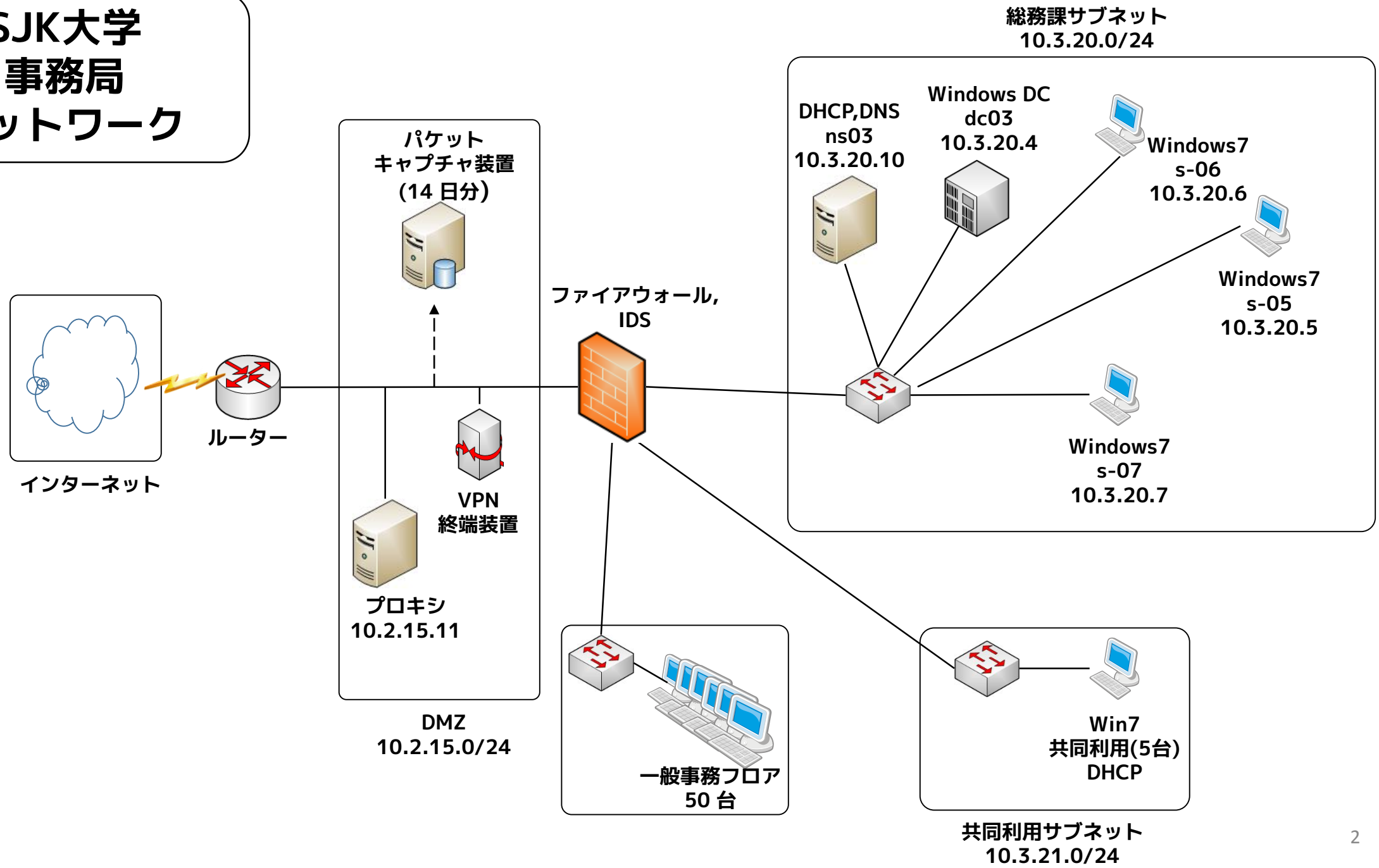
タイムライン解析結果

私立大学情報教育協会
大学情報セキュリティ研究講習会

SJK大学
事務局
ネットワーク



ミッション遂行の流れ

1. 不審なプロセスの確認

2. 不審なユーザーの

操作履歴の確認

3. 推測される被害状況

のまとめと今後の対応

タイムラインとは

【概要】ファイルシステムのタイムスタンプ情報を利用して、コンピュータの状態遷移を時系列的に調査できるように収集したデータ。

最近は、実行ファイルの起動やレジストリの変更履歴なども統合して扱われることが多い。

タイムラインとは

【収集される情報例】

1. MAC タイム（ファイルの作成・変更・アクセス日時）
2. 実行されたファイルの名前・場所・日時
3. イベントログ（ネットワークログオン成功など）
4. レジストリ変更履歴
5. Web 閲覧履歴
6. USB 利用履歴

本実習で扱うタイムライン

【対象】s-05端末
（総務課長が利用、機密情報が保管されている）

【期間】2014/04/01～2014/04/05

【項目】

1. MAC タイム
2. 実行されたファイルの名前・場所・日時
3. イベントログ
4. レジストリ変更履歴

1. 不審なプロセスの確認

PFファイル

1. PF ファイル
   - 最近アクセスしたファイルを記録し、アプリケーションの起動を高速に行うために自動的に作成されるファイル
   - 拡張子は .pf
2. 「Prefetch」フォルダ
   - PFファイルを収容するフォルダ
   - 起動された実行ファイルの痕跡調査のために、タイムラインの作成に参照される

PFファイル抜粋リスト（時系列）

date	time	filename
04/01/2014	14:16:11	/Windows/Prefetch/EXPLORER.EXE-7A3328DA.pf
04/01/2014	14:16:20	/Windows/Prefetch/DLLHOST.EXE-71214090.pf
04/01/2014	14:17:38	/Windows/Prefetch/ACRORD32.EXE-33939BD1.pf
04/03/2014	20:25:40	/Windows/Prefetch/VMWARETRAY.EXE-1DBB7768.pf
