

日本を襲った大規模な攻撃活動の実態

～ Backdoor.Emdiviによるサイバースパイ活動 ～

マクニカネットワークス株式会社
セキュリティ研究センター
政本 憲蔵

- 政本 憲蔵（まさもと けんぞう）
- <http://blog.macnica.net/>
- 暗号関連製品、WAF、IDS/IPS、マルウェア対策製品等の導入設計担当を経て、セキュリティインシデントの調査・分析を実施
- 海外のセキュリティ対策のトレンドを調査（米国、イスラエルを中心に）
- 各種セキュリティセミナーでの講演活動
- 好きな分野： OSINT、サイバーインテリジェンス、Webアプリケーションセキュリティ

blog.macnica.net

マクニカネットワークス セキュリティ研究センターブログ

弊社のブログ記事も合わせてご覧ください。

<http://blog.macnica.net/blog/2014/11/post-fca5.html>

<http://blog.macnica.net/blog/2015/01/post-39d4.html>

<http://blog.macnica.net/blog/2015/06/emdivi-201405-eea5.html>

◀ 2015年6月 ▶

日	月	火	水	木	金	土
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

カテゴリ

APT

Webアプリケーション

イベント

インテリジェンス

セミナー

ツール

トレンド

マルウェア

多層防御

標的型攻撃

2015年6月 8日 (月)

Emdivi を使う攻撃者の素性

世間で大きく報道されているマルウェアEmdivi (エムディヴィ) やCloudyOmega (クラウドイオメガ) に関連する件において、被害組織に対する非難の報道が多い一方で、本当に非難するべき対象は攻撃者であり、攻撃者に関する情報がほとんど報道されていないように見受けられます。この状況を少しでも変えるべく、弊社が把握している情報を、差支えない範囲で共有させていただきます。

[続きを読む](#)

投稿者 MASAMOTO 日時 2015年6月 8日 (月) 12:01 APT, インテリジェンス, マルウェア, 標的型攻撃 | [個別ページ](#)

いいね! 305 Tweet 83 8+1 4 23

2015年4月 1日 (水)

「Scanbox」が日本を偵察中

去年8月に米国AlienVault社のブログ(*1)で報告されたScanboxという偵察ツールがあります。これは、JavaScriptだけで書かれた偵察ツールで、Webサイトへ訪問しただけで、OS、ブラウザ、ウイルス対策ソフトを含む各種ソフトウェアの種別やバージョン情報が収集されてしまうものですが、弊社では、去年の秋くらいから、このツールが日本でも使われたことを数件確認しています。

[続きを読む](#)

プロフィール



セキュリティ研究センター



サイバーセキュリティに特化し研究することを目的として2013年4月に開設。

■ミッション

- ・サイバー攻撃の研究
- ・海外の最先端セキュリティ技術の発信
- ・予測的な策を講じるセキュリティ対策に基づいた包括的なソリューションの提案

[講演・メディア掲載情報はこちら](#)

Emdiviが添付された標的型攻撃メール

差出人: @yahoo.co.jp
 宛先: .co.jp **フリーメール (Yahooメール or Exciteメール)**
 CC:
 件名:  (日開催) の議事録送付

✉ メッセージ 📎 2015  .zip (176 KB)



