

MWS2012 ハンズオン インシデントレスポンス



2012/11/1

株式会社インターネットイニシアティブ
春山 敬宏、鈴木 博志

Ongoing Innovation

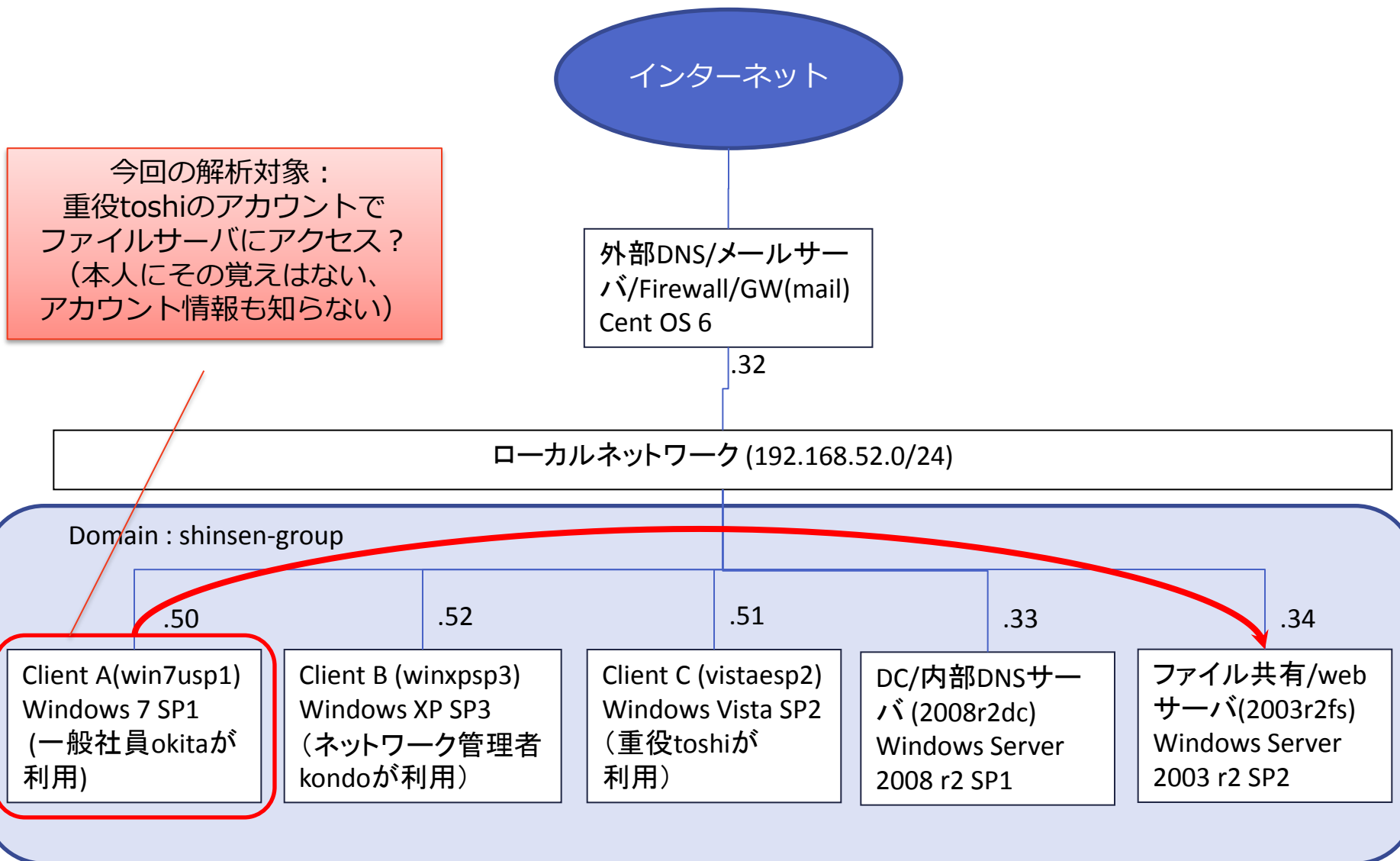
準備

- ハンズオンで使用するファイル群のコピー
 - USBメモリ内のmws2012フォルダをホストOSのC:¥にコピー
 - leaked_file
 - 漏洩したファイルを含む圧縮ファイル
 - WinHost
 - ホストOSで使用するデータ、ツール
 - WinVM
 - ゲストOS (Windows) で使用するデータ、ツール
 - Documents
 - ハンズオン資料、フォレンジック解析に関する解説文書
- ディスクイメージの展開
 - C:¥mws2012¥WinHost¥acquired_disk_image¥win7usp1.zip
 - ディスクイメージはハンズオンが終わったら削除してください

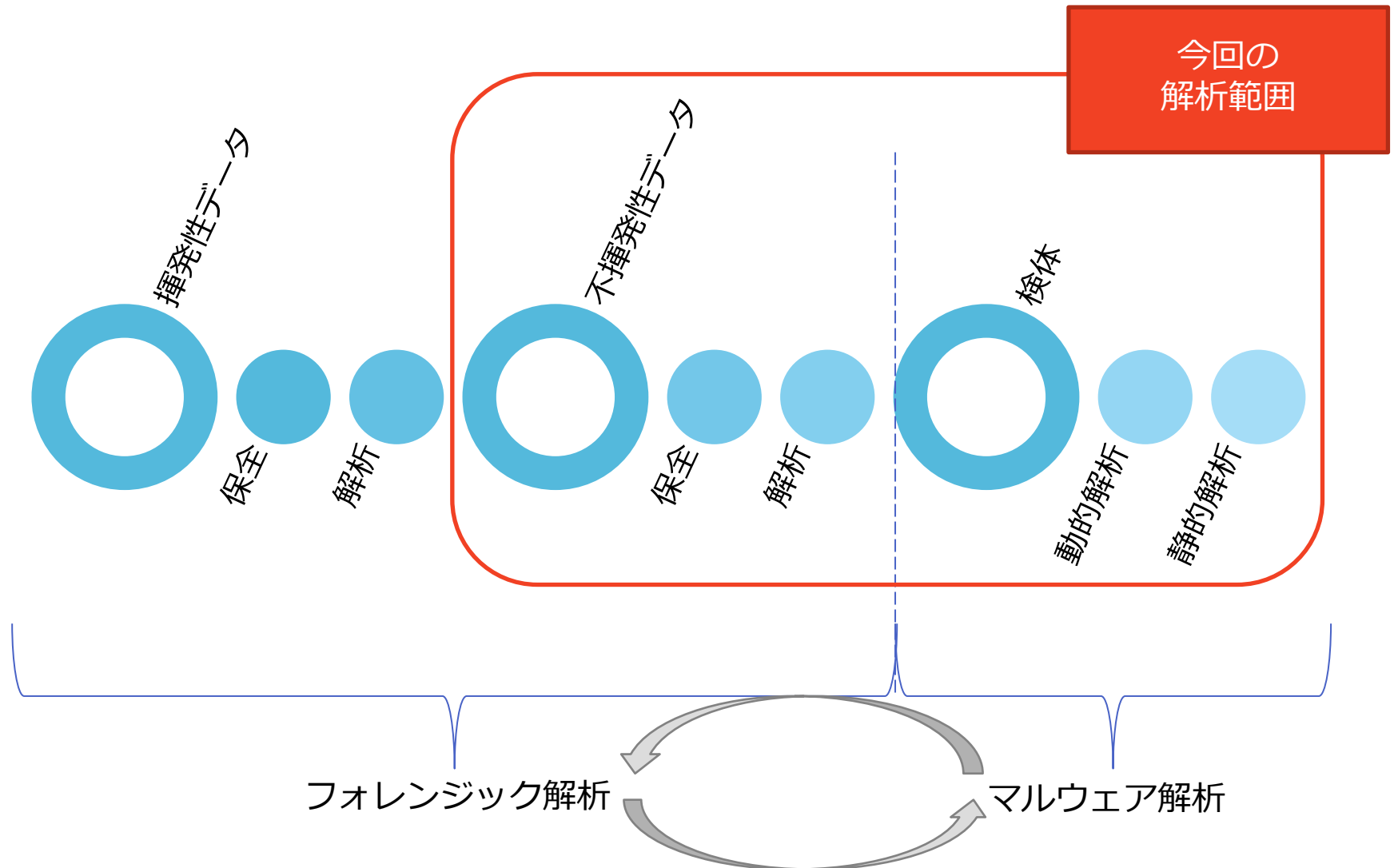
調査開始までのあらすじ

- あなたは某社でインシデントレスポンスを行うエンジニア
- あなたは顧客から「弊社の機密情報がインターネット上になぜか漏洩している。原因を調べてほしい」との依頼を受ける
- ヒアリングとファイルサーバのログ調査を行ったところ、不審な一台の端末が特定され、手始めにその端末を解析することになった

ネットワーク構成



インシデント対応における解析のフロー



本ケースの解析内容

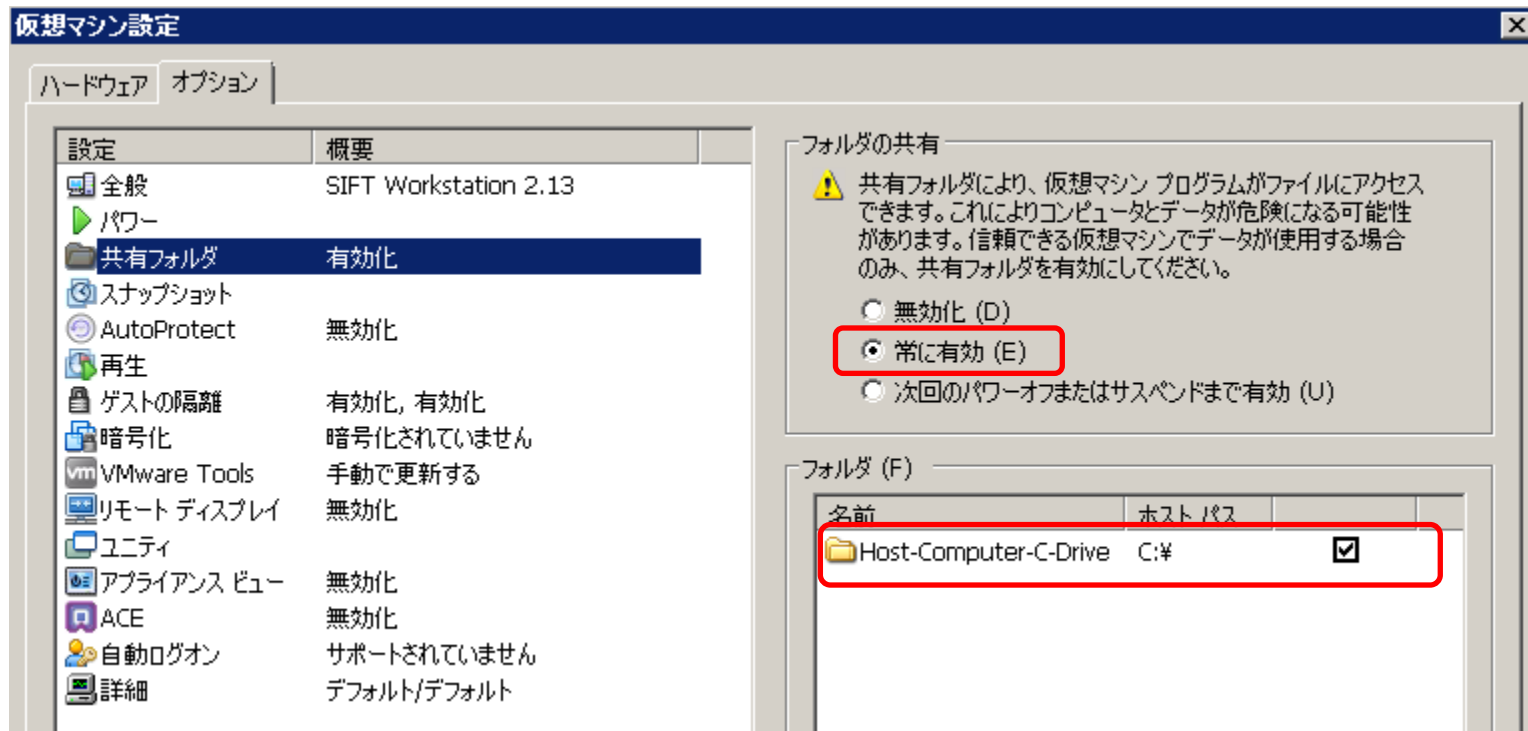
- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査 (ハンズオン#1)
 - マルウェアの登録時刻の特定
 - タイムラインの解析 (ハンズオン#2)
 - 悪性文書ファイルの解析 (ハンズオン#3)
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

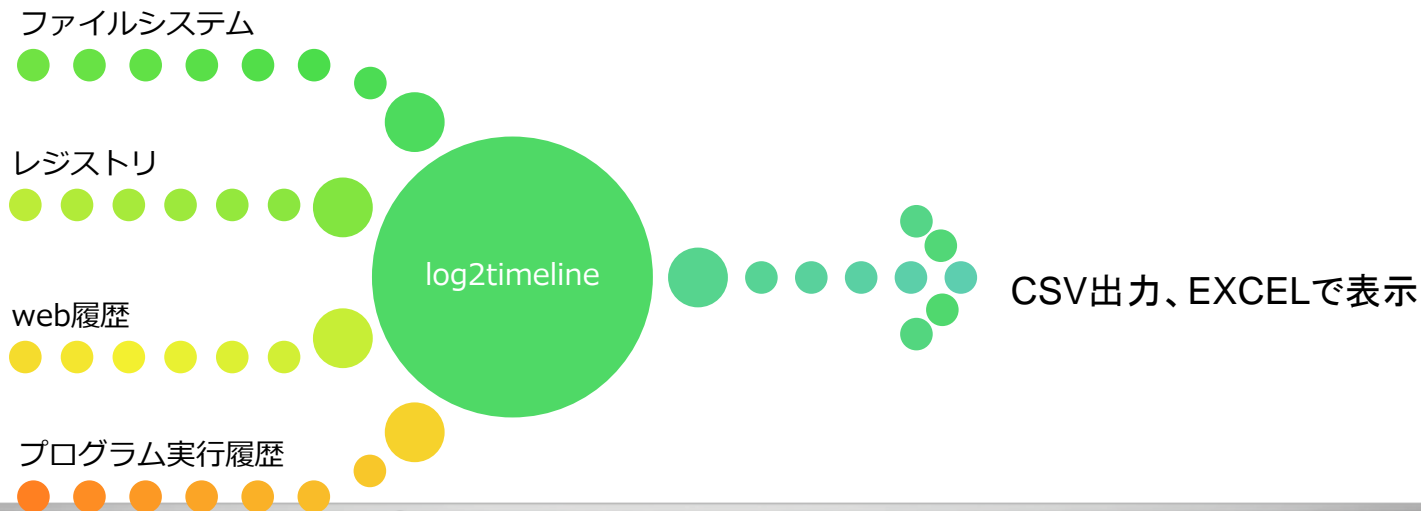
SIFTのVM設定、ログイン確認

- フォルダの共有設定
 - SIFTからホストのイメージファイルにアクセス可能にする
 - [VM] -> [設定]から[オプション]タブを選択
- ログインできることを確認
 - パワーオン、ID=sansforensics, password=forensicsでログイン
 - 使用しているVMWareが古くて起動しない場合は、以下の設定を参照
C:¥mws2012¥WinHost¥conf¥VMWare¥Workstation_SIFT_setting.txt



タイムラインの作成

- ファイルシステム・レジストリ等、様々なタイムスタンプを1つにまとめて表示
- マルウェアによる感染痕跡が残りやすい個所を調べて時刻を絞り込む
 - 事前にもらった情報（マルウェアのアクセス先URL等）があればそれを利用
- 絞り込んだ時刻の前後の活動を芋づる式に抽出していく
 - 前：感染原因
 - 後：マルウェアや攻撃者による活動



タイムラインの作成(Cont.)