04/03/2014	20:25:40	/Windows/Prefetch/VMWAREUSER.EXE-83D1845B.pf
04/03/2014	20:26:18	/Windows/Prefetch/NETPLWIZ.EXE-23BBB05C.pf
04/03/2014	21:03:30	/Windows/Prefetch/TOPLZAGU.EXE-4EFD8FD3.pf
04/03/2014	21:03:40	/Windows/Prefetch/RUNDLL32.EXE-6706170E.pf
04/03/2014	21:11:08	/Windows/Prefetch/PSEXESVC.EXE-51BA46F2.pf
04/03/2014	21:18:21	/Windows/Prefetch/OSCMPGPK.EXE-DDCC6901.pf
04/03/2014	21:19:56	/Windows/Prefetch/IPCONFIG.EXE-62724FE6.pf
04/03/2014	21:36:22	/Windows/Prefetch/CMD.EXE-89305D47.pf
04/03/2014	21:36:56	/Windows/Prefetch/DLLHOST.EXE-C85DDD7D.pf
04/03/2014	21:44:42	/Windows/Prefetch/NETSTAT.EXE-6D34D712.pf
04/03/2014	21:45:44	/Windows/Prefetch/WMIC.EXE-B77E8CD6.pf
04/03/2014	21:47:59	/Windows/Prefetch/DLLHOT.EXE-9BB7786D.pf
04/03/2014	22:08:25	/Windows/Prefetch/RUNDLL32.EXE-17E909EA.pf
04/03/2014	22:08:25	/Windows/Prefetch/IE4UINIT.EXE-0BC11EF2.pf
04/03/2014	22:08:26	/Windows/Prefetch/REGSVR32.EXE-55A4EE79.pf
04/03/2014	22:08:33	/Windows/Prefetch/WINMAIL.EXE-D6E90604.pf
04/03/2014	22:08:50	/Windows/Prefetch/PRINTISOLATIONHOST.EXE-.pf