ZIP or LZH

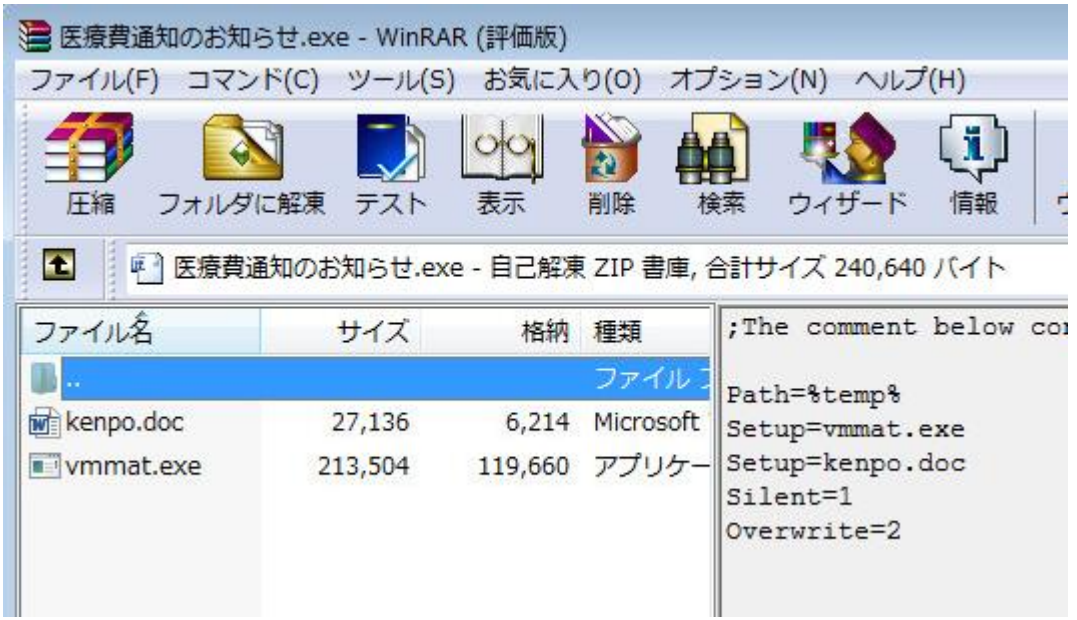
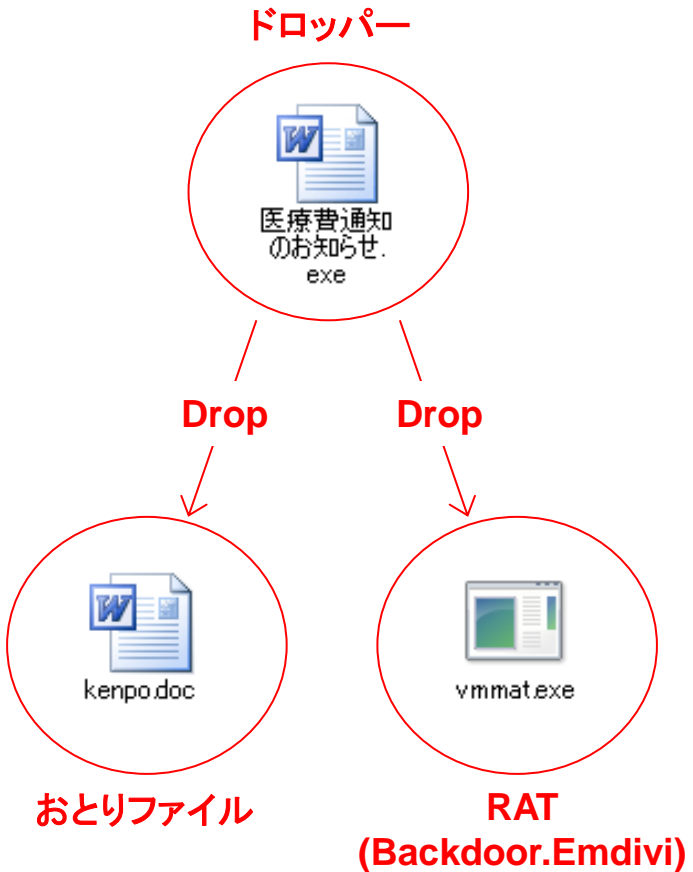
 各位

1月  の議事録を送付いたします。

何かお気づきの点等ございましたら、
 お手数ですがご連絡をお願いいたします。

 会

Tel:  Fax: 



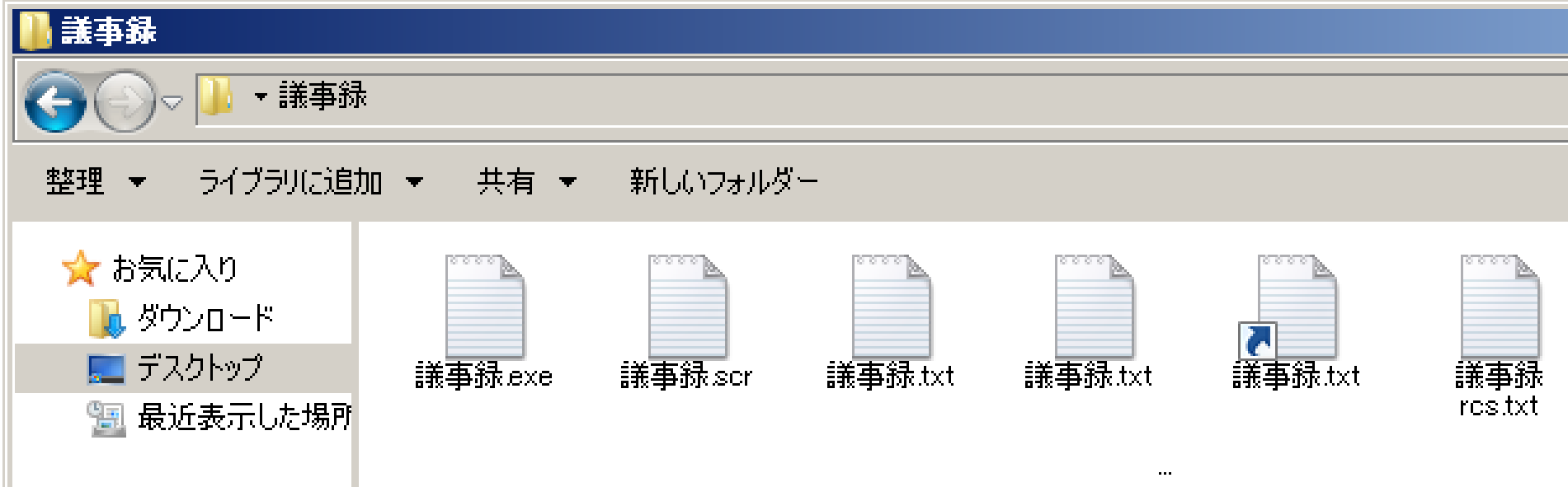
RARの圧縮ファイル(自己解凍形式)

