



仙台CTF2018 セキュリティ技術競技会(CTF)

# 問題解説 復習問題

平成30年11月10日  
仙台CTF推進プロジェクト  
五十嵐 良一



## Lab.01

---

# 問題1

---

## [シナリオ]

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、最近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、デスクトップに作成されていた身に覚えのないファイルを、マルウェアとして検知したようです。

あなたは、検知したファイル(検体)は、過去のいつかの時点で感染していたマルウェアである可能性が高いと判断し、社員用パソコンから調査に必要なエビデンスを証拠保全のうえ、感染原因を調査することとしました。

検体が作成および起動された日時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\Desktop¥	検査の種類	: オンデマンドスキャン
ファイル名 : 1.exe	処理結果	: 無視
脅威名 : BKDR_POISON.DS		

## [フラグ]

- 検体「1.exe」が作成および起動された日時(YYYY/MM/DD-hh:mm)(半角)  
例:2018/11/10-23:59

# 解説(1)

---

## 解き方その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、「1.exe」の最終起動日時を確認することができます。

## 解き方その2

- 問題ファイルの「Prefetch」は、ZIP圧縮された際にタイムスタンプが更新されています。
- 代わりに、\$MFTを「MFTECmd」および「mactime」でタイムライン解析し、「Prefetch」の本来のタイムスタンプを確認することでも、「1.exe」のおおよそ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](https://www.nirsoft.net/utils/win_prefetch_view.html)  
MFTECmd <https://github.com/EricZimmerman/MFTECmd/releases>  
mactime <https://www.sleuthkit.org/> (The Sleuth Kitに同梱)

# 解説(2) 解き方その1

The screenshot shows the WinPrefetchView application window. The main table lists files with columns for Filename, Created Time, Modified Time, File Si, Process EXE, Process Path, Run, and Last Run Time. The entry for '1.EXE-1C174A77.pf' is highlighted in blue, and a blue box with the text 'FLAG 2018/10/07-17:52' is overlaid on it. Below the main table is a detailed view of the selected file, showing its Full Path and Device Path.

Filename	Created Time	Modified Time	File Si	Process EXE	Process Path	Run	Last Run Time
1.EXE-1C174A77.pf	2018/10/07 18:39:53	2018/10/07 18:39:53	22,592	1.EXE	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥DESKTOP¥1.EXE	2	2018/10/07 17:52:38
AUDIODG.EXE-D0D...	2018/10/07 18:39:54	2018/10/07 18:39:54	30,590	AUDIODG.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥AUDIODG.	3	2018/08/25 9:11:31
BCDEDIT.EXE-23D6A...	2018/10/07 18:39:54	2018/10/07 18:39:54	6,064	BCDEDIT.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥BCDEDITE	1	2018/08/25 7:28:15
BFSVC.EXE-A870E99...	2018/10/07 18:39:54	2018/10/07 18:39:54	39,762	BFSVC.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥BFSVC.EXE	4	2018/08/25 8:43:15
CLEANUPINTLCACH...	2018/10/07 18:39:53	2018/10/07 18:39:53	7,914	CLEANUPINTL...	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS...	1	2018/08/25 8:43:12
CLEANUPUSERCURR...	2018/10/07 18:39:53	2018/10/07 18:39:53	6,476	CLEANUPUSER...	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS...	1	2018/08/25 8:43:15
CLEANUPUSERCURR...	2018/10/07 18:39:53	2018/10/07 18:39:53	6,464	CLEANUPUSER...	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS...	1	2018/08/25 8:43:13
CLEANUPUSERCURR...	2018/10/07 18:39:53	2018/10/07 18:39:53	6,476	CLEANUPUSER...	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS...	1	2018/08/25 8:43:14
CLEANUPUSERCURR...	2018/10/07 18:39:53	2018/10/07 18:39:53	6,488	CLEANUPUSER...	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥WINSXS¥X86_MICROS...	1	2018/08/25 8:43:15
CLRGC.EXE-22C68C7...	2018/10/07 18:39:53	2018/10/07 18:39:53	20,128	CLRGC.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CLRGC.EXE	1	2018/08/25 8:43:15
CMD.EXE-89305D47.	2018/10/07 18:39:54	2018/10/07 18:39:54	8,256	CMD.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CMD.EXE	1	2018/08/25 8:43:15