date	time	filename
04/03/2014	22:08:59	/Windows/Prefetch/SHSTAT.EXE-3E759080.pf
04/03/2014	22:08:59	/Windows/Prefetch/FIRETRAY.EXE-83604477.pf
04/03/2014	22:13:12	/Windows/Prefetch/TASKMGR.EXE-72398DC0.pf
04/03/2014	22:21:06	/Windows/Prefetch/FIREFOX.EXE-E60C0AA7.pf
04/03/2014	22:22:15	/Windows/Prefetch/HELPER.EXE-36267E56.pf
04/03/2014	22:39:19	/Windows/Prefetch/FIREFOX.EXE-E60C0AA7.pf
04/03/2014	23:09:26	/Windows/Prefetch/SPINLOCK.EXE-1610A75A.pf
04/03/2014	23:10:02	/Windows/Prefetch/NETSTAT.EXE-6D34D712.pf
04/03/2014	23:37:54	/Windows/Prefetch/REG.EXE-26976709.pf
04/03/2014	23:45:06	/Windows/Prefetch/SC.EXE-BC6DAF49.pf
04/03/2014	23:54:48	/Windows/Prefetch/A.EXE-8D56B1C4.pf
04/03/2014	23:54:56	/Windows/Prefetch/SVCHOST.EXE-BD36E5C8.pf
04/04/2014	0:08:58	/Windows/Prefetch/NTOSBOOT-B00DFAAD.pf
04/04/2014	0:13:15	/Windows/Prefetch/SVCHOST.EXE-135A30D8.pf
04/04/2014	0:13:17	/Windows/Prefetch/SEARCHINDEXER.EXE-.pf
04/04/2014	0:14:30	/Windows/Prefetch/WMIADAP.EXE-369DF1CD.pf
04/04/2014	0:43:06	/Windows/Prefetch/A.EXE-8D56B1C4.pf
04/04/2014	0:46:05	/Windows/Prefetch/RUNDLL32.EXE-85E123DD.pf
04/04/2014	1:09:03	/Windows/Prefetch/HYDRAKATZ.EXE-A0DADA85.pf
04/04/2014	1:18:22	/Windows/Prefetch/WERFAULT.EXE-B7E27BE5.pf
04/04/2014	1:52:26	/Windows/Prefetch/SC.EXE-BC6DAF49.pf

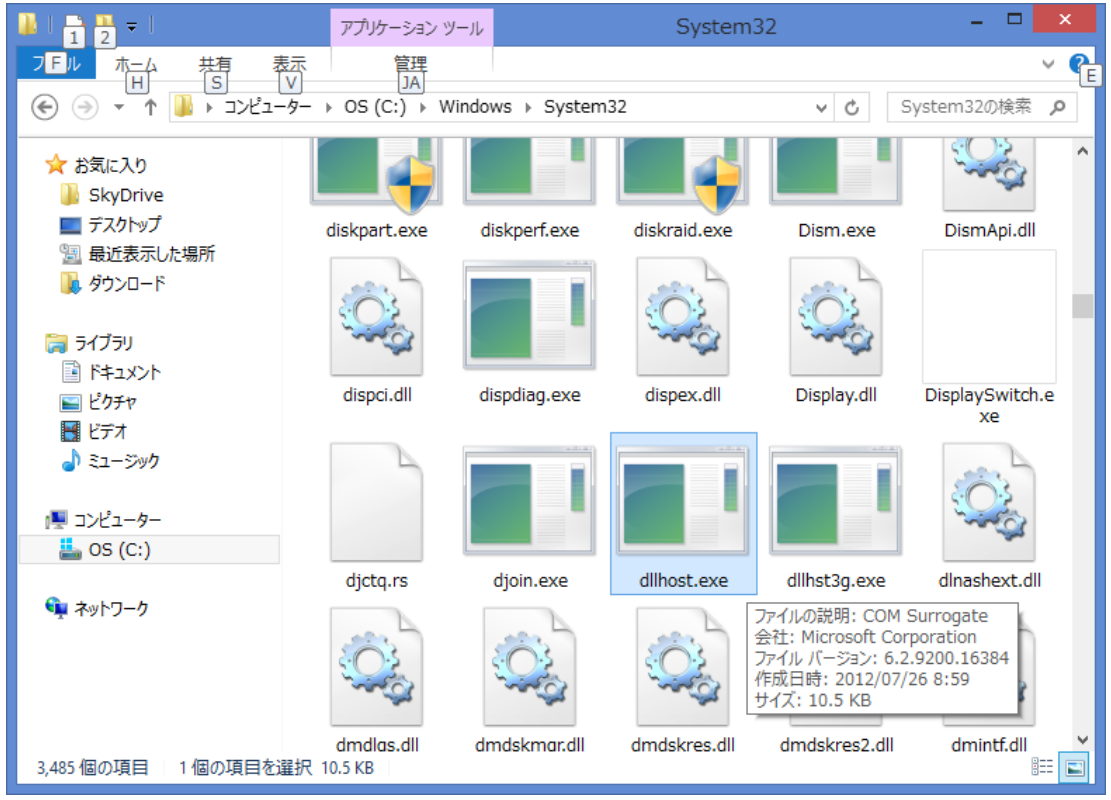
赤色：実行されることが疑わしいもの
黄色：通常のPC利用では実行されないもの

要調査

svchost.exe と spinlock.exe を調べてみよう

svchost.exe とは

ＯＳ内の各種サービスを起動するための親となるプロセスである。
ＯＳ起動時には、svchost.exe を経由して、各種のネットワーク・サービスが起動するようになっている。
¥Windows¥System32 にインストールされる。