- SIFTのlog2timeline-sift
 - 生成
 - log2timeline-sift -win7 -z Japan -i イメージファイルのパス
- ホストOS側と共有設定していれば、ホストOSのCドライブを/mnt/hgfsもしくはデスクトップから参照可能
- 詳しいコマンドオプションは以下を参照のこと
 - C:¥mws2012¥Documents¥log2timeline-cheatsheet.pdf

```
sansforensics@SIFT-Workstation:~$ log2timeline-sift -win7 -z Japan -i /mnt/hgfs/
Host-Computer-C-Drive/mws2012/WinHost/acquired_disk_image/win7usp1/win7usp1.raw
Image file (/mnt/hgfs/Host-Computer-C-Drive/mws2012/WinHost/acquired_disk_image/
win7usp1/win7usp1.raw) has not been mounted. Do you want me to mount it for you?
[y|n]: y
No partition nr. has been provided, attempting to print it out.
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

Slot	Start	End	Length	Description	
00:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
01:	-----	0000000000	0000002047	0000002048	Unallocated
02:	00:00	0000002048	0041940991	0041938944	NTFS (0x07)
03:	-----	0041940992	0041943039	0000002048	Unallocated

```
Which partion would you like to mount?: [1-3]: 2
sudo /bin/mount -o ro,loop,show,sys,files,streams,interface=windows,offset=10485
```

タイムラインの作成(Cont.)

- SIFTのlog2timeline-sift
 - 期間でフィルタリング
 - l2t_process -b /cases/timeline-output-folder/イメージファイル名_bodyfile.txt
開始日(..終了日) > 出力csvファイルのパス

```
sansforensics@SIFT-Workstation:~$ l2t_process -b /cases/timeline-output-folder/w  
in7usp1_bodyfile.txt 09-01-2012 > /cases/timeline-output-folder/20120901-win7usp  
1_bodyfile.csv  
There are 58 that fall outside the scope of the date range, yet show sign of pos  
sible timestomping.  
Would you like to include them in the output? [Y/n] Y  
  
Total number of events that fit into the filter (got printed) = 118949  
Total number of duplicate entries removed = 29853  
Total number of events skipped due to whitelisting = 0  
Total number of events skipped due to keyword filtering = 0  
Total number of processed entries = 477357  
Run time of the tool: 53 sec
```

タイムラインの作成(Cont.)

- SIFTのlog2timeline-sift
 - 抽出されたエントリのソースタイプを確認
 - `awk -F, '{print $6;}' /cases/timeline-output-f`
`older/tmp/win7usp1_bodyfile.csv | grep -v sourcetype | sort | uniq`
 - 処理の過程で抜け落ちるソースが存在
 - v2.13の場合、イベントログがタイムラインに含まれてこない