Filename	Full Path	Device Path
INDEX.DAT	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥LOCAL¥MICROSOFT¥WINDOWS¥HISTORY¥HISTORY.IE5¥INDEX.DAT	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥LOCAL¥MICROSOFT¥WINDOWS¥HISTORY¥HISTORY.IE5¥INDEX.DAT
INDEX.DAT	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥LOCAL¥MICROSOFT¥WINDOWS¥TEMPORARY INTERNET FILES¥CO	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥LOCAL¥MICROSOFT¥WINDOWS¥TEMPORARY INTERNET FILES¥CO
INDEX.DAT	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥ROAMING¥MICROSOFT¥WINDOWS¥COOKIES¥INDEX.DAT	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥APPDATA¥ROAMING¥MICROSOFT¥WINDOWS¥COOKIES¥INDEX.DAT
1.EXE	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥DESKTOP¥1.EXE	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USER01¥DESKTOP¥1.EXE
SORTDEFAULT.NLS	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥GLOBALIZATION¥SORTING¥SORTDEFAULT.NLS	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥GLOBALIZATION¥SORTING¥SORTDEFAULT.NLS
ADVAPI32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVAPI32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVAPI32.DLL
ADVPACK.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVPACK.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVPACK.DLL
APISETSHEMA.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥APISETSHEMA.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥APISETSHEMA.DLL
C_1252.NLS	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥C_1252.NLS	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥C_1252.NLS
CFGMR32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CFGMR32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CFGMR32.DLL
CRYPT32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CRYPT32.DLL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥CRYPT32.DLL

106 Files, 1 Selected      NirSoft Freeware. <http://www.nirsoft.net>

## 解説(3) 解き方その2

---

```
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 3.6170 seconds

Bodyfile output will be saved to '.¥20181007190039_MFTECmd_Output.body'

C:¥work>mactime -b 20181007190039_MFTECmd_Output.body -z Japan -m -d > timeline_mft.txt

C:¥work>
```



## 解説(4) 解き方その2

Line	Tag	Timestamp	macb	Meta	File Name	File Size
=	<input checked="" type="checkbox"/>	=	mac	Meta	File Name	File Size
643820	<input type="checkbox"/>	2018-10-07 17:52:05	mac.	353-144-0	c:/Users/user01/Desktop	0
643821	<input type="checkbox"/>	2018-10-07 17:52:06	m.c.	11953-128-4	c:/Windows/AppCompat/Programs/RecentFil...	15674
643822	<input type="checkbox"/>	2018-10-07 17:52:16	a.b	27131-128-4	1.EXE	22592
643823	<input type="checkbox"/>	2018-10-07 17:52:16	macb	27131-48-2	c:/Windows/Prefetch/1.EXE-1C174A77.pf (\$FIL	22592
643824	<input type="checkbox"/>	2018-10-07 17:52:16	mac.	43308-144-0	c:/Windows/Prefetch	0
643825	<input type="checkbox"/>	2018-10-07 17:52:32	m.c.	43995-128-4	c:/Windows/Prefetch/WMIAPSRV.EXE-57628...	22970
643826	<input type="checkbox"/>	2018-10-07 17:52:36	.c.	18089-128-3	c:/Users/user01/AppData/Roaming/Microsoft...	65536
643827	<input type="checkbox"/>	2018-10-07 17:52:36	m.c.	44246-128-11	c:/Users/user01/AppData/Roaming/Adobe/Fl...	0
643828	<input type="checkbox"/>	2018-10-07 17:52:38	m.c.	15685-128-3	c:/Users/user01/AppData/Roaming/Microsoft...	98304
643829	<input type="checkbox"/>			3-4	c:/Users/user01/AppData/Local/Microsoft/W...	5754
643830	<input type="checkbox"/>			2	c:/Users/user01/AppData/Local/Microsoft/W...	5754
643831	<input type="checkbox"/>			4-0	c:/Users/user01/AppData/Local/Microsoft/In...	0
643832	<input type="checkbox"/>	2018-10-07 17:52:38	macb	18088-128-4	c:/Users/user01/AppData/Local/Microsoft/W...	2219
643833	<input type="checkbox"/>	2018-10-07 17:52:38	macb	18088-48-2	c:/Users/user01/AppData/Local/Microsoft/W...	2219
643834	<input type="checkbox"/>	2018-10-07 17:52:38	m.c.	18329-128-3	c:/Users/user01/AppData/Local/Microsoft/W...	212992
643835	<input type="checkbox"/>	2018-10-07 17:52:38	mac	18332-144-0	c:/Users/user01/AppData/Local/Microsoft/W...	0