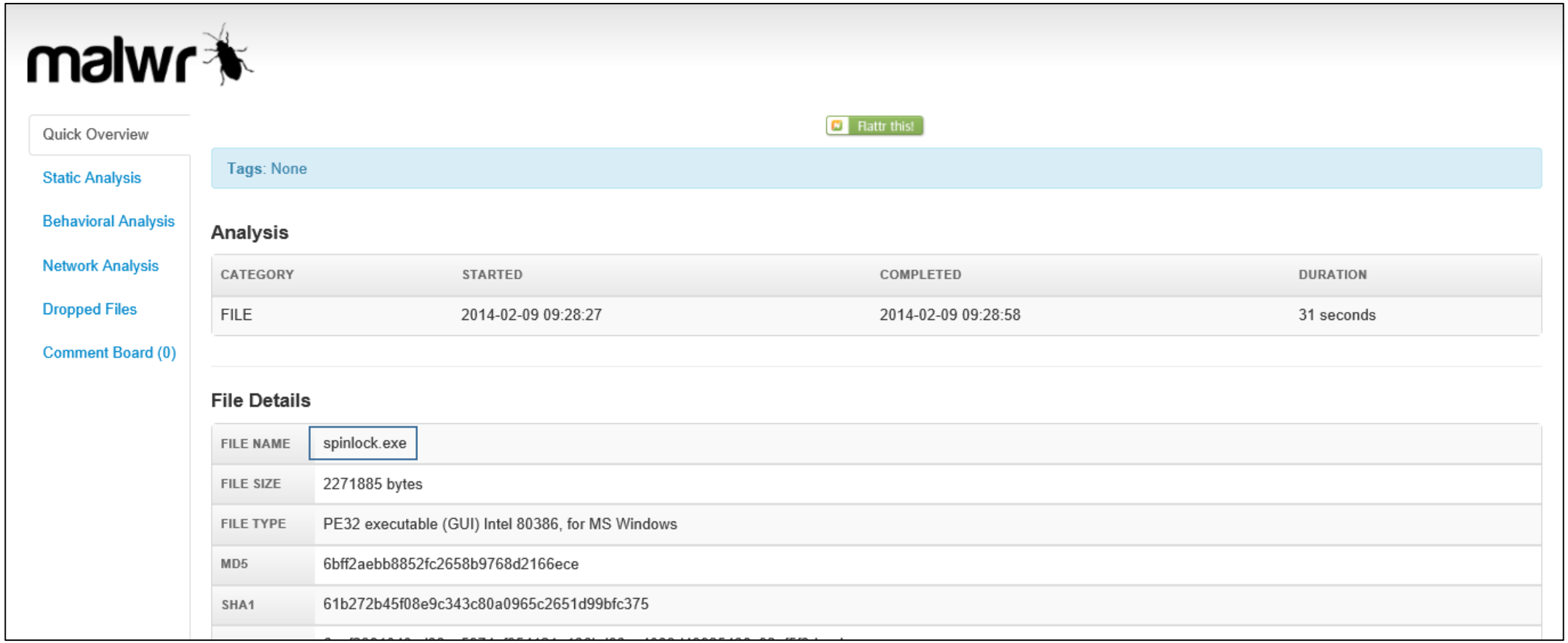
s-05 の「svchost.exe」の不審点

インストール場所

date	time	MACB	source	sourcetype	type	desc
04/04/2014	2:22:00	A.B	FILE	NTFS $MFT	$SI [.A.B] tin	/Users/keiko/AppData/Local/Temp/a.exe
04/04/2014	2:22:00	..C.	FILE	NTFS $MFT	$SI [..C.] tim	/Windows/System32/dllhost/svchost.exe
04/04/2014	2:22:00	MACB	PRE	Vista/Win7 Prefet	Last run	SVCHOST.EXE-BA833CD4.pf - [SVCHOST.EXE] was executed
04/04/2014	2:22:02	.A.B	FILE	NTFS $MFT	$SI [.A.B] tin	/Windows/Prefetch/A.EXE-F91CBA0E.pf
04/04/2014	2:22:10	MA.B	FILE	NTFS $MFT	$SI [MA.B] t	/Windows/Prefetch/SVCHOST.EXE-BA833CD4.pf