```
sansforensics@SIFT-Workstation:~$ awk -F, '{print $6;}' /cases/timeline-output-f
older/tmp/win7usp1_bodyfile.csv | grep -v sourcetype | sort | uniq
Application
Chrome History
Deleted Registry
EXIF metadata
FileExts key
Firefox Cache
Flash Cookie
Internet Explorer
Map Network Drive MRU key
Microsoft Windows Application Experience/Program Inventory
```

本ケースの解析内容

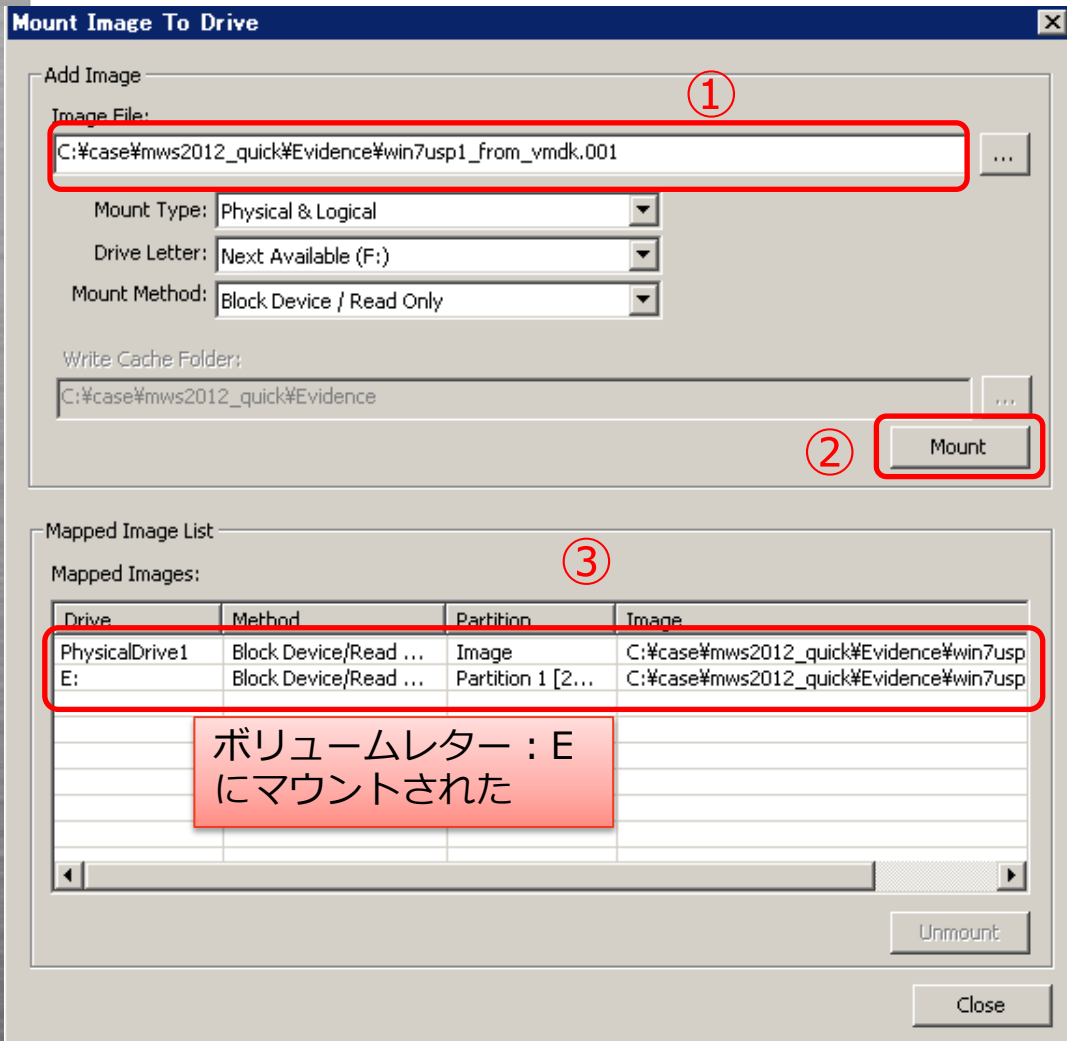
- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査 (ハンズオン#1)
 - マルウェアの登録時刻の特定
 - タイムラインの解析 (ハンズオン#2)
 - 悪性文書ファイルの解析 (ハンズオン#3)
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

自動起動設定プログラムの調査

- マルウェアはシステム起動時・ログイン時に自身を実行するための設定を登録することが多い
 - 感染時期や原因、マルウェアに関する情報等が事前に無い場合、まずは起動設定を調べる
- AutoRuns
 - レジストリやスタートアップ等、自動起動設定に関する情報を一括表示
 - 起動中のシステムだけでなく、オフラインのシステムボリュームの設定を表示することも可能
- FTK Imager
 - 保全したディスクイメージをマウント

ハンズオン#1:自動起動設定プログラムの調査

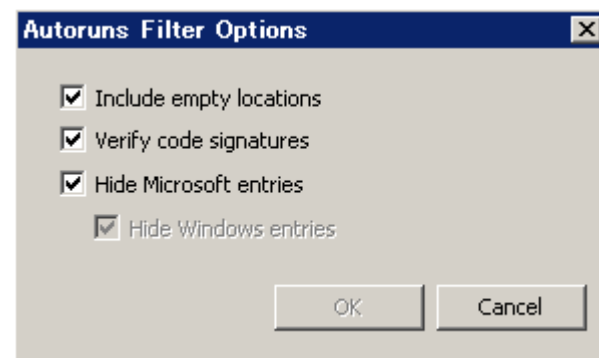
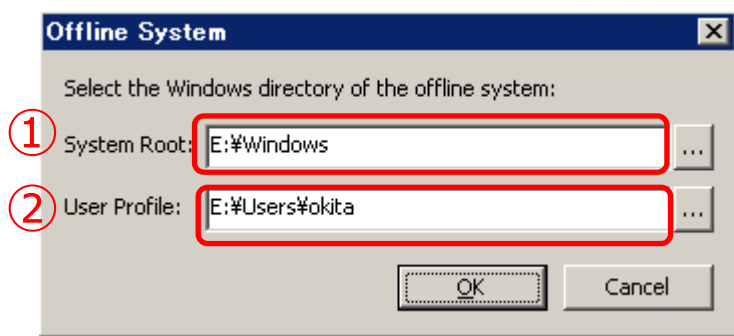
- FTK Imager
 - インストール
 - C:¥mws2012¥Win Host¥tools¥Access Data%20FTK%20Imager.exe
 - [File] -> [Image Mounting...]
 1. イメージファイルを指定
 2. マウント
 3. Mapped Imagesを確認
 - AutoRunsで指定すべきボリュームを判別



ハンズオン#1:自動起動設定プログラムの調査 (Cont.)

• AutoRuns

- "C:¥mws2012¥WinHost¥tools¥Autoruns.zip"を展開、autoruns.exeを管理者権限で実行
- [File] -> [Analyze Offline System...]
 1. System Rootに「レター番号:¥Windows」をセット
 2. User Profileに「レター番号:¥Users¥okita」をセット
- [Options] -> [Filter Options]でノイズを除去



HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run	
<input checked="" type="checkbox"/> WMI	c:¥users¥okita¥appdata¥roaming¥wmi.exe
<input checked="" type="checkbox"/> {4C7E21F6-4FB1-281B-7DEE-576EB386C91C}	c:¥users¥okita¥appdata¥roaming¥wmi.exe
HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce	

- ※ HKLM (Hive Key Local Machine): システムレジストリ
HKCU (Hive Key Current User): 指定したユーザプロファイルのレジストリ

本ケースの解析内容

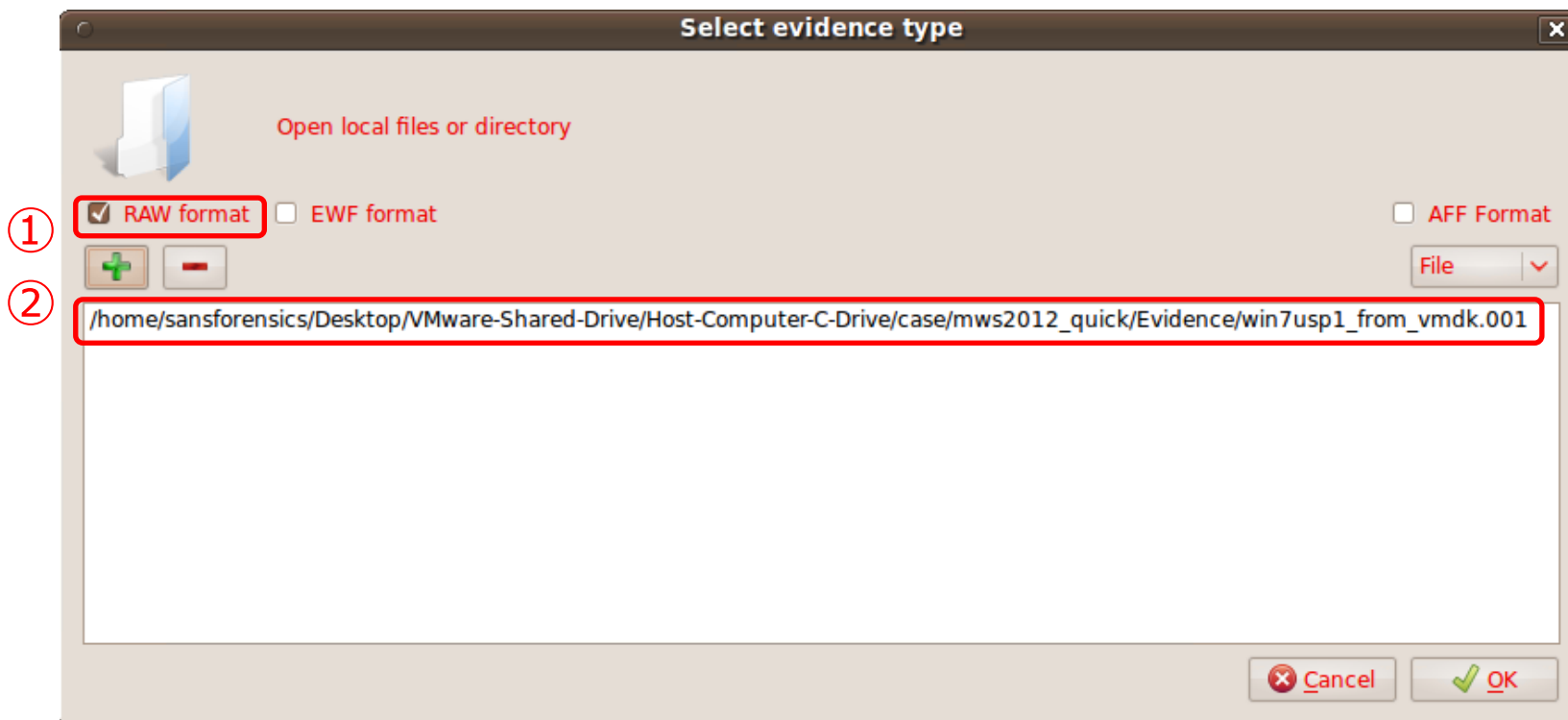
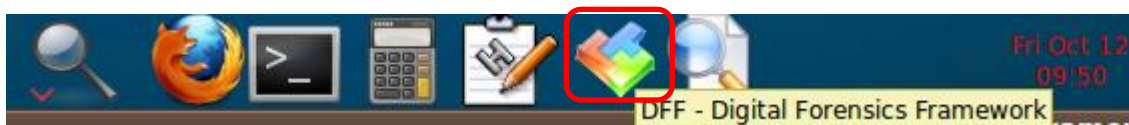
- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

マルウェアの登録時刻の特定

- レジストリキーには最終更新時刻の情報が含まれる
 - AutoRunsで発見した不審なエントリが追加された時刻を特定し、それ以前のタイムラインを遡っていく
- Registry Decoder
 - ディスクイメージ、レジストリファイルを解析してレジストリの情報を検索・表示
- Digital Forensic Framework
 - 削除・未使用領域を含めたファイルの検索、表示、抽出

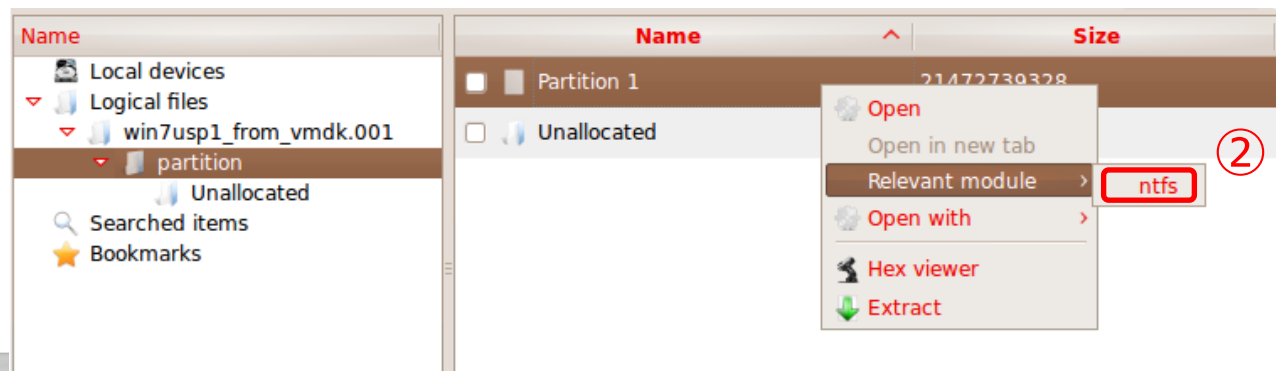
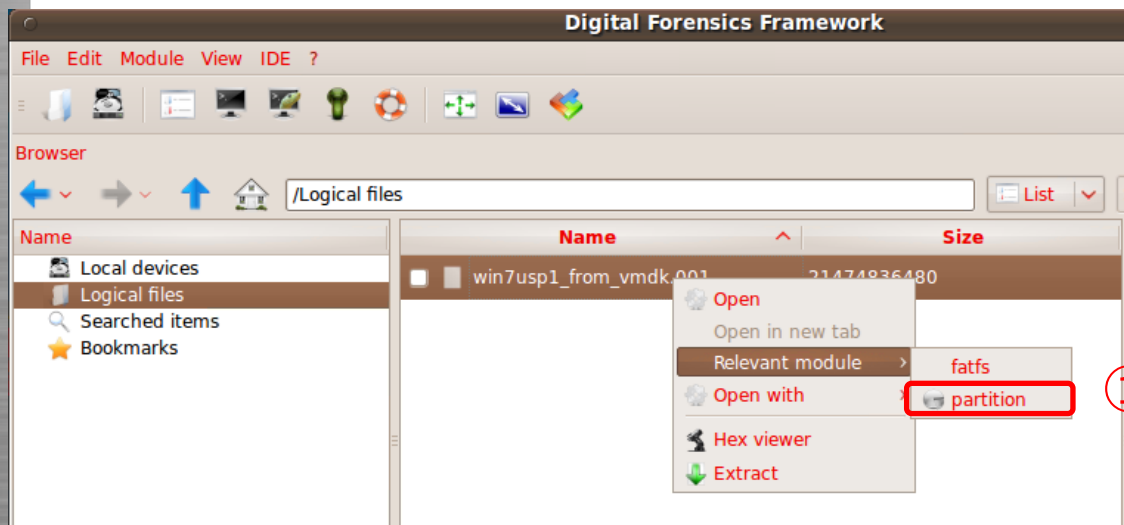
マルウェアの登録時刻の特定(Cont.)

- SIFTのDigital Forensic Framework
 - SIFT VMメニューバーのアイコンをクリック
 - [File] -> [Open evidence file(s)]
 - ①ファイルフォーマット、②読み込むイメージファイルを指定



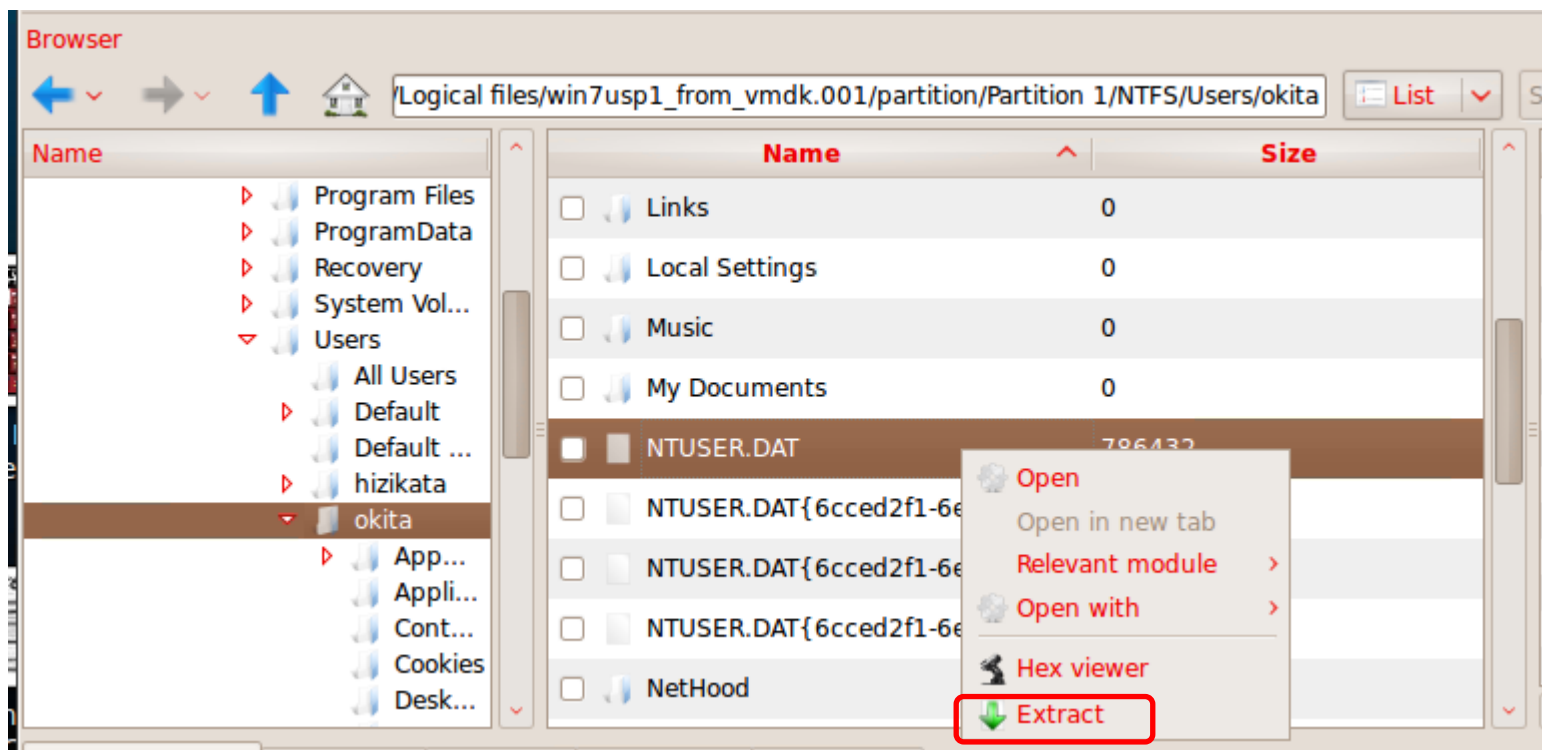
マルウェアの登録時刻の特定(Cont.)

- SIFTのDigital Forensic Framework
 - 対応するモジュールを指定してNTFSをパース
 - [Relevant module] -> ①partition, ②ntfs



マルウェアの登録時刻の特定(Cont.)

- SIFTのDigital Forensic Framework
 - 対象のレジストリファイルを抽出
 - 保存先はホストOSのファイルシステムのフォルダを指定



マルウェアの登録時刻の特定(Cont.)

- Registry Decoder
 - "C:¥mws2012¥WinHost¥tools¥regedcoderR103.zip"を展開、regdecoderR103.exeを実行
 - [Start a new case]を選択、Next
 - ケースの作成
 - Case Directoryは必ず空のフォルダを指定
 - レジストリファイルの追加
 - Add Evidenceで抽出したレジストリファイルを選択

ケースの作成

Case Name:

Case Number:

Investigator Name:

Comments:

Case Directory:

レジストリファイルの追加

Registry Decoder - Digital Forensics Solutions

File Reporting

	File Path	Alias (Optional)
1	C:¥case¥mws2012_quick¥Export¥NTUSER.DAT	

Registry Types (Disk Images Only): Current Backups (System Restore)

マルウェアの登録時刻の特定(Cont.)

- Registry Decoder
 - ブラウジング
 - [File View] タブでレジストリファイルを選択、[View] をクリック
 - [Browse] タブが開くので、注目しているレジストリパスをたどる

The screenshot shows the Registry Decoder interface. The left pane displays a tree view of the registry path: `C:\mws2012\WinHost\tools\regedecoderR103\NTUSER.DAT`. The right pane shows a table of registry values:

1	2	3
{4C7E21F6-4FB1-281B-7DEE-576EB386C91C}	REG_SZ	C:\Users\okita\AppData\Roaming\wmi.exe
WMI	REG_SZ	C:\Users\okita\AppData\Roaming\wmi.exe

A red box highlights the first two rows of the table. A red arrow points from a text box to the 'Last Modified' column of the registry tree, which shows the value: `4291-A7DC-7AED1C75B67C}\Software\Microsoft\Windows\CurrentVersion\Run -- 2012/10/05 18:48:30`.

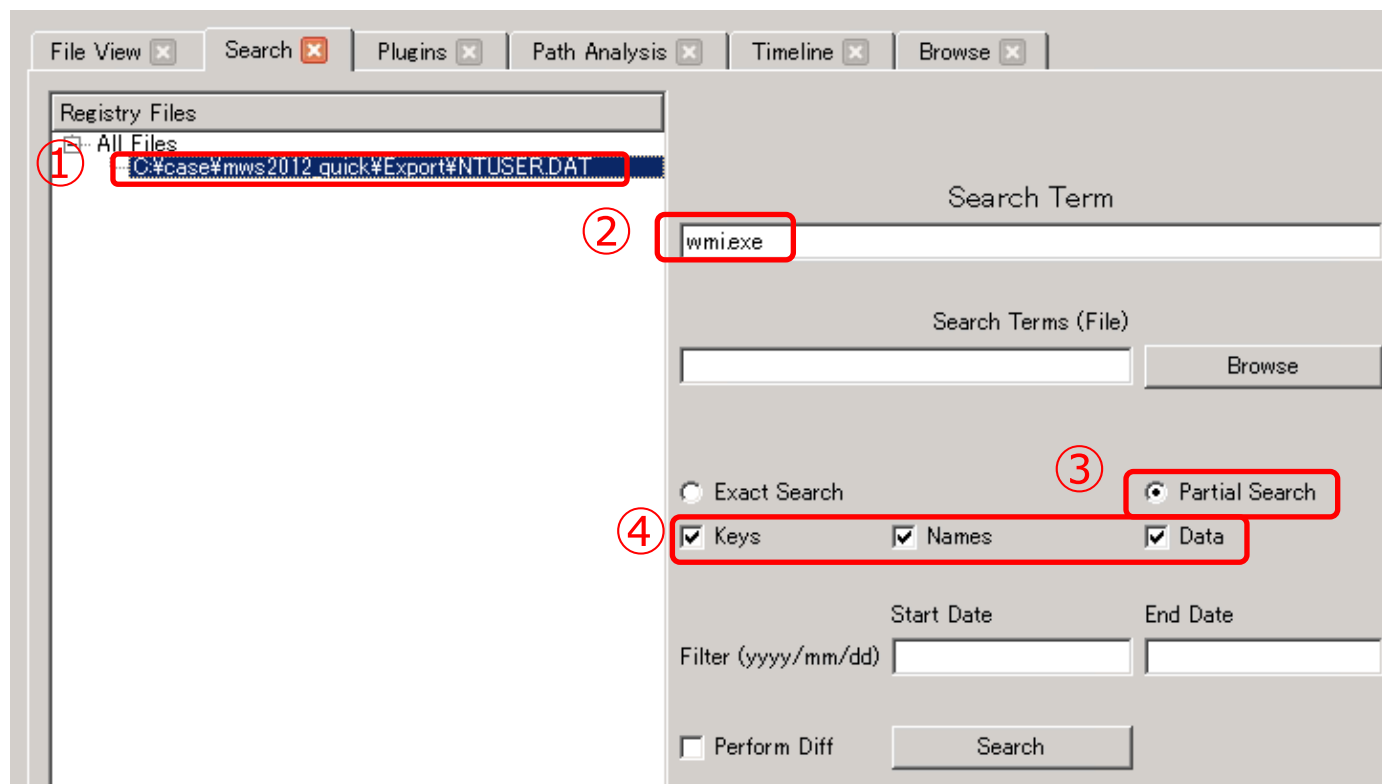
Runキーの最終更新時刻
(上書きされる可能性あり)

マルウェアの登録時刻の特定(Cont.)

- Registry Decoder

- 検索

1. [Search] タブで対象のレジストリファイルを選択
2. [Search Term] 内でキーワードを入力
3. [Partial Search] を選択
4. 検索対象を全てチェック



本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査 (ハンズオン#1)
 - マルウェアの登録時刻の特定
 - タイムラインの解析 (ハンズオン#2)
 - 悪性文書ファイルの解析 (ハンズオン#3)
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

タイムラインのチェック

- 感染原因に迫るアプローチ
 - 自動起動設定されているwmi.exeの様々なタイムスタンプを参照する

	Registry key	Filesystem	Prefetch	ShimCache
Description	last written time	MACB times	first & last run time	file modification time
Tool	log2timeline, Registry Decoder	log2timeline	Windows Prefetch Parser	ShimCache Parser
Risk	別のエントリによる上書き	マルウェアや攻撃者による変更	SSD/ESXiのイメージ	? (シャットダウンが必要)
Result	2012/10/5 18:48:30	2012/10/5 17:05:56	無	2012/10/5 17:05:56

ハンズオン#2:タイムラインのチェック

- log2timeline-siftが生成したCSVをチェック
 - C:\mws2012\WinHost\timeline\win7usp1-current\20120901-win7usp1-bodyfile.zipを展開、CSVをExcelでオープン
 - Officeが無い場合、SIFT内の表計算ソフトも利用可能

A, B, D, E, F, Mのカラムに
注目する

modification/last access/entry modified/creation

date	time	timezone	MACB	source	sourcetype	type	user
10/27/2006	9:49:52	Japan	M...	FILE	NTFS \$MFT	\$SI [M...] time	-

タイムスタンプの種類を表す

host	short	desc	VE
WIN7USP1	C:/Users/okita/AppData/Local/Temp/	C:/Users/okita/AppData/Roaming/Micr	

既に削除されているエントリの場合、
パスの後ろに(deleted)が入る

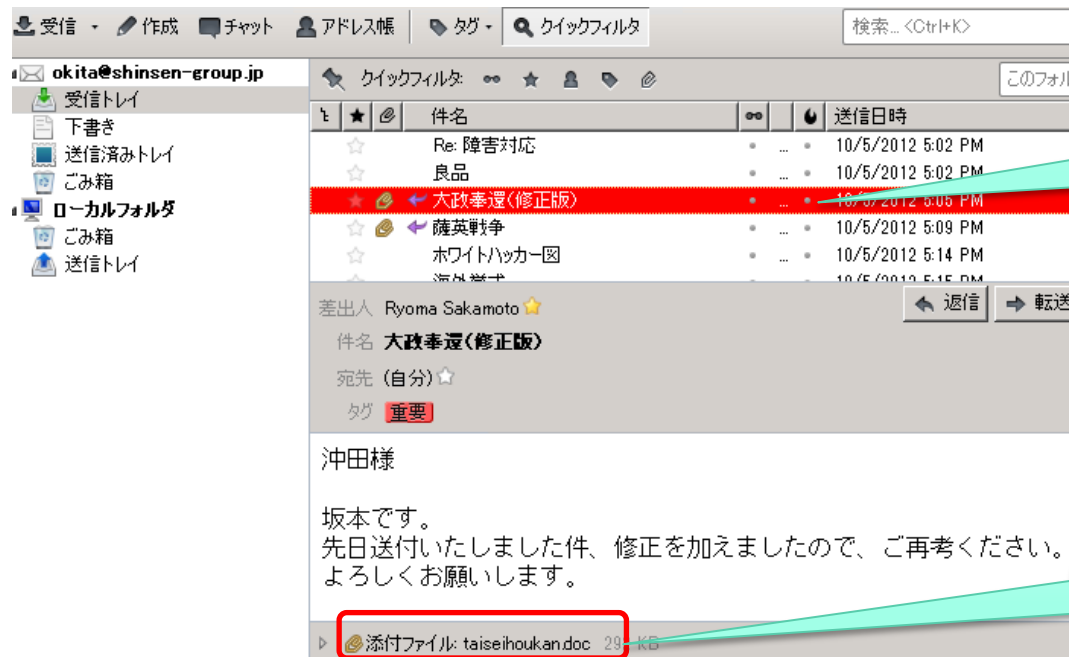
ハンズオン#2:タイムラインのチェック (Cont.)

- ShimCacheに残っていたファイルの更新時刻から、直前の活動を遡る
 - ファイルの生成
 - C:/Users/okita/AppData/Local/~EFGOI.tmp
 - デスクトップからWordファイルをオープン
 - taiseihoukan.doc
 - Flashオブジェクトを含む?
- 以下の疑問について確認していく
 - 「~EFGOI.tmp」とは何か?
 - 「taiseihoukan.doc」はどこから来たファイルか? (e.g., web or mail)

Time	Date	Location	Account	File Name	File Type	File Size	File Path	File Action
10/05/2012	17:05:03	Japan	.A.B	FILE	NTFS \$MFT	\$SI [A.B] time	C:/Users/okita/Desktop/taiseihoukan.doc	WIN7USP1 visited file:///C:/User...
10/05/2012	17:05:03	Japan	.ACB	WEBHIST	Internet Explo	Last Visited	okita	WIN7USP1 visited file:///C:/User...
10/05/2012	17:05:06	Japan	M..	FILE	NTFS \$MFT	\$SI [M..] time	C:/Users/okita/Desktop/taiseihoukan.doc	WIN7USP1 C:/Users/okita/Desktop/taiseihoukan.doc
10/05/2012	17:05:33	Japan	MAC.	FILE	NTFS \$MFT	\$SI [MAC.] time	C:/Users/okita/AppData/Roaming/Microsoft/Templates	WIN7USP1 C:/Users/okita/AppData/Roaming/Microsoft/Templates
10/05/2012	17:05:33	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/AppData/Roaming/Microsoft/Templates/~\$Normal.dotm	WIN7USP1 C:/Users/okita/AppData/Roaming/Microsoft/Templates/~\$Normal.dotm
10/05/2012	17:05:33	Japan	.A.B	FILE	NTFS \$MFT	\$SI [A.B] time	C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C	WIN7USP1 C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C
10/05/2012	17:05:35	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/Desktop/taiseihoukan.doc	WIN7USP1 C:/Users/okita/Desktop/taiseihoukan.doc
10/05/2012	17:05:35	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/Desktop/taiseihoukan.doc	WIN7USP1 C:/Users/okita/Desktop/taiseihoukan.doc
10/05/2012	17:05:36	Japan	.A.B	FILE	NTFS \$MFT	\$SI [A.B] time	C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C	WIN7USP1 C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C
10/05/2012	17:05:37	Japan	.C.	FILE	NTFS \$MFT	\$SI [.C.] time	C:/Users/okita/Desktop/taiseihoukan.doc	WIN7USP1 C:/Users/okita/Desktop/taiseihoukan.doc
10/05/2012	17:05:37	Japan	..B	FILE	NTFS \$MFT	\$SI [..B] time	C:/Users/okita/Office/Recent/taiseihoukan.LNK	WIN7USP1 C:/Users/okita/Office/Recent/taiseihoukan.LNK
10/05/2012	17:05:38	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/AppData/Local/Temp/Word8.0	WIN7USP1 C:/Users/okita/AppData/Local/Temp/Word8.0
10/05/2012	17:05:38	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/AppData/Local/Temp/Word8.0/ShockwaveFlashObjects.exe	WIN7USP1 C:/Users/okita/AppData/Local/Temp/Word8.0/ShockwaveFlashObjects.exe
10/05/2012	17:05:38	Japan	M.C.	FILE	NTFS \$MFT	\$SI [M.C.] time	C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C	WIN7USP1 C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C
10/05/2012	17:05:39	Japan	MACB	EVTX	System	Event Logged	win7usp1.s Event ID System/Service Control Manager ID [7036] :EventData/Data -> param1 = Diagr	win7usp1.s Event ID System/Service Control Manager ID [7036] :EventData/Data -> param1 = Diagr
10/05/2012	17:05:50	Japan	MACB	EVTX	Security	Event Logged	win7usp1.s Event ID Security/Microsoft-Windows-Security-Auditing ID [4672] :EventData/Data -> S	win7usp1.s Event ID Security/Microsoft-Windows-Security-Auditing ID [4672] :EventData/Data -> S
10/05/2012	17:05:50	Japan	MACB	EVTX	Security	Event Logged	win7usp1.s Event ID Security/Microsoft-Windows-Security-Auditing ID [4624] :EventData/Data -> S	win7usp1.s Event ID Security/Microsoft-Windows-Security-Auditing ID [4624] :EventData/Data -> S
10/05/2012	17:05:52	Japan	MACB	EVTX	System	Event Logged	win7usp1.s Event ID System/Service Control Manager ID [7036] :EventData/Data -> param1 = Wind	win7usp1.s Event ID System/Service Control Manager ID [7036] :EventData/Data -> param1 = Wind
10/05/2012	17:05:55	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/AppData/Local/~EFGOI.tmp	WIN7USP1 C:/Users/okita/AppData/Local/~EFGOI.tmp
10/05/2012	17:05:56	Japan	MACB	FILE	NTFS \$MFT	\$SI [MACB] tin	C:/Users/okita/AppData/Local/taiseihoukan.doc	WIN7USP1 C:/Users/okita/AppData/Local/taiseihoukan.doc
10/05/2012	17:05:56	Japan	.A.	LNK	Shortcut	LNK Access	C:/Users/okita/AppData/Local/taiseihoukan.doc <-//mnt/windows_mount/User	WIN7USP1 C:/Users/okita/AppData/Local/taiseihoukan.doc <-//mnt/windows_mount/User

ファイルの内容や由来に関する調査

- 「~EFGOI.tmp」とは何か？
 - Digital Forensic Frameworkを用いたハッシュ値の照合
 - “~EFGOI.tmp”と“wmi.exe”は同一のファイル
- 「taiseihoukan.doc」はどこから来たファイルか？
 - web履歴（explorerによるファイルアクセスも残る）
 - Web Historian
 - writableで再マウント、ホームフォルダにアクセスしてアクセス権限を取得
 - メールの調査
 - Thunderbirdのメールフォルダを抽出、VM上にセットアップしたThunderbirdに読み込み
 - Users/okita/AppData/Roaming/Thunderbird/Profiles/*.default/Mail



2012/10/5
17:05:10送信の
「大政奉還(修正版)」

”taiseihoukan.doc”
が添付されている

ユーザ活動の調査

- ユーザが実行したGUIプログラムの調査
 - ユーザレジストリのUserAssistキー（実行回数、最後に実行された時刻）
 - Registry DecoderのUser Assistプラグイン
- ファイルのオープンに関する調査
 - Officeの最近開いたファイル
 - C:¥Users¥<user>¥AppData¥Roaming¥Microsoft¥Office¥Recent¥
 - JumpList
 - C:¥Users¥user¥AppData¥Roaming¥Microsoft¥Windows¥Recent
 - JumpLister
 - ユーザレジストリ
 - Shell Bag, RecentDocs, etc..
 - Registry Decoderの各プラグイン（Searchも有効）

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査 (ハンズオン#1)
 - マルウェアの登録時刻の特定
 - タイムラインの解析 (ハンズオン#2)
 - 悪性文書ファイルの解析 (ハンズオン#3)
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

Officeドキュメントの解析

- embeddedなコード・ファイルの確認
 - 文字列検索
 - Flash/JavaScript/ActiveXコンポーネント (ScriptBridge), etc..
 - 文字列抽出ツール、バイナリエディタを使う
 - e.g., BinText
 - OLE構造をパースして確認
 - FileInsight
 - Pyew/hachoir-subfile (REMnuxに収録)
- スキャン
 - OfficeMalScanner
 - 実行ファイル・シェルコード、swfの抽出

Officeドキュメントの解析(Cont.)

- FileInsight
 - VM内の
"C:¥mws2012¥WinVM¥tools¥fileinsight.exe"を実行してインストール
 - taiseihoukan.docを読み込んで中身を確認

The screenshot displays the FileInsight interface for the file 'taiseihoukan.doc'. The left-hand 'Navigation' pane shows a tree structure of the document's internal components, with 'Contents' (202740) selected. The main window shows a hex dump of the file's data. A red box highlights the signature 'Flashファイルのシグネチャ' (Flash file signature), which is located in the hex dump at offset 00003600. The signature is '66 55 66 55 A8 16 03 00 46 57 53 0D AD D6 00 00 fUfU... FWS...'. A red arrow points from the text box to the 'FWS.' signature in the hex dump.

Officeドキュメントの解析(Cont.)

- OfficeMalScanner
 - VM内の"C:¥mws2012¥WinVM¥tools¥OfficeMalScanner.zip"を展開
 - OfficeMalScanner.exeのscanコマンドを実行
 - 実行ファイルやシェルコードのパターンを検索・抽出
 - bruteオプションでone-byte XORを試行
 - Flashファイルの抽出も可能