RAT = Remote Access Trojan/Tool

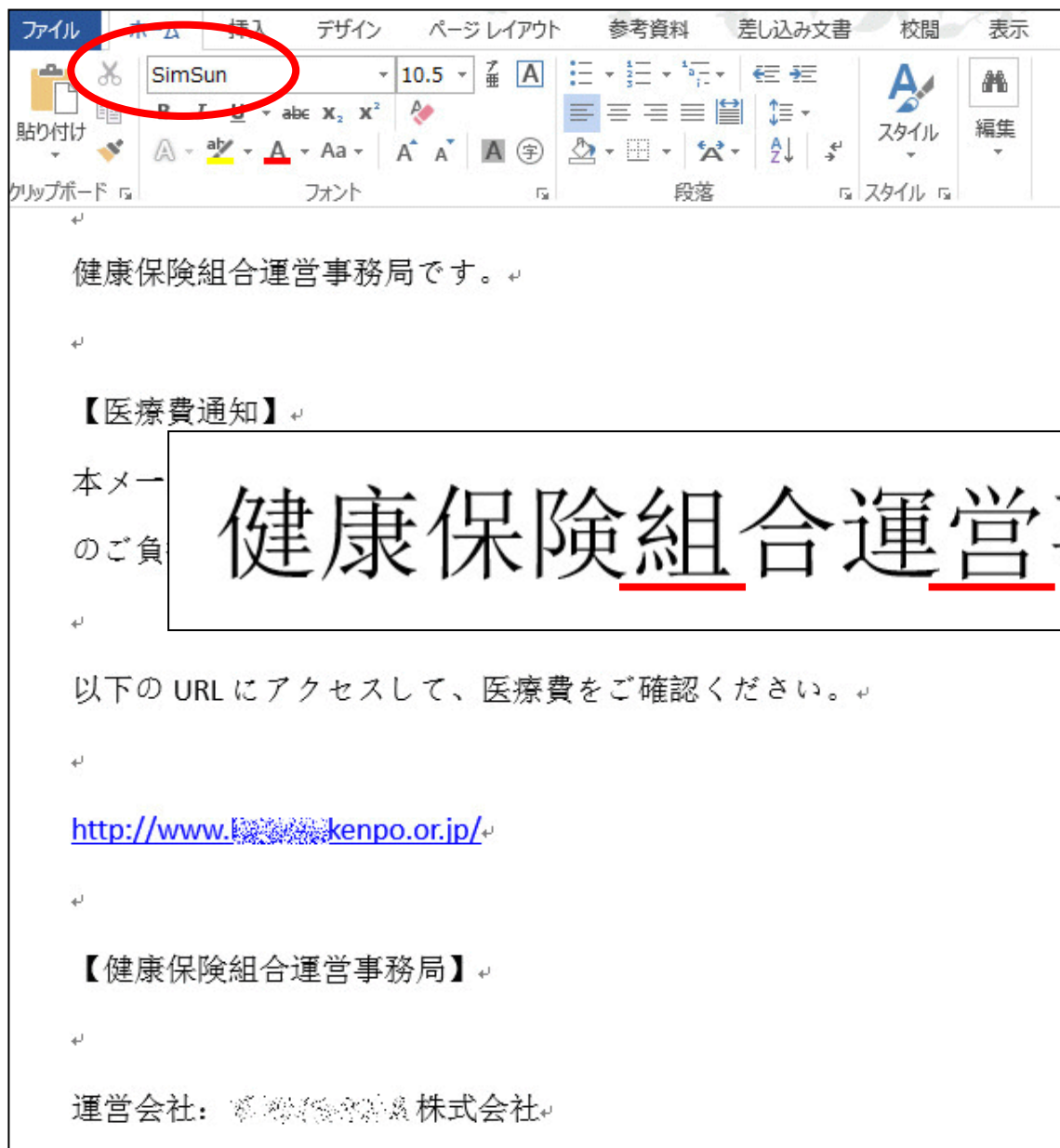


- アイコンを偽装（PDF、Word、Excelなどのドキュメントを装う）
- 実行ファイル(exe)