不審点
　インストール場所がおかしい。
　　本来であれば、¥Windows¥System32 フォルダであるが、dllhost フォルダが作成・保存されている

spinlock.exe とは



“spinlock.exe” の機能からの推測－１

読み込まれる DLL リスト

date	time	MACB	source	type	filename
04/04/2014	0:01:44	...B	FILE	$SI [...B] time	/Users/keiko/AppData/Local/Temp/_MEI57722
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/unicodedata.pyd
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/kernel32.dll
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/_ctypes.pyd
04/04/2014	0:01:45	MAC.	FILE	$SI [MAC.] time	/Users/keiko/AppData/Local/Temp/_MEI57722
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/spinlock.exe.manifest
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/bz2.pyd
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/python25.dll
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/MSVCR71.dll

推測される機能
この実行ファイルは、Pythonで作成され、_ctypes.pyd によりDLLが読み込まれている。
unicode.pyd からは、一般的な文字コードで書かれたファイルを処理する機能が推測される。
bz2.pyd からは、ファイルの圧縮機能が推測される。また、圧縮機能は、ネットワーク転送目的に用いられることが多い。

“spinlock.exe” の機能を推測－２

s-05端末の通信先 IP アドレス一覧

Offeset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner
0x7d8b0b50	TCPv4	0.0.0.0:445	0.0.0.0	Listening	4	System
0x7d8b0b50	TCPv6	:::445	:::0	Listening	4	System
…						
0x7F451dF8	TCPv4	-:62331	224.0.0.252:443	CLOSED	7816	Skype.exe
0x7F60AdF8	TCPv4	127.0.0.1:5678	127.0.0.1:62608	CLOSED	6404	svchost.exe
0x7F632008	TCPv4	-:62336	69.171.229.13:443	CLOSED	7816	Skype.exe
0x7F69A310	TCPv4	10.3.20.5:62617	10.3.20.4:445	CLOSED	4	System
0x7F6E81B8	TCPv4	10.3.20.5:62294	10.3.20.4:135	CLOSED	4172	taskhost.exe
0x7F6FF8D0	TCPv4	10.3.20.5:62295	10.3.20.4:49156	CLOSED	4172	taskhost.exe
0x7F7D6448	TCPv4	10.3.20.5:49805	10.3.20.4:445	ESTABLISHED	4	System
0x7F839098	TCPv4	10.3.20.5:50817	199.73.28.114:443	CLOSED	1328	spinlock.exe

推測される動作
IPアドレス199.73.28.114 のポート番号 443 に対して通信を行っている。ポート番号から推測して、HTTPS 通信の可能性が高い。

2. 不審なアカウントの操作履歴の確認

svchost.exe と spinlock.exe を起動したユーザー

svchost.exe と spinlock.exe の起動履歴

① svchost.exe

date	time	MACB	source	sourcetype	type	desc
04/04/2014	2:22:00	.A.B	FILE	NTFS $MFT	$SI [.A.B] t	/Users/keiko/AppData/Local/Temp/a.exe
04/04/2014	2:22:00	..C.	FILE	NTFS $MFT	$SI [..C.] tir	/Windows/System32/dllhost/svchost.exe
04/04/2014	2:22:00	MACB	PRE	Vista/Win7 Prefet	Last run	SVCHOST.EXE-BA833CD4.pf - [SVCHOST.EXE] was executed
04/04/2014	2:22:02	.A.B	FILE	NTFS $MFT	$SI [.A.B] t	/Windows/Prefetch/A.EXE-F91CBA0E.pf
04/04/2014	2:22:10	MA.B	FILE	NTFS $MFT	$SI [MA.B]	/Windows/Prefetch/SVCHOST.EXE-BA833CD4.pf

② spinlock.exe

date	time	MACB	source	type	filename
04/04/2014	0:01:44	...B	FILE	$SI [...B] time	/Users/keiko/AppData/Local/Temp/_MEI57722
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/unicodedata.pyd
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/kernel32.dll
04/04/2014	0:01:44	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/_ctypes.pyd
04/04/2014	0:01:45	MAC.	FILE	$SI [MAC.] time	/Users/keiko/AppData/Local/Temp/_MEI57722
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/spinlock.exe.manifest
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/bz2.pyd
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/python25.dll
04/04/2014	0:01:45	MACB	FILE	$SI [MACB] time	/Users/keiko/AppData/Local/Temp/_MEI57722/MSVCR71.dll