```
C:¥work¥tools¥OfficeMalScanner>OfficeMalScanner C:¥work¥malwares¥cve-2012-1535_m
odified_20120914¥cve-2012-1535_modified¥mws¥final¥taiseihoukan.doc scan

-----+
|           OfficeMalScanner v0.55           |
| Frank Boldwin / www.reconstructor.org     |
|-----+-----|

[*] SCAN mode selected
[*] Opening file C:¥work¥malwares¥cve-2012-1535_modified_20120914¥cve-2012-1535_
modified¥mws¥final¥taiseihoukan.doc
[*] Filesize is 298496 (0x48e00) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Format type Winword
[*] Scanning now...

Embedded Flash signature found at offset: 0x3608

Flash Header Information:
-----+-----
File is uncompressed
File version: 13
File size: 54957 bytes

Dumping flash file as filename: taiseihoukan__FLASHFILE__OFFSET=0x3608.swf

Analysis finished!
```


Flashの簡易解析(Cont.)

- PDF Stream Dumper
 - VM内の"C:¥mws2012¥WinVM¥tools¥PDFStreamDumper_Setup.exe"を実行してインストール
 - [Tools] -> [Decompile Flash w/ AS3 Sourcerer]
 - 評価版なので文字列コピー等の操作は不可
- 特徴的な文字列をwebで検索
 - "Main_FontClass"、シエルコードの文字列
 - CVE-2012-1535 ?