クイズ！ 開いても安全なファイルはどれ？



おとりファイル



健康保険組合運営事務局です。

【医療費通知】

本メー
のご負

健康保険組合運営事務局です。

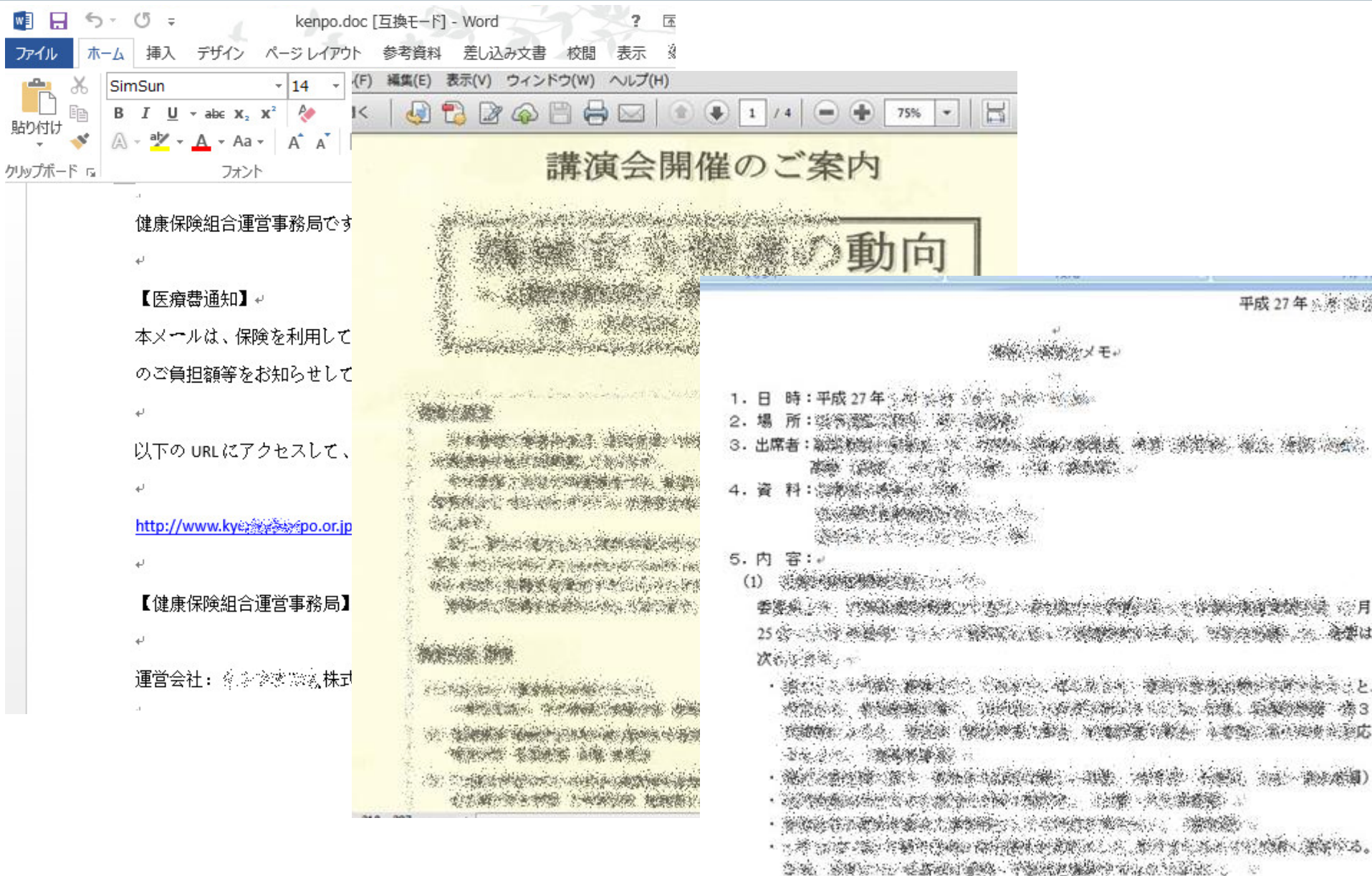
以下の URL にアクセスして、医療費をご確認ください。

<http://www.kenpo.or.jp/>

【健康保険組合運営事務局】

運営会社: 株式会社

おとりファイル



- 医療費通知のお知らせ
- セミナーへの参加申込書
- 収支計算書
- 社員向けの保険金配当の案内
- 懇談会、講演会、勉強会、協議会の案内
- 複数社間の打ち合わせ議事録
- GW休日と緊急連絡先の一覧表
- 韓国沈没船に関する情報

Emdivi ドロPPERに残された痕跡

The screenshot shows a Windows Resource Explorer window with three overlapping instances. The foreground instance displays a tree view of resources for a file named '101 [中国語 (简体字、中国)]'. The tree includes folders like 'Dialog' and 'Icon', and various string resources such as 'ASKNEXTVOL', 'GETPASSWORD1', 'LICENSEDLG', 'RENAMEDLG', 'REPLACEFILEDLG', and 'STARTDLG'. The 'STARTDLG' resource is selected.

Overlaid on the Resource Explorer is a WinRAR dialog box titled 'WinRAR 自解压文件'. It contains a table of resources:

ID	String
100	选择目标文件夹
101	正在解压 %s

Below the table, there is a text input field for '目标文件夹 (D):' with a '浏览 (W)...' button. An '安装进度' (Installation progress) bar is visible below that. At the bottom of the dialog are '安装' (Install) and '取消' (Cancel) buttons.

Backdoor.Emdiviの検体 (2015年3~4月)

Stirling - [vmatam_exe]

ファイル(E) 編集(E) 検索・移動(S) 設定(O) ウィンドウ(W) ヘルプ(H)