**FLAG**

**2018/10/07-17:52**



## Lab.02

---



## 問題2

---

あなたは、感染パソコンをタイムライン解析したところ、ウェブサイト閲覧中に脆弱性攻撃を受けた痕跡を発見しました。

\$MFT (Lab.01の添付ファイル)のタイムライン解析、ならびにInternet Explorerの一時ファイル(この問題の添付ファイル)の解析により、感染に利用された脆弱性攻撃コードのファイル名を推測してください。

なお、脆弱性攻撃コードのファイルは、内容をテキストに書き換えてあるため、危険はありません。

### [フラグ]

- 感染に利用された脆弱性攻撃コードのファイル名(半角)  
例: abc.swf

## 解説(1)

- \$MFTを「MFTECmd」および「mactime」でタイムライン解析し、「1.exe」が作成・起動された直前の状況を確認し、脆弱性攻撃に悪用される不審なファイルへのアクセスが発生していないか確認します。(例: Adobe Flash、Java、PDFなど)

```
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 3.6170 seconds

Bodyfile output will be saved to '.\20181007190039_MFTECmd_Output.body'

C:\work>mactime -b 20181007190039_MFTECmd_Output.body -z Japan -m -d > timeline_mft.txt

C:\work>
```

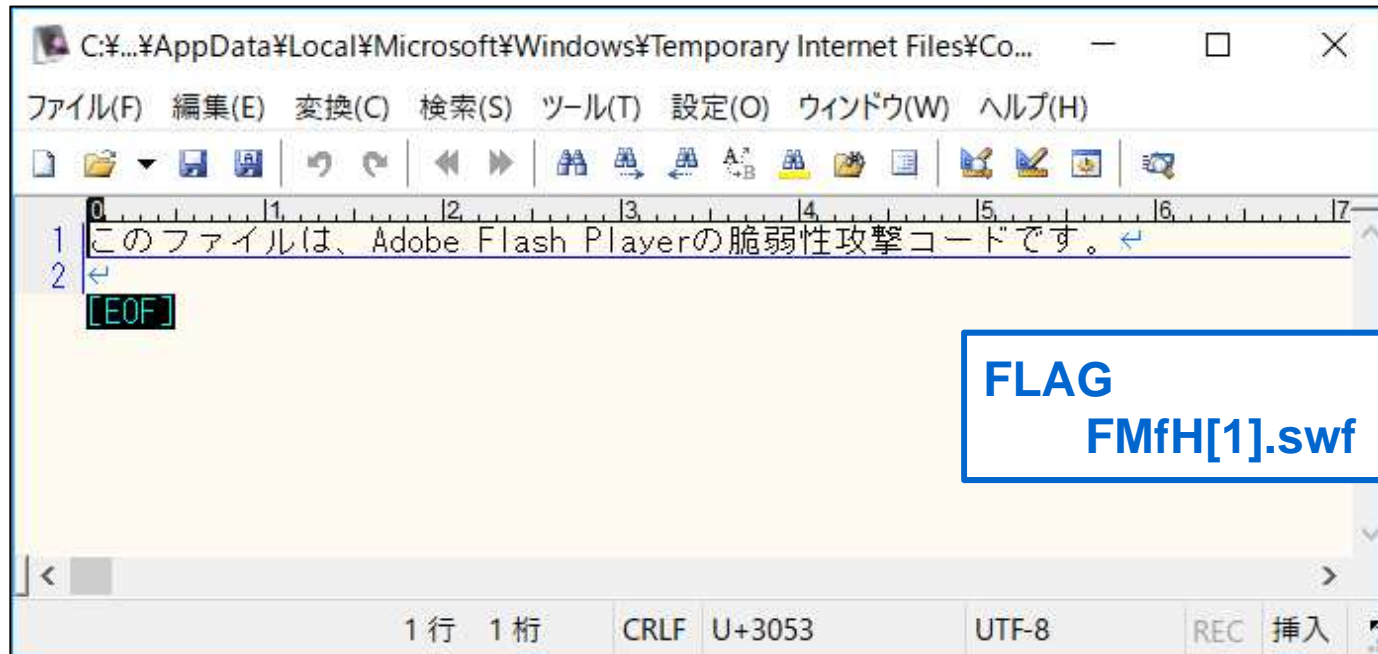
## 解説(2)