```
53         _local4 = (_local4 + (_local5.height + 2));
54         addChild(_local5);
55         _local5 = _arg1.createTextLine(_local5, _local2);
56     };
57 }
58
59 public function heapSpray():void
60 {
61     var _local1:uint;
62     _local1 = 0;
63     this.kbArray = new ByteArray();
64     this.kbArray.endian = Endian.LITTLE_ENDIAN;
65     var _local2:* = "0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c909090";
66     var _local3:* = (_local2 + "9090909090E947010000C28F36D8A0DF16D5B5F0");
67     var _local4:String = _local3;
68     var _local5:ByteArray = this.hexToBin(_local4);
69     var _local6:uint = (_local4.length / 2);
70     _local1 = 0;
71     while (_local1 < 0x0400)
```

悪性文書ファイルの動的解析

- CVE-2012-1535
 - Adobe Flash Player 11.3.300.270 およびそれ以前のバージョンが対象
 - 感染端末のFlashのバージョンを調べる
 - SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Adobe Flash Player ActiveX
 - DisplayVersion = 11.2.202.233
- 動的解析
 - 同じバージョンのFlashをインストールしたWindows VM上で対象ドキュメントを開いて挙動を観察する
 - ファイル入出力、プロセスの動作解析
 - Process Hacker/Process Explorer
 - CaptureBAT
 - エミュレーションサーバ
 - FakeNet
 - レジストリ、ファイルシステム差分取得
 - regshot
 - Windows VMにOfficeをインストールしていない場合は、wmi.exeを代わりに実行する

Windows VMの設定

- VMWare Toolsをインストールしていない場合は入れておく
- マルウェアを実行するので以下の設定を行う
 - ネットワークの設定をホストオンリーに
 - 実行前の状態に戻せるようにしておく
 - VMWare Workstationの場合、スナップショットを作成
 - [VM] -> [スナップショット] -> [スナップショットの作成]
 - VMWare Playerの場合、VM停止後に変更を破棄できるように設定を編集
 - C:¥mws2012¥WinHost¥conf¥VMWare¥Player_Win_setting.txt
- パワーオン、ログイン
- ホストOSの"C:¥mws2012¥WinVM"をWindows VM内のC:¥mws2012にコピー

仮想マシン設定

ハードウェア オプション

デバイス	概要
メモリ	1024 MB
プロセッサ	1
ハード ディスク(SCSI)	20 GB
CD/DVD(IDE)	自動検出
フロッピー	自動検出
ネットワーク アダプタ	ホストオンリー
USB コントローラ	存在します
サウンド カード	自動検出
プリンタ	存在します
シリアル ポート 2	名前付きパイプ ¥#.¥pipe¥com_1 の使用
ディスプレイ	自動検出

デバイスのステータス

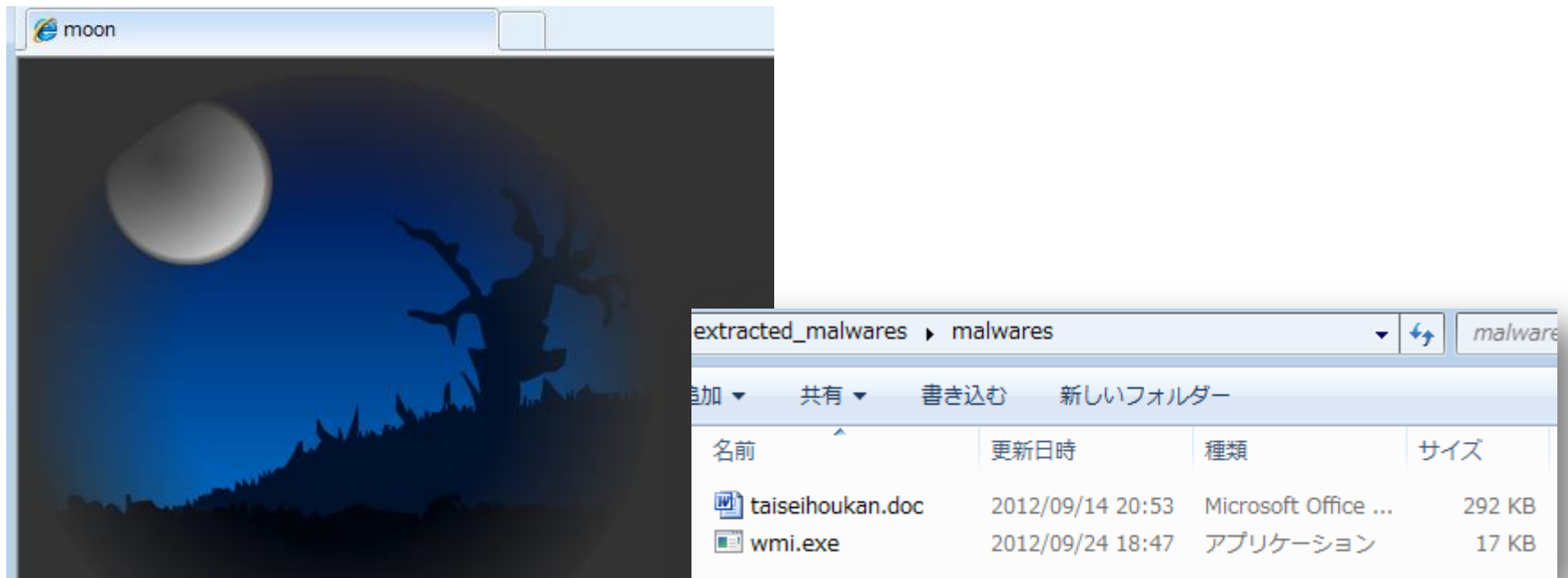
- 接続済み (C)
- 起動時に接続 (O)

ネットワーク接続

- ブリッジ: 物理ネットワークに直接接続 (B)
- 物理ネットワーク接続の状態を複製 (P)
- NAT: ホストの IP アドレスを共有して使用 (N)
- ホストオンリー: プライベートネットワークをホストと共有 (H)
- カスタム: 特定の仮想ネットワーク (S)

ハンズオン#3: 悪性文書ファイルの動的解析

- VM内環境の準備
 - Flashのインストール
 - "C:¥mws2012¥WinVM¥tools¥flashplayer11_2r202_233_winax_32bit.exe"の実行
 - 動作確認
 - テスト用のコンテンツにIEでアクセス
 - "C:¥mws2012¥WinVM¥tools¥flash_IE_test_page¥moon.html"
 - "C:¥mws2012¥WinVM¥extracted_malwares¥malwares.zip"を展開
 - パスワード : infected



ハンズオン#3:

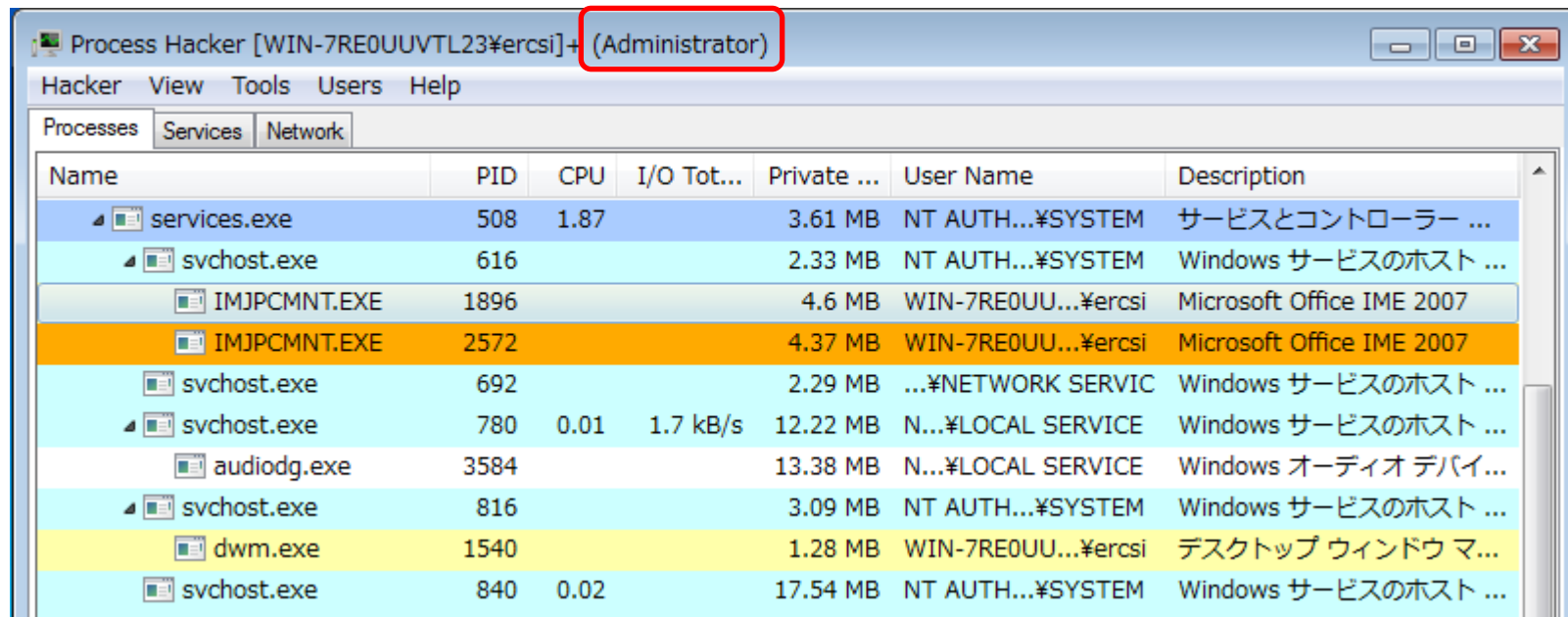
悪性文書ファイルの動的解析

- CaptureBATのインストール
 - “C:¥mws2012¥WinVM¥tools¥CaptureBAT¥CaptureBAT.exe”を実行してインストール
 - インストールに失敗する場合、“Visual C++2005 Redistrib Package.exe”を実行
 - インストール後、再起動が必要

ハンズオン#3:

悪性文書ファイルの動的解析

- Process Hacker
 - "C:¥mws2012¥WinVM¥tools¥processhacker-2.28-bin.zip"を展開、x86¥ProcessHacker.exeを管理者権限で起動
 - プロセス、サービス、ネットワーク情報等を表示



Name	PID	CPU	I/O Tot...	Private ...	User Name	Description
services.exe	508	1.87		3.61 MB	NT AUTH...¥SYSTEM	サービスとコントローラー ...
svchost.exe	616			2.33 MB	NT AUTH...¥SYSTEM	Windows サービスのホスト ...
IMJPCMNT.EXE	1896			4.6 MB	WIN-7RE0UU...¥ercsi	Microsoft Office IME 2007
IMJPCMNT.EXE	2572			4.37 MB	WIN-7RE0UU...¥ercsi	Microsoft Office IME 2007
svchost.exe	692			2.29 MB	...¥NETWORK SERVIC	Windows サービスのホスト ...
svchost.exe	780	0.01	1.7 kB/s	12.22 MB	N...¥LOCAL SERVICE	Windows サービスのホスト ...
audiodg.exe	3584			13.38 MB	N...¥LOCAL SERVICE	Windows オーディオ デバイ...
svchost.exe	816			3.09 MB	NT AUTH...¥SYSTEM	Windows サービスのホスト ...
dwm.exe	1540			1.28 MB	WIN-7RE0UU...¥ercsi	デスクトップ ウィンドウ マ...
svchost.exe	840	0.02		17.54 MB	NT AUTH...¥SYSTEM	Windows サービスのホスト ...

ハンズオン#3:

悪性文書ファイルの動的解析

- FakeNet
 - ファイアウォール設定の無効化
 - “C:¥mws2012¥WinVM¥tools¥Fakenet1.0c.zip”を展開、管理者権限のコマンドプロンプトから起動
 - nslookupコマンドでlocalhostに向くことを確認



```
管理者: コマンド プロンプト - fakenet
C:¥mws¥tools¥windows_VM¥Fakenet1.0c¥Fakenet1.0b>fakenet
FakeNet Version 1.0
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Scanning Installed Providers
Installing Layered Providers
Preparing To Reorder Installed Chains
Reordering Installed Chains
Saving New Protocol Order
[Listening for DNS traffic on port: 53.]
[Listening for traffic on port 80.]
[Listening for SSL traffic on port 443.]
[Listening for SSL traffic on port 8443.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 31337.]
[Listening for ICMP traffic.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
```

ハンズオン#3: 悪性文書ファイルの動的解析

- CaptureBATの実行
 - 管理者権限のコマンドプロンプトから起動
 - 出力をリダイレクトして保存
 - -c: 変更もしくは削除されたファイルをキャプチャ
 - -n: ネットワークパケットをキャプチャ
 - 起動後、サービスがインストールされることを確認

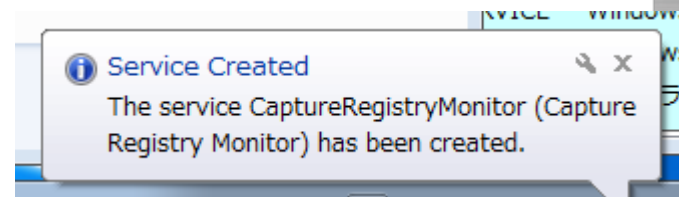
```
管理: コマンドプロンプト - CaptureBAT.exe -c
le or outputted to stdout.