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0002E850	54	00	00	00	53	45	52	56	45	52	20	45	52	52	4F	52	T...SERVER ERROR
0002E860	00	00	00	00	43	48	45	43	4B	53	55	4D	20	45	52	52CHECKSUM ERR
0002E870	4F	52	00	00	3A	00	2F	00	2F	00	00	00	3B	00	00	00	OR...:/./.....
0002E880	5C	66	75	63	6B	2E	79	6F	75	2E	73	79	6D	74	65	63	¥fuck.you. [REDACTED]
0002E890	00	00	00	00	50	00	52	00	4F	00	58	00	59	00	00	00P.R.O.X.Y...
0002E8A0	6D	??	??	??	??	??	??	??	??	??	??	??	??	??	77	33	mW74P...IVOf...iw3
0002E8B0	48	??	??	??	??	??	??	??	??	??	??	??	??	??	68	30	HW...8h0
0002E8C0	30	??	??	??	??	??	??	??	??	??	??	??	??	??	00	00	OM... ..
0002E8D0	71	??	??	??	??	??	??	??	??	??	??	??	??	??	50	72	qS...MWP r
0002E8E0	4A	??	??	??	??	??	??	??	??	??	??	??	??	??	65	4C	Ja...3feL
0002E8F0	41	??	??	??	??	??	??	??	??	??	??	??	??	??	71	41	AT...3qA
0002E900	75	??	??	??	??	??	??	??	??	??	??	??	??	??	00	00	uR... ..
0002E910	79	??	??	??	??	??	??	??	??	??	??	??	??	??	51	2F	yj...4Q/
0002E920	39	??	??	??	??	??	??	??	??	??	??	??	??	??	51	6B	9Q...4Qk
0002E930	67	5A	37	53	4D	51	6E	6D	6B	30	33	57	6E	74	61	42	e77SMQ...Wptar

0x0002E71E 上書 216576 Bytes SHIFT-JIS

体系化されたバージョン管理



```

ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF ^
00028B00 45 4E 20 46 49 4C 45 00 46 49 4C 45 20 4E 4F 54 EN FILE.FILE NOT
00028B10 20 46 4F 55 4E 44 00 00 53 4C 45 45 50 49 4E 47 FOUND..SLEEPING
00028B20 00 00 00 00 4E 4F 54 20 41 4C 4C 4F 57 45 44 00 ....NOT ALLOWED.
00028B30 63 6D 64 20 2F 63 00 00 2E 00 00 00 28 45 72 72 cmd /c.....(Err
00028B40 6F 72 29 00 2A 00 00 00 74 31 37 2E 30 38 2E 31 or).*...t17.08.1
00028B50 36 2E 00 00 44 00 49 00 52 00 45 00 43 00 54 00 6...D.I.R.E.C.T.
00028B60 0C 00 00 00 04 00 00 00 17 00 00 00 46 00 00 38 ....Gmf
    
```

2014年8月

```

ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF ^
0002E830 00 00 00 00 22 61 6E 6A 24 4C 31 22 61 6A 67 62 ...2ac4l12njb
0002E840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ni...
0002E850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Ny...LxB
0002E860 2F 2B 41 77 55 77 3D 3D 00 00 00 00 28 45 72 72 /+AwUw==....(Err
0002E870 6F 72 29 00 2A 00 00 00 74 31 37 2E 30 38 2E 32 or).*...t17.08.2
0002E880 36 2E 4B 45 4E 50 4F 30 32 30 32 00 44 00 49 00 6.KENPO0202.D.T.
0002E890 52 00 45 00 43 00 54 00 00 00 00 00 58 46 4B 52 R.E.C.T....XFKR
    
```