Line	Timestamp	macb	Meta	File Name
643808	2018-10-07 17:51:06	macb	27126-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/ZJH275HV/directlink.min[1].js (\$FILE_NAME)
643809	2018-10-07 17:51:07	m.c.	12381-128-1	c:/System Volume Information/{7b920070-a7f5-11e8-bf79-000c29c6c7e2}{3808876b-c176-4e48-b7ae-04046e6cc752}
643810	2018-10-07 17:51:10	m.c.	18948-128-4	c:/Users/user01/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Active/{18599294-CA0E-11E8-8D64-F48C503B644B}.c
643811	2018-10-07 17:51:12	m.c.	17773-128-3	c:/Windows/ServiceProfiles/NetworkService/AppData/Roaming/Microsoft/SoftwareProtectionPlatform/Cache/cache.dat
643812	2018-10-07 17:52:02	ma.b	24790-128-4	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/KGV7F0TS/sc2018_attacker_com[1].htm
643813	2018-10-07 17:52:02	macb	24790-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/KGV7F0TS/sc2018_attacker_com[1].htm
643814	2018-10-07 17:52:03	ma.b	26223-128-4	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/gksoLx[1].htm
643815	2018-10-07 17:52:03	macb	26223-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/gksoLx[1].htm (\$FILE_NAME)
643816	2018-10-07 17:52:03	ma.b	27128-128-4	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/ZJH275HV/FMfH[1].swf
643817	2018-10-07 17:52:03	macb	27128-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/ZJH275HV/FMfH[1].swf (\$FILE_NAME)
643818	2018-10-07 17:52:05	macb	27130-128-3	c:/Users/user01/Desktop/1.exe
643819	2018-10-07 17:52:05	macb	27130-48-2	c:/Users/user01/Desktop/1.exe (\$FILE_NAME)
643820	2018-10-07 17:52:05	mac.	353-144-0	c:/Users/user01/Desktop
643821	2018-10-07 17:52:06	m.c.	11953-128-4	c:/Window
643822	2018-10-07 17:52:16	a.b	27131-128-4	c:/Window
643823	2018-10-07 17:52:16	macb	27131-48-2	c:/Window
643824	2018-10-07 17:52:16	mac.	43308-144-0	c:/Window
643825	2018-10-07 17:52:32	m.c.	43995-128-4	c:/Window
643826	2018-10-07 17:52:36	.c.	18089-128-3	c:/Users/

「1.exe」が作成される直前に、Adobe Flashファイル「FMfH[1].swf」にアクセスしている。

## 解説(3)

### ◆ 「 FMfH[1].swf 」の内容



```
C:\...\AppData\Local\Microsoft\Windows\Temporary Internet Files\Co...
ファイル(F) 編集(E) 変換(C) 検索(S) ツール(T) 設定(O) ウィンドウ(W) ヘルプ(H)
このファイルは、Adobe Flash Playerの脆弱性攻撃コードです。
[EOF]
```

**FLAG**  
**FMfH[1].swf**

1行 1桁 CRLF U+3053 UTF-8 REC 挿入



## Lab.03

---

## 問題3

---

あなたは、脆弱性攻撃コードのダウンロード元URLを特定し、プロキシサーバで通信を遮断したいと考えました。

Internet Explorerの一時ファイル(Lab.02の添付ファイル)を解析し、脆弱性攻撃コードのダウンロード元URLを特定してください。

[フラグ]

脆弱性攻撃コードのダウンロード元URL(半角、小文字)

例: `http://www.example.com/aaa.swf`



## 解説(1)

- 問題ファイル(Internet Explorerの一時ファイル)を、Plaso(log2timeline)でタイムライン解析し、問題2で特定した脆弱性攻撃コード「FMfH[1].swf」のダウンロード元URLを特定します。

```
C:¥work>log2timeline.py db.plaso Users¥
Checking availability and versions of dependencies.
[OPTIONAL]      missing: lzma.
[OK]
(以下略)
C:¥work>psort.py -z Japan -o l2tcsv -w timeline_plaso.txt db.plaso
2018-10-07 21:23:25,953 [WARNING] (MainProcess) PID:1252 <psort_tool> Appending to an already existing storage
file.
Processing completed.

***** Export results *****
      Events processed : 3138
      Events MACB grouped : 2331
      Events filtered : 0
      Events from time slice : 0
-----

C:¥work¥misc>
```