Usage: CaptureClient.exe [-chn] [-s server address -a vm server id -b vm id] [-l
file]

-h          Print this help message
-s address  Address of the server the client connects up to. NOTE -a & -b
            must be defined when using this option
-a server id Unique id of the virtual machine server that hosts the client
-b vm id    Unique id of the virtual machine that this client is run on
-l file     Output system events to a file rather than stdout

-c          Copy files into the log directory when they are modified or
            deleted
-n          Capture all incoming and outgoing network packets from the
            network adapters on the system and store them in .pcap files in
            the log directory

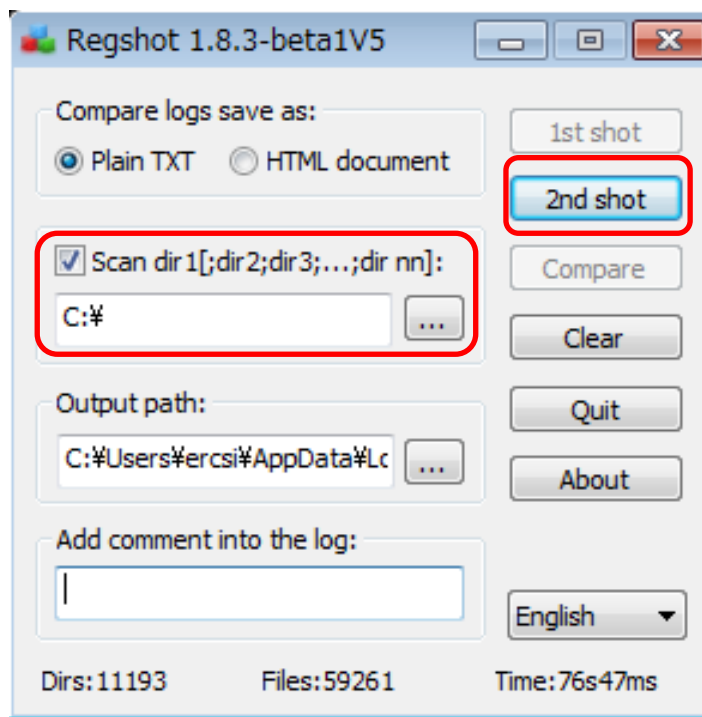
If -s is not set the client will operate in standalone mode
C:\Program Files\Capture>CaptureBAT.exe -c > malware.log
```



ハンズオン#3:

悪性文書ファイルの動的解析

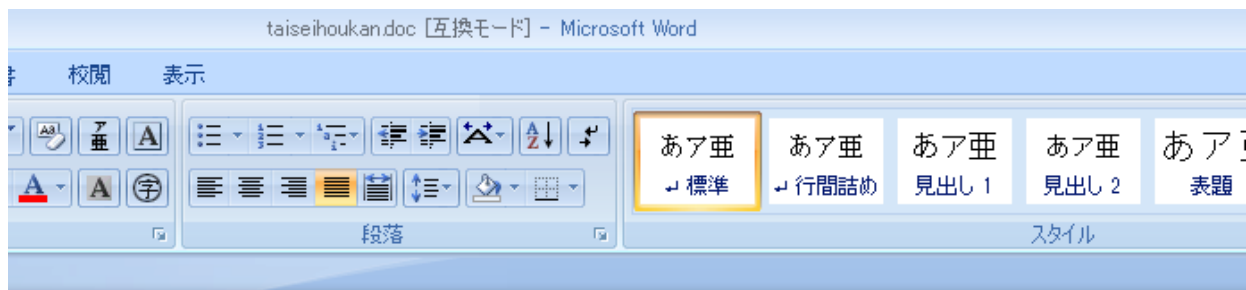
- regshot
 - 管理者権限で起動
 - "C:¥mws2012¥WinVM¥tools¥v5_regshot_1.8.3_beta1_win32_x64_src_bin_v5¥regshot.exe"
 - [Scan dir1...]をチェック、対象ディレクトリはC:¥
 - [1st shot] -> [shot]をクリック
 - [2nd shot]が有効になっていることを確認



ハンズオン#3:

悪性文書ファイルの動的解析

- 悪性ドキュメントのオープン
 - "C:¥mws2012¥WinVM¥extracted_malwares¥malwares.zip"展開後の taiseihoukan.docをオープン
 - VM内にOffice環境が無い場合、ドロップされたマルウェア(wmi.exe)を実行してください
- exploitが成功すると、ダミードキュメントが開く



江戸時代、徳川将軍は日本の統治者として君臨していたが、形式的には朝廷より将軍宣下があり、幕府が政治の大権を天皇から預かっているという大政委任論も広く受け入れられていた。幕末、朝廷が自立的な政治勢力として急浮上し、主に対外問題における幕府との不一致により幕府権力の正統性が脅かされる中で、幕府は朝廷に対し大政委任の再確認を

ハンズオン#3:

悪性文書ファイルの動的解析

- ツールの終了、結果の確認
 - regshot (今回は未実施)
 - [2nd shot] -> [Compare]
 - 実行ファイルのインストール、レジストリ登録を確認
 - CaptureBAT
 - 適当にキーを押す
 - regshotの差分では把握できない詳細部分や削除ファイルの実体を参照
 - FakeNet
 - Ctrl-Cを押す
 - www.fewjriehgusuoh.comを名前解決、ポート80番にプロトコル不明な通信

regshot

```

C:\Users\ercsi\AppData\Local#\$.iseihoukan.doc
C:\Users\ercsi\AppData\Local\EFGOI.tmp
C:\Users\ercsi\AppData\Roaming\Microsoft\Office\Recent
C:\Users\ercsi\AppData\Roaming\Microsoft\Office\Recent
C:\Users\ercsi\AppData\Roaming\Microsoft\Office\Recent
C:\Users\ercsi\AppData\Roaming\Microsoft\Templates\$.N
C:\Users\ercsi\AppData\Roaming\Microsoft\Windows\Recen
C:\Users\ercsi\AppData\Roaming\Microsoft\Windows\Recen
C:\Users\ercsi\AppData\Roaming\Microsoft\Windows\Recen
C:\Users\ercsi\AppData\Roaming\wmi.exe
  
```

fakenet

```

[DNS Query Received.]
Domain name: www.fewjriehgusuoh.com
[DNS Response sent.]
  
```

```

[Received new connection on port: 80.]
[New request on port 80.]
[Received unsupported HTTP request.]
  
```

CaptureBAT

```

title: CaptureBAT.exe / C:\Program Files\Capture\malware.log
file: write C:\Program Files\Microsoft Office\Office12\WINWORD.EXE -> C:\Users\ercsi\AppData\Local\EFGOI.tmp
process: created C:\Program Files\Microsoft Office\Office12\WINWORD.EXE -> C:\Users\ercsi\AppData\Local\EFGOI.tmp
file: Write C:\Program Files\Microsoft Office\Office12\WINWORD.EXE -> C:\Users\ercsi\AppData\Local\EFGOI.tmp
file: Write C:\Windows\explorer.exe -> C:\Users\ercsi\AppData\Roaming\wmi.exe
registry: SetValueKey C:\Windows\explorer.exe -> HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{4C7E21F6-4FB1-281B-7DEE-57
registry: SetValueKey C:\Windows\explorer.exe -> HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WMI
registry: DeleteValueKey C:\Windows\System32\taskhost.exe -> HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
process: terminated C:\Program Files\Microsoft Office\Office12\WINWORD.EXE -> C:\Users\ercsi\AppData\Local\EFGOI.tmp
  
```

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

シェルコードの解析

- 補足：exploit後の動作をコードレベルで確認したい場合
 - デコンパイルしたコード or p-codeを読んでシェルコードを特定
 - swfファイルからシェルコードを抽出する
 - バイナリエディタ
 - シェルコードのエミュレーション（呼び出すAPIをチェック）
 - e.g., libemu
 - ただし、このシェルコードには効果がない
 - シェルコードのデバッグ
 - デバッガにbinary paste もしくは ランチャーを使う
 - <http://practicalmalwareanalysis.com/labs/>
 - シェルコードの静的解析
 - IDA Pro

```

push    ecx
push    [ebp+sc.field_113_hFile_exp_doc]
call    [ebp+sc.field_8_kernel32_GetFileSize]
cmp     eax, [ebp+sc.field_12F_word_doc_size]
jnz     short loc_1E2
push    ebp
push    0
push    80h ; 'I'
push    2
push    0
push    1
push    GENERIC_WRITE
lea     eax, [ebp+sc.field_34_aWordl_tmp]
push    eax
add     [ebp+sc.field_4_kernel32_CreateFileA], 5
jmp     short loc_224 ; opening C:\WINDOWS\WORDL.tmp

```


実行されたマルウェアの特定

- 動的解析でキャプチャした通信の特徴
 - Wireshark
 - TCP80番宛に **ランダムな256bytes**の通信
- PoisonIvy?
 - Camellia Encryption
 - 最初にチャレンジレスポンスのネゴシエーションを行う
 - <https://media.blackhat.com/bh-eu-10/presentations/Dereszowski/BlackHat-EU-2010-Dereszowski-Targeted-Attacks-slides.pdf>
 - <http://labs.alienvault.com/labs/index.php/category/blog/page/3/>

```

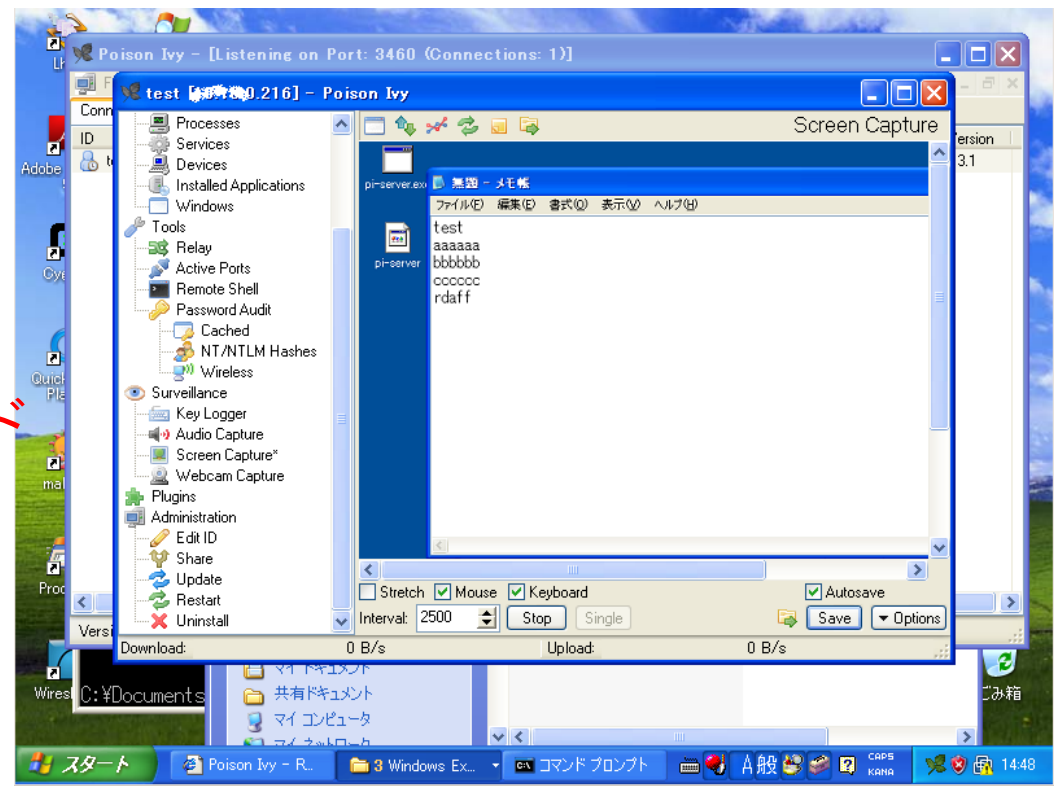
■ Data (256 bytes)
  Data: 85d9136fb07238f8a41a9a0daf41e5fa79a957c0bffa5f7f...
  [Length: 256]

0000 45 00 01 28 00 00 00 00 50 06 6b cd 7f 00 00 02 E..(....P.k.....
0010 7f 00 00 01 51 05 00 50 00 00 00 02 00 00 00 02 ....Q...P.....
0020 50 10 04 00 00 00 00 00 85 d9 13 6f b0 72 38 f8 P..... .o.r8.
0030 a4 1a 9a 0d af 41 e5 fa 79 a9 57 c0 bf fa 5f 7f ....A..y.W...
0040 75 93 06 37 fb ac 4c 62 44 16 b8 be 26 12 4f d5 u..7..Lb D...&.O.
0050 73 01 a9 18 7e f9 1f 17 9b 9a 0d 15 7a 31 63 d2 s...~... ..z1c.
0060 0f d5 e8 3c e5 76 9f 22 05 17 87 03 ab 0e 12 cc ...<.v.".....
0070 4f e5 8d ea 89 86 d0 55 ef 62 5a f2 5b 56 6d 0d o.....U .bz.[Vm.
0080 90 66 ac 4d 39 5b 1e f9 46 95 78 1f 63 4e 74 c9 .f.M9[. .F.x.cNt.
0090 2b e9 1f 31 8f 0b a3 fb f4 34 73 59 04 13 ed 89 +..1.... .4sY...
00a0 7f 83 cc 02 08 3e 48 bb 93 6b f9 e9 1c b7 88 67 .....>H. .k.....g
00b0 7a 3a 61 aa ad 4d 14 09 b8 38 e9 4b d5 83 a7 d8 z:a..M.. .8.K....
00c0 5e 86 cb 51 0c e8 5b 36 c2 bb 7f e8 23 1b 04 8e ^..Q..[6 ..#...
00d0 ca d3 c8 2f 50 5c d2 ff 2e 4e 2d ba 8e 5a 11 2b .../P\.. .N-..Z.+
00e0 1a 25 36 d2 97 91 f8 05 bb 0e 02 b3 3a 1c ed 01 .%6.....:...
00f0 7d ce a8 19 b7 9f f4 ba 50 3b 37 b2 02 c0 78 14 }..... P;7...x.
0100 5f b8 7f e1 4d cd e0 c1 ae 76 70 a8 1b a6 6b 80 ...M... .vp...k.
0110 7f 8a a7 54 22 82 fc fb 7f 33 e1 0d c1 44 d9 31 ...T"....3...D.1
0120 e8 c4 21 24 63 9f 6b d7 ..!$c.k.
  
```

Poison Ivyとは

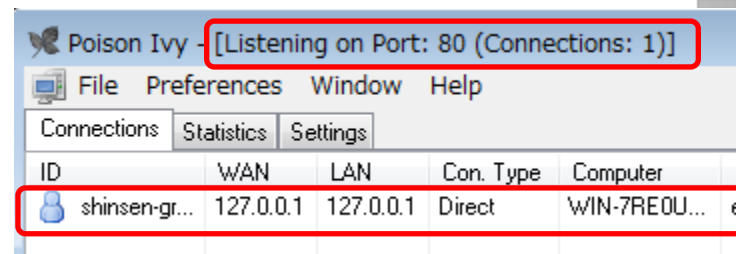
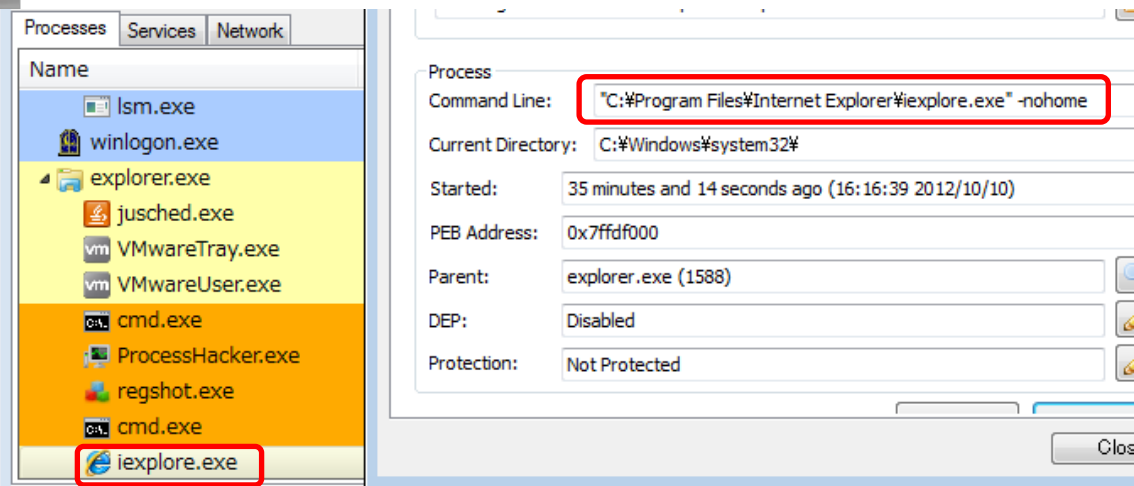
- RAT(Remote Administration Tool)と呼ばれ、リモートから端末を操作するためのツールの一種
- 現状でも配布用Webサイトが生存しており、だれでも入手可能

- 画面操作
- マウスやキーボードの操作
- キー入力の盗聴
- WebCam(カメラ)の盗撮
- マイクの盗聴
- 任意のファイルのダウンロード、アップロード、実行などが可能



実行されたマルウェアの特定(Cont.)

- Process Hackerで見てみると・・・
- メモリフォレンジックツール (Redline) による検出
 - iexplore.exeが含む特徴的なハンドル名：!VoqA.I4
 - ただし、ビルド時に自由に変更可能
 - コードインジェクションされたとおぼしき領域も存在
- PoisonIvyのGUIクライアントを起動
 - 該当プログラムが接続に来るか？
 - デフォルトパスワード(admin)のまま接続可能



Malware Risk Index Hits



This process has a module which imports a suspicious Handle (Mutant)!\VoqA.I4. "Process has a known Poison Ivy mutant".

実行されたマルウェアの詳細解析

- 補足：コードレベルで特徴を把握したい場合
 - アンパック
 - VirtualAllocEx/VirtualProtectEx等の動的な領域確保・属性変更のAPIに着目
 - デバッグ
 - フラグメント化したコードのインジェクション
 - wmi.exe: explorer.exeへインジェクション
 - explorer.exe: iexplore.exeを起動、マルウェアのインストール、インジェクション
 - iexplore.exe
 - クライアントへの接続を開始
 - 静的解析
 - shellcodeライクなAPI呼び出し
 - call [esi + *]

