00
17653776	01	00	01	00	38	00	01	00	30	01	00	00	00	04	00	00
17653792	00	00	00	00	00	00	00	00	03	00	00	00	B0	00	00	00
17653808	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
17653824	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
17653840	EA	F5	55	1E	92	5B	D4	01	03	99	6A	26	92	5B	D4	01
17653856	03	99	6A	26	92	5B	D4	01	EA	F5	55	1E	92	5B	D4	01
17653872	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
17653888	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00
17653904	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00
17653920	00	00	00	00	00	00	02	00	5C	00	00	00	18	00	01	00
17653936	28	00	00	00	00	00	01	00	EA	F5	55	1E	92	5B	D4	01
17653952	EA	F5	55	1E	92	5B										
17653968	EA	F5	55	1E	92	5B										
17653984	00	00	00	00	00	00										
17654000	0D	00	6B	00	65	00										
17654016	65	00	72	00	2E	00	74	00	78	00	74	00	00	00	00	00
17654032	80	00	00	00	18	00	00	00	00	00	18	00	00	00	01	00
17654048	00	00	00	00	18	00	00	00	FF	FF	FF	FF	82	79	47	11
17654064	73	65	72	30	31	0D	0A	5D	72	40	74	64	65	66	5B	72
17654080	30	2D	73	40	0D	0A	0D	0A	0D	0A	00	00	00	00	00	00
17654096	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00
17654112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Sector 34,480 of 102,400 | Offset: 17,653,760