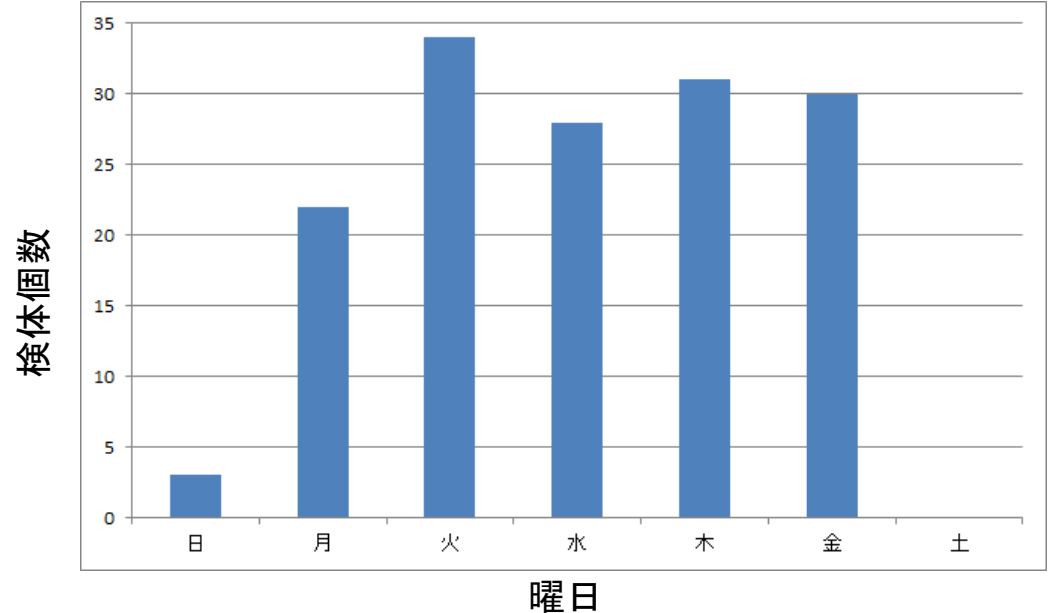
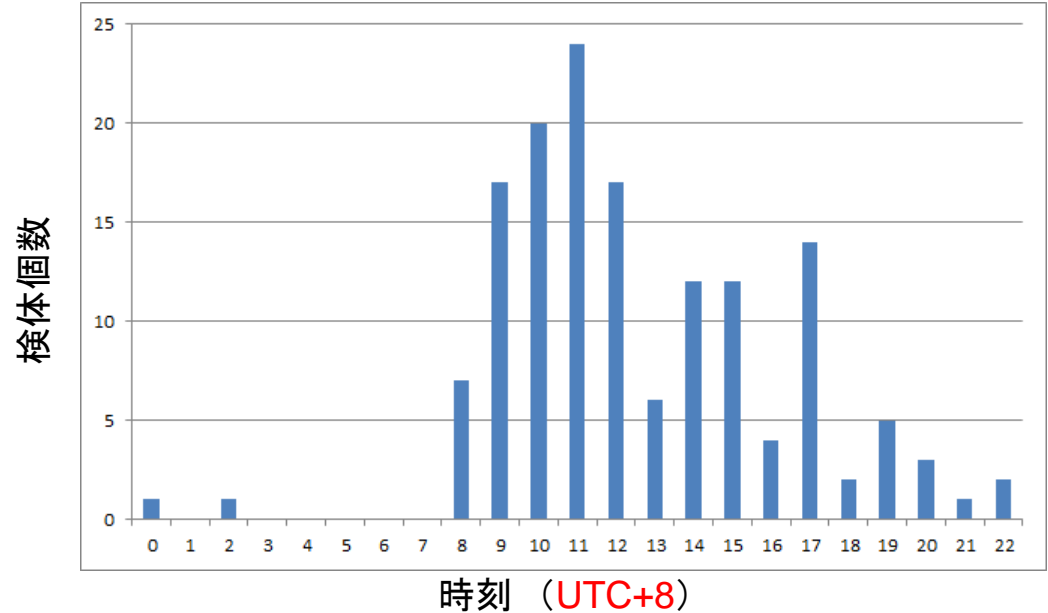
2015年1月

```

ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF ^
0003F130 46 41 49 4C 45 44 20 54 4F 20 4F 50 45 4E 20 46 FAILED TO OPEN F
0003F140 49 4C 45 00 46 49 4C 45 20 4E 4F 54 20 46 4F 55 ILE.FILE NOT FOU
0003F150 4E 44 00 00 53 4C 45 45 50 49 4E 47 00 00 00 00 ND..SLEEPING....
0003F160 4E 4F 54 20 41 4C 4C 4F 57 45 44 00 63 6D 64 20 NOT ALLOWED.cmd
0003F170 2F 63 00 00 50 4F 53 54 00 00 00 00 74 31 37 2E /c..POST...t17.
0003F180 30 38 2E 33 31 2E 44 47 66 6C 61 73 68 30 37 31 08.31.DGfIash071
0003F190 34 00 00 00 2F 00 00 00 56 75 6A 54 66 69 59 34 4...W...V4
0003F1A0 3C 00 00 00 04 00 00 00 00 00 00 3D 3D 9St...=
0003F1B0 0C 00 00 00 05 00 00 00 00 00 00 47 50 ...P
0003F1C0 6E 00 00 00 30 00 00 00 00 00 00 00 00 00 kZl...
0003F1D0 45 00 00 00 05 00 00 00 00 00 00 38 62 ECk...ib
0003F1E0 41 72 70 43 77 67 3D 3D 00 00 00 00 28 45 72 72 ArpUw==....(err
0003F1F0 6F 72 29 00 2A 00 00 00 44 00 49 00 52 00 45 00 or).*...D.I.R.E.
0003F200 43 00 54 00 00 00 00 00 6B 73 30 54 77 37 37 6B C.T....ks0Tw77k
    
```