```
push    40h                ; fIProtect
push    3000h              ; fIAllocationType
push    [ebp+dwSize]      ; dwSize
push    0                  ; lpAddress
push    [ebp+hProcess]    ; hProcess
call    [esi+pi_struct.field_b1_kernel32_VirtualAllocEx]
push    eax
lea     edi, [ebp+var_4]
push    edi                ; *lpNumberOfBytesWritten
push    [ebp+dwSize]      ; nSize
push    [ebp+arg_C]       ; lpBuffer
push    eax                ; lpBaseAddress
push    [ebp+hProcess]    ; hProcess
call    [esi+pi_struct.field_b5_kernel32_WriteProcessMemory]
```

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査 (ハンズオン#1)
 - マルウェアの登録時刻の特定
 - タイムラインの解析 (ハンズオン#2)
 - 悪性文書ファイルの解析 (ハンズオン#3)
 - シェルコード・マルウェアの解析
 - **調査結果**
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

感染原因に関する調査結果

- 攻撃のトリガ
 - 攻撃者は2012/10/5 17:05:10にファイルを添付したメールを送信
 - このWordファイル内に悪性のswfファイルが含まれていた
 - exploitはCVE-2012-1535の脆弱性についてマルウェアをドロップ
- インストールされたマルウェア
 - マルウェアのインストールパス
 - ファイルシステム
 - C:/Users/okita/AppData/Roaming/wmi.exe
 - レジストリ
 - HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
 - PoisonIvyというRATに分類されるマルウェア
 - C&Cサーバ
 - www.fewjriehgusuoh.com
- 今後は、感染後の影響範囲に関する調査が必要
 - 端末内のデータの詐取
 - そこを踏み台として他端末やサーバへの不正アクセス

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

その後の活動の調査

- マルウェアが生成された時刻から漏えいしたデータのタイムスタンプまでの期間を調査
 - wmi.exeの最終更新時刻
 - 2012/10/5 17:05:56
 - a.7z内のaフォルダの最終更新時刻
 - 2012/10/5 18:34:29
- 漏えいしたファイル名 (a.7z) を検索してもヒットしない
- wmi.exe生成後、大量のレジストリへのアクセスや周辺端末へのログイン試行が見られる
 - イベントログの閲覧、フィルタ、検索
 - イベントビューア
 - Event Log Explorer
 - Poison Ivyインストール後の情報列挙か？
 - 何らかのツールを利用している可能性が高い
- 2012/10/5 19:44:45にメモリダンプ(C:/Windows/MEMORY.DMP)を生成、システムクラッシュ
 - ここまでにそれらしきツールのエントリは無し

その後の活動の調査 (Cont.)

- wmi.exe実行後から大量のレジストリエントリ発生までの間を再調査
- フォルダ"t"
 - いくつかの実行ファイルが存在
 - ただし、タイムスタンプが対象期間内ではない
 - 本当に無関係？

10/05/2012	17:10:26	Japan	MACB	EVTX	Application	Event Logged	-	win7uspl.s Event ID Application/[Application/Desktop Window Manager ID [9013
10/05/2012	17:10:29	Japan	MACB	EVTX	Application	Event Logged	-	win7uspl.s Event ID Application/[Application/Desktop Window Manager ID [9013
10/05/2012	17:10:34	Japan	...B	FILE	NTFS \$MFT	\$SI [...B] time	-	WIN7USP1 C:/Users/okita/AppData/Local/Temp/t
10/05/2012	17:10:59	Japan	MACB	EVTX	Microsoft-Win	Event Logged	-	win7uspl.s Event ID Microsoft-Windows-TaskScheduler/Operation

Name	Size	accessed	altered	creation
7z.dll	914432	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
7z.exe	163840	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
Abel.dll	37888	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
Abel.exe	31232	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
Abel64.dll	114688	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
Abel64.exe	104448	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
GoogleUpdateSetup.exe24...	763232	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM
PsExec.exe	381816	7/14/09 1:14 AM	7/14/09 1:14 AM	7/14/09 1:14 AM

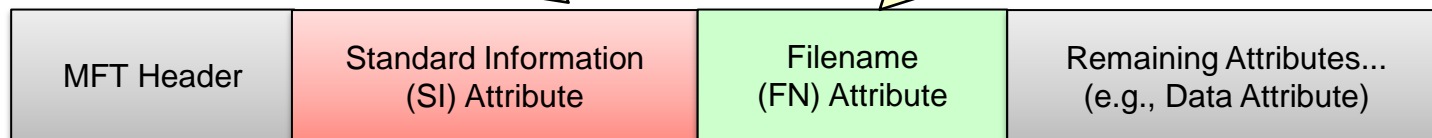
アンチフォレンジック(1)

- タイムスタンプの変更
 - timestomp
 - マルウェアによって一般的に行われる
- 変更の検出
 - NTFSファイルシステムには2種類のタイムスタンプが存在する
 - Standard Information (SI): 通常参照される
 - File Name (FN): 参照されない、変更するAPIも無い
 - FN属性も含めてタイムラインを生成する(win7usp1-current-with-fn)
 - tフォルダ以下は対象期間内に生成されたファイル

一般にOSやアプリケーションによって参照されるタイムスタンプを保持。APIによって任意の時間に変更可能。

更新されにくいタイムスタンプを保持。SI属性のタイムスタンプより一般に古くなる。APIによって変更できない。

ファイル毎の
メタデータ
レコード



0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/scan.bat
0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/woot_x64.exe
0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/plink.exe
0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/stone.exe
0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/Abel.dll
0/05/2012	17:10:33	Japan	ACB	FILE	NTFS \$MFT \$FN [ACB] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t/PsExec.exe
0/05/2012	17:10:34	Japan	MACB	FILE	NTFS \$MFT \$FN [MACB] tim-	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t
0/05/2012	17:10:34	Japan	...B	FILE	NTFS \$MFT \$SI [..B] time -	WIN7USP1 C:/Users/cC:/Users/okita/AppData/Local/Temp/t

アンチフォレンジック(2)

- ファイルデータ、フォルダのメタデータの上書き削除
 - sdelete.exe
 - マルウェアによってまれに行われる or 時間の経過によって自然に行われる
- 過去のファイルシステムの参照
 - Volume Shadow Copyを調べる
 - ホストのWindowsで調べる場合
 - ddイメージをvhdに変換 (vhdttools)
 - » 勝手に上書きするのでイメージのバックアップを取っておく
 - Windows7の標準機能でマウント
 - ShadowKitでブラウジング、エクスポート
 - SIFTで調べる場合
 - fdiskでイメージのsector数とunit数を調べる
 - vshadowmountでVSSのイメージをマウント
 - マウントしたイメージからファイルをTSKで抽出、log2timelineでタイムラインを作成

攻撃者がアップロードしたツール

- 以下のツールをアップロードしている
 - scan.bat
 - ネットワーク・アカウント・ファイル情報の収集
 - wce.exe/wce_x64.exe
 - パスワード/パスワードハッシュのダンプ、pass-the-ticket/pass-the-hash
 - PsExec.exe
 - 遠隔でコマンドを実行
 - PwDump7.exe
 - パスワードハッシュのダンプ
 - timestomp.exe
 - タイムスタンプの変更
 - sdelete.exe
 - フォルダ・ファイルの上書き削除
 - stone.exe
 - トンネリングツール
 - plink.exe
 - SSHクライアント
 - woot.exe/woot_x64.exe
 - ?
- 実際にツールが使われたか？
 - AppCache内には実行痕跡が存在していない
 - 無い場合もそれが実行されていないとは限らないので注意が必要
 - SysInternalsのツールはDEFAULTレジストリにEULAを承諾したデータが入る（キー生成時刻 = 初回実行時刻）
 - wce.exeは実行の度にwceaux.dllをspawnする
 - キーワード検索で総当り的に探す（SIFTのsrch_strings_wrap）

2012/10/05 17:35:40
psexec実行

2012/10/09 19:05:09
sdelete実行

wce.exeとは

- パスワードハッシュのダンプやpass-the-hash, pass-the-ticketなどの機能を持つ
 - パスワード自体の抽出も可能
 - Pass-the-Hash Toolkitの後継 (同じ作者)
- ハッシュのダンプやパスワードの抽出には**管理者権限が必要**
- dll (wceaux.dll) を動的に生成して利用する
 - 運が良ければその痕跡を見つけられることも

```
C:\work\wce_v1_3beta_x64>wce -w
WCE v1.3beta (X64) (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

hoge¥HOGE:hogehoge
aduser1¥HOGE:hogeADpass1
WIN7ULTIMATE$¥HOGE:<contains-non-printable-chars>
```

Name	Ext.	Type	Path
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp
wceaux.dll	dll	dll	\Users\okita\AppData\Local\Temp

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの詳細解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

攻撃者ツール(woot.exe)の解析

- Stringsコマンドで特徴的な文字列

kernel32.dll

lsWow64Process

ntdll.dll

NtQueryIntervalProfile

NtAllocateVirtualMemory

NtDeviceIoControlFile

NtQuerySystemInformation

HalDispatchTable

PsInitialSystemProcess

PsReferencePrimaryToken

PsGetThreadProcess

127.0.0.1

cmd.exe

open

赤: kernel exploitでよく用いられる
関数、変数

緑: 特徴的な文字列

攻撃者ツール(woot.exe)の解析(Cont.)

- 検索キーワード: NtQueryIntervalProfile NtQuerySystemInformation HalDispatchTable PsInitialSystemProcess PsReferencePrimaryToken 127.0.0.1

Google

ile NtQuerySystemInformation| HalDispatchTable PsInitialSystemProcess Psf

検索 約 244 件 (0.23 秒)

ウェブ

[MS11-080,MS11-046 漏洞利用代码vc++6.0 - 怖客官方网站](#)

www.bkhack.com/.../MS11-080-MS11-0... - キャッシュ - このページを訳す

画像

地図

動画

ニュース

ショッピング

もっと見る

この場所の付近を
検索...

現在地を入力

設定

ウェブ全体から検索

日本語のページを検索

翻訳して検索

もっとツールを見る

[MS11-080 WINDOWS 2003 XP 提权 ODAY 源码- VC++ 教程- 怖客官方 ...](#)

www.bkhack.com/vc/268.html - キャッシュ - このページを訳す

2012年4月3日 - ... ULONG);; NtQueryIntervalProfile_ NtQueryIntervalProfile;;
NtAllocateVirtualMemory_ NtAllocateVirtualMemory;; NtQuerySystemInformation_
NtQuerySystemInformation;; ULONG PsInitialSystemProcess,
PsReferencePrimaryToken, ... WriteToHalDispatchTable =
(ULONG)GetProcAddress(ntoskrnl, "HalDispatchTable") - (ULONG)ntoskrnl +
NtoskrnlBase + ... peer.sin_port = htons(4455);; peer.sin_addr.s_addr =
inet_addr("127.0.0.1");; tcp_socket = socket(AF_INET, ...

[MS11-080: 辅助功能驱动程序本地提权 通向内核之地 百度空间](#)

hi.baidu.com/.../49c813d7c7dc44c0a344... - キャッシュ - このページを訳す

2011年12月5日 - mov esi,PsReferencePrimaryToken ... mov

MS11-046 or MS11-080

攻撃者ツール(woot.exe)の解析(Cont.)

- MS11-046
 - この時点でサポートされていたすべてのバージョンのWindowsに脆弱性が存在
 - 要点
 - このセキュリティ更新プログラムは、**一般で公開された 1 件の Microsoft Windows Ancillary Function ドライバー (AFD) の脆弱性**を解決します。この脆弱性により、攻撃者がユーザーのシステムにログオンし、特別に細工されたアプリケーションを実行した場合、**特権が昇格される**可能性があります。これらの脆弱性が悪用されるには、有効なログオン資格情報を所持し、ローカルでログオンできることが攻撃者にとっての必要条件となります。
 - <http://technet.microsoft.com/ja-jp/security/bulletin/ms11-046>

攻撃者ツール(woot.exe)の解析(Cont.)

● MS11-080

影響を受けるソフトウェア

オペレーティングシステム	最も深刻な脆弱性
Windows XP Service Pack 3	特権の昇格
Windows XP Professional x64 Edition Service Pack 2	特権の昇格
Windows Server 2003 Service Pack 2	特権の昇格
Windows Server 2003 x64 Edition Service Pack 2	特権の昇格
Windows Server 2003 with SP2 for Itanium-based Systems	特権の昇格

この脆弱性の対象がXP, 2003のみなので、Windows7で動作するMS11-046の方が有力

影響を受けないソフトウェア

オペレーティングシステム

Windows Vista Service Pack 2

Windows Vista x64 Edition Service Pack 2

Windows Server 2008 for 32-bit Systems Service Pack 2

Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 for Itanium-based Systems Service Pack 2

Windows 7 for 32-bit Systems および Windows 7 for x64-based Systems

Windows 7 for x64-based Systems および Windows 7 for 32-bit Systems

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 R2 for Itanium-based Systems Service Pack 1

<http://technet.microsoft.com/ja-jp/security/bulletin/ms11-080>

攻撃者ツール(woot.exe)の解析(Cont.)

- MS11-046

- 前項までの情報をもとに、パッチ適用の有無で脆弱性が発動するかを確認するか、もしくは・・・
- 検索結果から、いくつかのコードを読むと以下のことがわかる
 - NtDeviceIoControlFile で指定するdwIoControlCode が0x12007 (AfdConnect) の時、その戻り値 (4バイト) を任意のアドレスに書き込める
 - これを使って任意のコードのアドレスをHalDispatchTable + 4に書き込む
 - NtQueryIntervalProfile (HalDispatchTable+4) を呼び、任意のコードを実行



コードレベルでExploitの挙動を確認する

攻撃者ツール(woot.exe)の静的解析

- 補足：静的解析による大まかな挙動の把握
 - アドレス 1 (ページ 0 に切り捨て) にシェルコード用の領域を確保
 - シェルコードは System プロセスのトークンを現在のプロセスにセットするコード
 - NtDeviceIoControlFile のコードのメモリ属性を変更、フックのインストール
 - フック先では IoControlCode をチェック
 - 12007h の場合、出力バッファを HalDispatchTable + 4 を上書きするようセット
 - 戻り値を 0 にすることでページ 0 を HalDispatchTable + 4 が指すようにする
 - connect を呼び出して NtDeviceIoControlFile を間接的に実行
 - NtQueryIntervalProfile (HalDispatchTable + 0x4) をコール、シェルコードを実行