アカウント「keiko」の操作履歴を調査

不審ユーザー(keiko)の操作履歴

次ページ参照

	date	time	MACB	source	sourcetype	type	short
1	04/03/2014	21:03:05	MACB	EVTX	Security	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4624
	04/03/2014	21:03:05	MACB	EVTX	Security	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4672
2	04/03/2014	21:03:06	.A.B	FILE	NTFS $MFT	$SI [.A.B] time	/Windows/TopLZAGU.exe
	04/03/2014	21:03:23	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	/Windows/TopLZAGU.exe
3	04/03/2014	21:03:27	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7030
	04/03/2014	21:03:27	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7045
4	04/03/2014	21:03:30	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7036
	04/03/2014	21:03:30	MACB	REG	SOFTWARE key	Last Written	CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809}/
	04/03/2014	21:03:30	MACB	REG	SOFTWARE key	Last Written	CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809}/
	04/03/2014	21:03:30	MACB	PRE	Vista/Win7 Prefet	Last run	TOPLZAGU.EXE-4EFD8FD3.pf: TOPLZAGU.EXE was executed
	04/03/2014	21:03:30	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7036
	04/03/2014	21:03:30	MA.B	FILE	NTFS $MFT	$SI [MA.B] time	/Windows/Prefetch/TOPLZAGU.EXE-4EFD8FD3.pf
	04/03/2014	21:03:30	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7036
5	04/03/2014	21:03:31	MACB	EVTX	Security	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4634
6	04/03/2014	21:03:31	.A.B	FILE	NTFS $MFT	$SI [.A.B] time	/Windows/Temp/svc.exe
7	04/03/2014	21:11:07	MACB	EVTX	Security	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4624
	04/03/2014	21:11:07	MACB	EVTX	Security	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4672
8	04/03/2014	21:11:07	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7036
	04/03/2014	21:11:07	MACB	EVTX	System	Event Logged	Event ID System/Service Control Manager:7045
9	04/03/2014	21:11:08	.A.B	FILE	NTFS $MFT	$SI [.A.B] time	/Windows/Prefetch/PSEXESVC.EXE-51BA46F2.pf

不審アカウント(keiko)のリモートログオンの痕跡

Security/Microsoft-Windows-Security-Auditing ID [4624] :
（中略）
TargetUserName = keiko
（中略）
LogonType = 3 （ネットワークログオン）
LogonProcessName = NtLmSsp
AuthenticationPackageName = NTLM
（中略）
IpAddress = 10.3.20.7
IpPort = 3072

不審ユーザー(keiko)の操作履歴

keiko が実行したアプリと開いたファイル

① 実行したアプリケーション

date	time	MACB	source	sourcetype	type	user	short
04/04/2014	15:41:55	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	/Users/keiko/AppData/Roaming/Microsoft/Excel/XLSTART
04/04/2014	15:41:55	MACB	REG	NTUSER key	Last Written	keiko	Software/Microsoft/IMEMIP
04/04/2014	15:41:55	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	/Users/keiko/AppData/Roaming/Microsoft/AddIns
04/04/2014	15:41:55	MAC	FILE	NTFS $MFT	$SI [MAC] time	-	/Users/keiko/AppData/Local/Microsoft
04/04/2014	15:41:55	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	/Users/keiko/AppData/Roaming/Microsoft/Excel
04/04/2014	15:41:55	...B	FILE	NTFS $MFT	$SI [...B] time	-	/Users/keiko/AppData/Local/Microsoft/Office

② 開いたファイル

date	time	MACB	source	sourcetype	type	user	desc
04/04/2014	15:37:11	MACB	REG	RecentDocs key	File opened	keiko	Recently opened file of extension: .JPG - value: hq-1.JPG
04/04/2014	15:42:58	MACB	REG	RecentDocs key	File opened	keiko	Recently opened file of extension: .xlsx - value: SJK大学教員マスター名簿.xlsx
04/04/2014	15:43:17	MACB	REG	RecentDocs key	File opened	keiko	Recently opened file of extension: .xls - value: SJK大学職員マスター名簿.xls

推測される被害
「SJK大学教員名簿」、「SJK大学職員名簿」が、ユーザー(keiko)を名乗る利用者によって、Excelで開かれた。

3. 推測される被害状況のまとめと今後の対策

解析結果（推測）のまとめ

1. 不正と推測されるプログラムはどれか？

2. 侵入経路はどこか？

3. 標的型攻撃である可能性がある場合、その根拠を示せ

今後の対策

4. 推測される被害は？

5. 被害拡大防止のためには、何をすべきか？

6. 次に何を調べるべきか？