Plaso(log2timeline)

<https://github.com/log2timeline/plaso>

## 解説(2)

Line	Timestamp	macb	Long Description
1362	2018-10-07 17:51:44	0	Location: https://s.yimg.jp/lib/news/socialModule/tab_1_10-min.js Number of hits: 1 Cached file: RYYA134L¥tab_1_10-min[1].js Cach...
1363	2018-10-07 17:51:54	0	Location: https://s.yimg.jp/images/top/sp/cgrade/pb_bg.gif Number of hits: 2 Cached file: ZJH275HV¥pb_bg[1].gif Cached file size: 94...
1364	2018-10-07 17:51:56	0	Location: https://s.yimg.jp/images/jpnews/js/tpc/pages.ult.min.js?date=20160720 Number of hits: 2 Cached file: RYYA134L¥pages.ult...
1365	2018-10-07 17:51:58	0	Location: https://s.yimg.jp/images/jpnews/cre/pickup/pc/images/ico_light.png Number of hits: 2 Cached file: KGV7F0TS¥ico_light[1]...
1366	2018-10-07 17:52:02	0	Location: https://s.yimg.jp/yui/jp/mh/pc/1.5.3/css/std.css Number of hits: 6 Cached file: RYYA134L¥std[1].css Cached file size: 121...
1367	2018-10-07 17:52:02	0	Location: http://sc2018.attacker.com/ Number of hits: 1 Cached file: KGV7F0TS¥sc2018_attacker_com[1].htm Cached file size: 7295...
1368	2018-10-07 17:52:04	0	Location: http://sc2018.attacker.com/gksoLx/ Number of hits: 2 Cached file: RYYA134L¥gksoLx[1].htm Cached file size: 1723 HTTP ...
1369	2018-10-07 17:52:04	0	Location: http://sc2018.attacker.com/gksoLx/FMfH.swf Number of hits: 2 Cached file: ZJH275HV¥FMfH[1].swf Cached file size: 43233
1370	2018-10-07 17:52:04	0	Location: http://sc2018.attacker.com/ Number of hits: 1 Cached file: KGV7F0TS¥sc2018_attacker_com[1].htm Cached file size: 7295...
1371	2018-10-07 17:52:20	0	Location: https://s.yimg.jp/images/top/sp/cgrade/iconMail.gif Number of hits: 2 Cached file: KGV7F0TS¥iconMail[1].gif Cached file si...
1372	2018-10-07 17:52:36	0	Location: https://s.yimg.jp/images/jpnews/cre/bylines/js/common_v1.js?v=1535507123 Number of hits: 1 Cached file: ZJH275HV¥co...
1373	2018-10-07 17:52:36	0	Location: http://sc2018.attacker.com/gksoLx/ Number of hits: 2 Cached file: RYYA134L¥gksoLx[1].htm Cached file size: 1723 HTTP ...
1374	2018-10-07 17:52:36	0	Location: http://sc2018.attacker.com/gksoLx/FMfH.swf Number of hits: 2 Cached file: ZJH275HV¥FMfH[1].swf Cached file size: 43233
1375	2018-10-07 17:52:38	0	Location: https://s.yimg.jp/images/jpnews/js/libs/knockout/3.3.0/knockout.min.js Number of hits: 2 Cached file: RYYA134L¥knockout...
1376	2018-10-07 17:52:38	0	Location: res://ieframe.dll/acr_error.htm Number of hits: 1 Cached file: KGV7F0TS¥acr_error[1] Cached file size: 5754
1377	2018-10-07 17:52:38	0	Location: res://ieframe.dll/ErrorPageTemplate.css Number of hits: 1 Cached file: MA7LM1OQ¥ErrorPageTemplate[1] Cached file size...
1378	2018-10-07 17:52:38	0	Location: res://ieframe.dll/errorPageStrings.js Number of hits: 1 Cached file: RYYA134L¥errorPageStrings[1] Cached file size: 2383

**FLAG**

<http://sc2018.attacker.com/gksoLx/FMfH.swf>