```

mov     eax, [edx+1] ; // == 32bit NtDeviceIoControlFile
; // ALL Args in Stack
; // 7C94D270 B8 43000000 MOV EAX, 42 < USE_HERE
; // 7C94D275 BA 0003FE7F MOV EDX, 7FFE0300
; // 7C94D27A FF12 CALL DWORD PTR DS:[EDX]
; // 7C94D27C C2 0400 RETN 4
; // 7C94D27F 90 NOP
mov     ds:Ssdt IdOfNtDeviceIoControlFile, eax
mov     eax, offset ToHookNtDeviceIoControlFile ; hook code
sub     eax, edx
mov     [ebp+OffsetOfHookedNtDeviceIoControlFile], eax
mov     byte ptr [edx], 0E8h ; CALL (create hook)
mov     eax, [ebp+OffsetOfHookedNtDeviceIoControlFile]
mov     [edx+1], eax
  
```

フックのインストール

```

nop
7+cmp   [esp+arg_14], 12007h ; dwIoControlCode
jnz     short loc_4021A8
  
```

```

00 mov     eax, ds:HalDispatchTablePlus4
      mov     [esp+arg_20], eax ; lpOutBuffer
:00+mov   [esp+arg_24], 0 ; nOutBufferSize
  
```

```

loc_4021A8:
)0 mov     eax, ds:Ssdt IdOfNtDeviceIoControlFile
      retn
  
```

フック先の処理

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

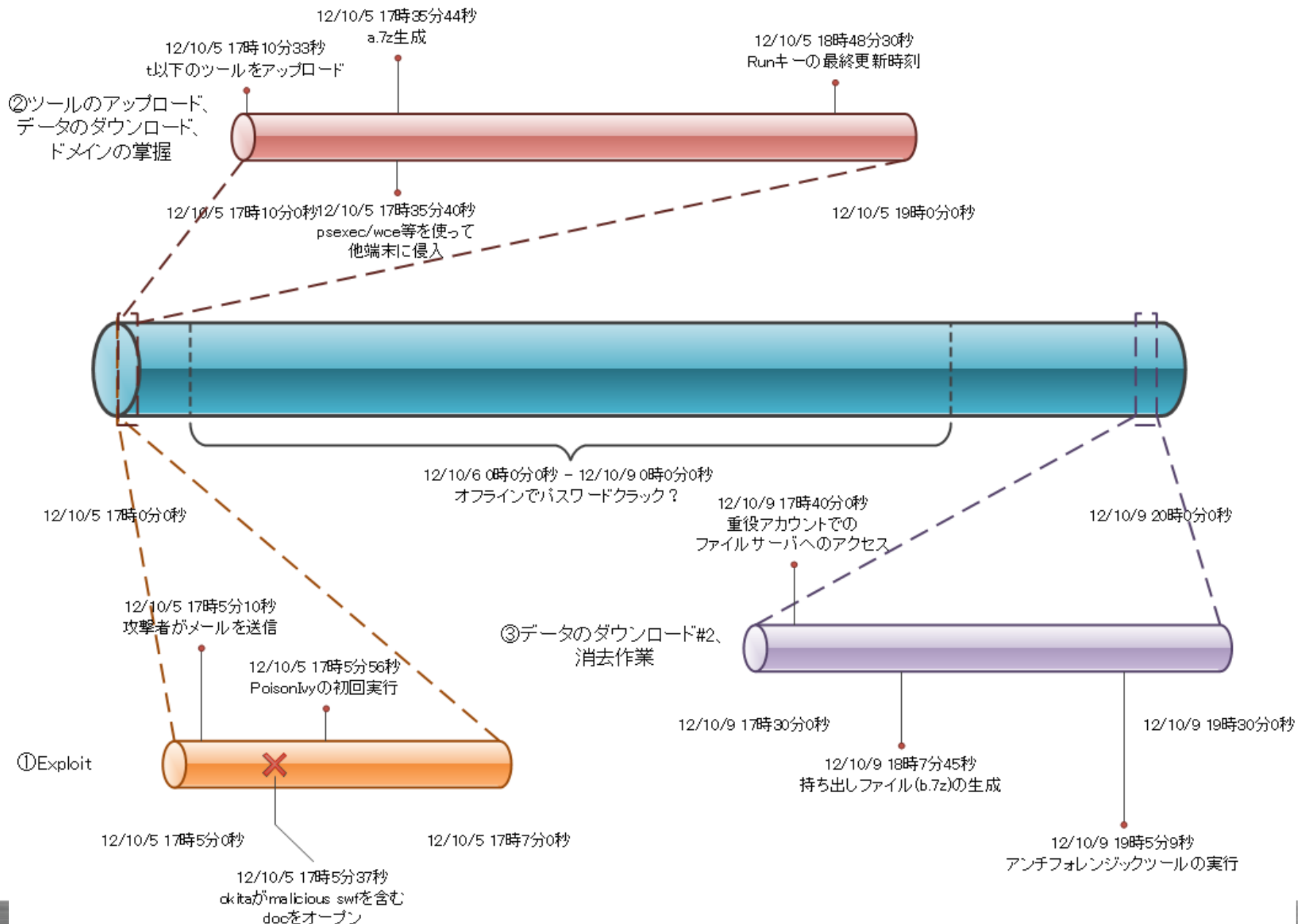
感染後の影響範囲に関する調査結果

- ツールの種類やファイルシステムのタイムスタンプ、漏洩したファイルの内容やタイムスタンプ、ファイルサーバのログ等から、以下の行動が推測できる
 - 2012/10/5 17:10:33
 - ツールのアップロード
 - ? (ツールのアップロードからpsexec実行までの間)
 - CVE-2011-1249を悪用するプログラムとwceを用いて、感染端末内のパスワードやハッシュを取得
 - 2012/10/05 17:35:40頃
 - psexec/wce等を使い、pass-the-ticket? でなりすましを行い、他の端末に侵入
 - 2012/10/05 18:35:44頃
 - 取得した情報を圧縮ファイルa.7zにまとめ、ダウンロード?
 - a.7zに含まれるハッシュ取得のログやDBファイルから、ドメイン管理者権限を取得された可能性大
 - 2012/10/09 17:40以降 (ファイルサーバのイベントログ)
 - 重役アカウントでのファイルサーバへのアクセス
 - 2012/10/09 18:07:45頃
 - 取得した情報を圧縮ファイルb.7zにまとめ、ダウンロード?
 - 2012/10/09 19:05:09頃
 - アンチフォレンジックとしてツールのタイムスタンプ変更、圧縮ファイルの完全削除を実施
- 他の端末にいつ頃侵入したか等については、他の端末やサーバを調査しなければ正確に把握できない
 - 認証系のイベントログ
 - psexecの実行痕跡 (PSEXESVC)
 - 削除ファイル (psexesvc.exe + リモートで実行されたexe)
 - レジストリの削除領域 (サービスの登録)、ページファイル内の実行ファイルパス, etc..

本ケースの解析内容

- タイムラインの作成
- 感染原因に関する解析
 - 自動起動設定プログラムの調査（ハンズオン#1）
 - マルウェアの登録時刻の特定
 - タイムラインの解析（ハンズオン#2）
 - 悪性文書ファイルの解析（ハンズオン#3）
 - シェルコード・マルウェアの解析
 - 調査結果
- 感染後の影響範囲に関する解析
 - その後の活動の調査
 - 未知のバイナリの解析
 - 調査結果
- まとめ
 - インシデントのタイムライン

インシデントのタイムライン



最後に

- インシデントレスポンスではフォレンジック解析・マルウェア解析を組み合わせることで以下を明らかにしていく
 - マルウェア感染の有無、種別、機能
 - 感染原因
 - 被害範囲
- 実際のディスクイメージはよりカオスなので、数をこなして経験値を上げていく
 - AVや管理者による検疫・削除、設定変更
 - 大量のデータ、用途不明なプログラム群
 - 調査開始までのタイムラグ
- フリーのツールでもある程度までの解析は可能
 - より効率的にやりたい場合は商用ツールを使う
 - IDA Pro
 - EnCase/X-Ways Forensics
 - etc..

参考URL

- フォレンジック解析
 - SANS SIFT Forensic Workstation
 - <http://computer-forensics.sans.org/community/downloads>
 - Digital Forensic Framework
 - <http://www.digital-forensic.org/>
 - log2timeline-siftで、タイムライン生成時に\$fn (\$filename) 属性タイムスタンプも含めるための変更箇所
 - <http://list-archives.org/2012/07/10/dfir-lists-sans-org/log2timeline-vs-log2timeline-sift/f/4359338113>
 - vshadowmountを用いたVolume Shadow Copyボリュームのマウント手順
 - <http://code.google.com/p/libvshadow/wiki/Mounting>
 - AutoRuns
 - <http://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx>
 - FTK Imager
 - <http://accessdata.com/support/product-downloads>
 - Registry Decoder
 - <http://www.digitalforensicsolutions.com/registrydecoder/>
 - Prefetch Parser
 - <http://computer-forensics.sans.org/blog/2010/02/12/prefetch-parser-v1-4/>
 - ShimCacheParser
 - <https://github.com/mandiant/ShimCacheParser>
 - Web historian
 - <http://www.mandiant.com/resources/download/web-historian>
 - JumpLister
 - http://www.woanware.co.uk/?page_id=266
 - Redline
 - <http://www.mandiant.com/resources/download/redline/>
 - Event Log Explorer
 - <http://www.eventlogxp.com/>
 - vhdtool
 - <http://archive.msdn.microsoft.com/vhdtool>
 - ShadowKit
 - <http://redrocktx.blogspot.jp/p/shadowkit.html>
 - TSK
 - <http://www.sleuthkit.org/>

参考URL (Cont.)

- マルウェア解析
 - FileInsight
 - <http://www.mcafee.com/us/downloads/free-tools/fileinsight.aspx>
 - FileInsightで利用できるドキュメントマルウェア解析用プラグイン
 - <https://github.com/nmantani/FileInsight-plugins>
 - REMnux
 - <http://zeltser.com/remnux/>
 - OfficeMalScanner
 - <http://www.reconstructor.org/code.html>
 - PDF Stream Dumper
 - <http://sandsprite.com/blogs/index.php?uid=7&pid=57>
 - SWFINvestigator
 - <http://labs.adobe.com/technologies/swfinvestigator/>
 - IDA Pro Free
 - http://www.hex-rays.com/products/ida/support/download_freeware.shtml
 - OllyDbg
 - <http://www.ollydbg.de/>
 - Immunity Debugger
 - <http://debugger.immunityinc.com/>
 - libemu
 - <http://libemu.carnivore.it/>
 - process hacker
 - <http://processhacker.sourceforge.net/>
 - captureBAT
 - <http://www.honeynet.org/node/315>
 - regshot
 - <http://sourceforge.net/projects/regshot/>
 - FakeNet
 - <http://practicalmalwareanalysis.com/fakenet/>
 - NT Kernel Resources: PsExec Internals
 - <http://www.ntkernel.com/w&p.php?id=15>

参考URL (Cont.)

- Exploit
 - CVE-2012-1535
 - <http://contagiodump.blogspot.jp/2012/08/cve-2012-1535-samples-and-info.html>
 - <http://contagio.deependresearch.org/docs/CVE-2012-1535-Adobe-Flash-Player-Integer-Overflow-Vulnerability-Analysis.pdf>
 - <http://labs.alienvault.com/labs/index.php/2012/cve-2012-1535-adobe-flash-being-exploited-in-the-wild/>
 - CVE-2011-1249 (MS11-046)
 - <http://www.exploit-db.com/wp-content/themes/exploit/docs/18712.pdf>

お勧め文献

- フォレンジック解析
 - File System Forensic Analysis
 - Windows Forensic Analysis DVD Toolkit
 - Mastering Windows Network Forensics and Investigation
- マルウェア解析
 - アナライジングマルウェア
 - Rootkits: Subverting the Windows Kernel
 - The Rootkit Arsenal
 - Malware Analyst's Cookbook and DVD
 - Practical Malware Analysis
- その他
 - はじめて読む486
 - IDA Pro Book
 - Windows Internals (インサイド Microsoft Windows)
 - Reversing: Secrets of Reverse Engineering
 - 解析魔法少女美咲ちゃん