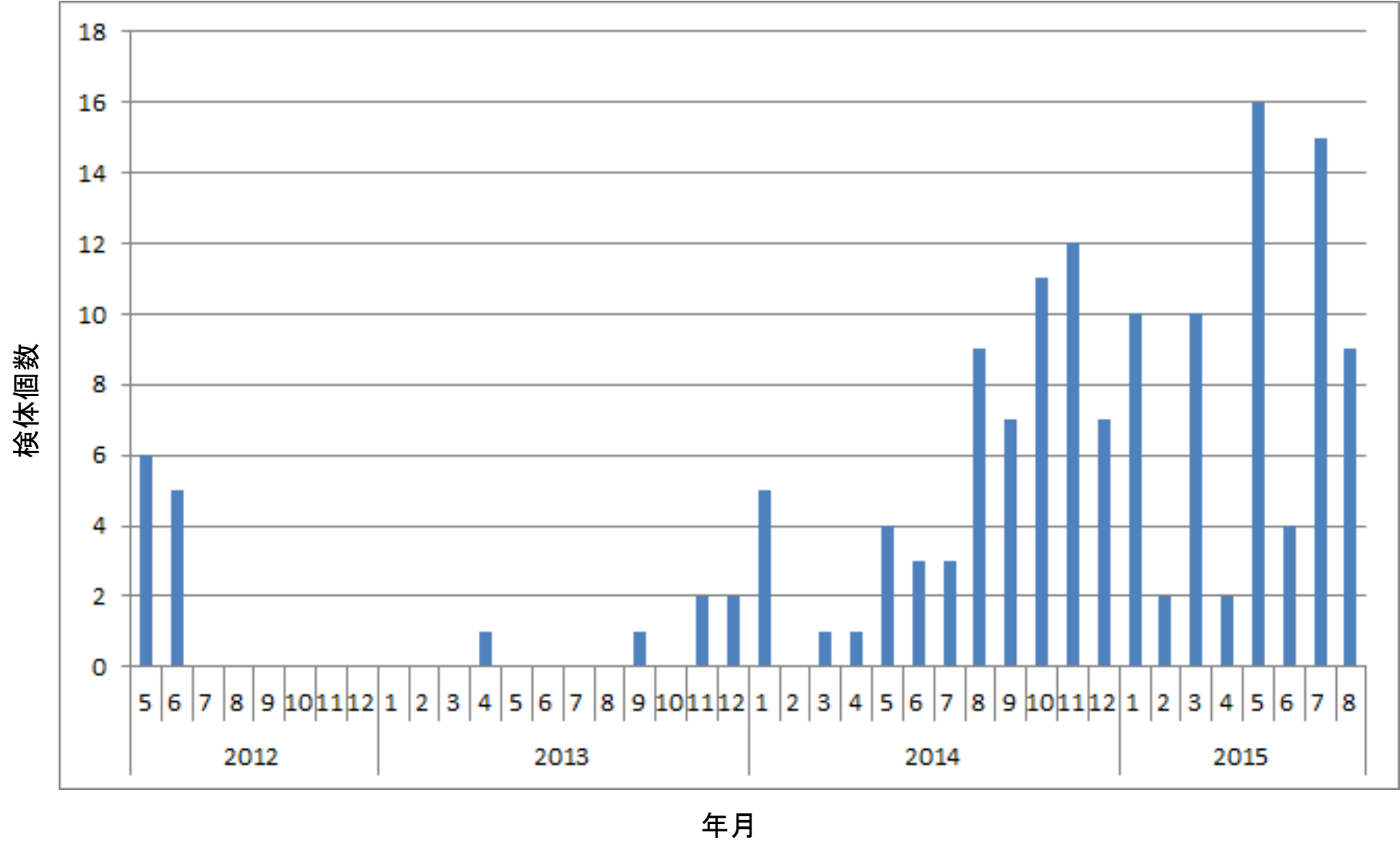
2015年7月

Emdivi RAT コンパイル時刻の分析 (時刻 & 曜日)



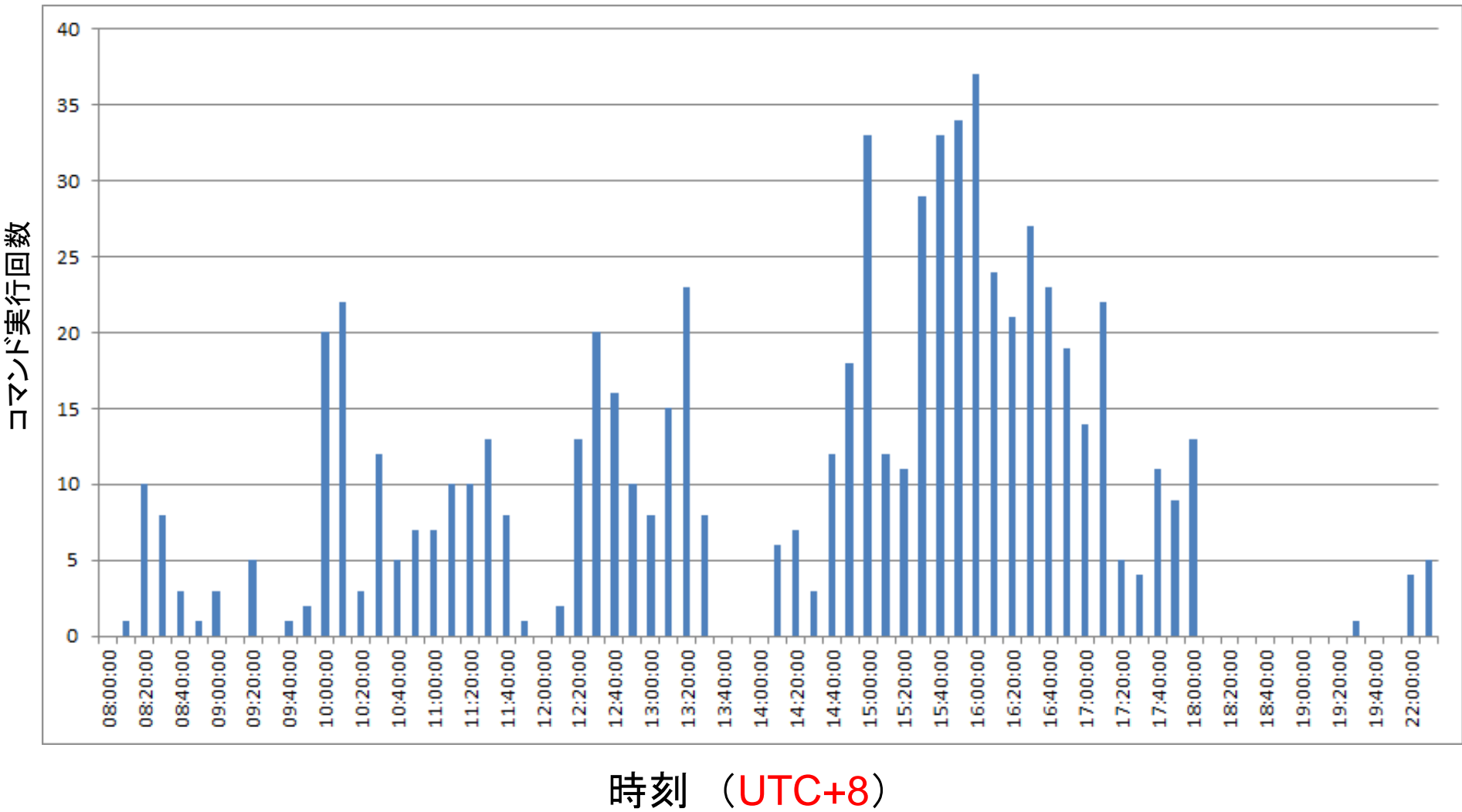
- 弊社で保有しているEmdivi RAT (148個、2015年11月4日時点)のコンパイル時刻を分析。
- UTC+8で見ると、一般的なサラリーマン・公務員の労働時間にほぼ収まる。
- 曜日で見ると、土日で作成されたRATがほとんどない。
- 個人によるものではなく、明確な目的を持った組織によって開発されたRATであると推測される。

Emdivi RAT コンパイル時刻の分析 (年月)



C&Cサーバ(指令サーバ)

ww[redacted]ill.jp	ww[redacted]pe.ne.jp	da[redacted]o.jp	ww[redacted]net.co.jp
ww[redacted]ye.com	ww[redacted]on.com	ww[redacted]ina.gr.jp	ww[redacted].com
ww[redacted]ne.com	ww[redacted].jp	ww[redacted]world.jp	ww[redacted]ss.com
ww[redacted]o.jp	ww[redacted]ya.jp	ww[redacted].co.jp	ww[redacted]ken.jp
hi[redacted]kura.com	ww[redacted]-ai.com	ww[redacted]san.biz	ww[redacted]ph.jp
ww[redacted]bm.com	ww[redacted]ing.co.jp	ww[redacted]os.jp	sr[redacted]o.or.jp
ww[redacted].jp	ww[redacted]ku.co.jp	ww[redacted]n.jp	ww[redacted]hip.co.jp
ww[redacted]e.co.jp	ww[redacted]nti.com	ww[redacted]to.jp	ww[redacted]arm.com
ha[redacted]dani.jp	mi[redacted]com	ww[redacted]fe.co.jp	ww[redacted]air.jp
ww[redacted]rd.co.jp	ww[redacted]-c.jp	ww[redacted]net.com	ww[redacted]aku.co.jp
ww[redacted]ne.jp	ww[redacted]tec.co.jp	ww[redacted]com.jp	ww[redacted]grm.jp
ww[redacted]prest.jp	ww[redacted]te.com	ww[redacted]o.biz	ww[redacted]ch.co.jp
ww[redacted]p.co.jp	ww[redacted]lom.com	ww[redacted]hori.com	ww[redacted]kan.jp
ww[redacted]no.jp	ww[redacted]ce.co.jp	ww[redacted].org.hk	jp[redacted].biz
ww[redacted]ye.co.jp	ww[redacted]uzin.com	ww[redacted]lin.info	ww[redacted]sub.com
ww[redacted]co.jp	ww[redacted]urin.or.jp	ww[redacted]to.co.jp	ww[redacted]cc.asia
ww[redacted]ome.co.jp	ww[redacted]ou.com	ww[redacted]sg.com	ww[redacted]s.com
ww[redacted]norei.com	ww[redacted]-fp.jp	ww[redacted]n.info	ww[redacted]golf.com
ww[redacted]gu.jp	ww[redacted]gr.jp	ww[redacted]ool.com	ww[redacted]nai.org
ww[redacted]esh.jp	ww[redacted]s.co.jp	ww[redacted]ng-sv.jp	



侵入後に使った内部偵察コマンド

- ipconfig /all
- net localgroup administrators
- net group "domain admins" /domain
- dir %logonserver%netlogon
- tasklist /v
- net view

```

c:\Users\%6>net group "domain admins" /domain
この要求はドメイン %4.co.jp のドメイン コントローラーで処理されます。

グループ名      Domain Admins
コメント        ドメインの管理者

メンバー

-----
7/20/2015 10:16:46 AM      7/20/2015 10:16:46 AM      Administrator
a\%6                        a\%4                        C:\%MIN
c:\%min                     d:\%in                      F:\%User
H:\%MIN                      H:\%min                     i:\%
i:\%min                      k:\%og                       m:\%n
m:\%min                      M:\%DA                       M:\%tor
o:\%min                      S:\%min

コマンドは正常に終了しました。

```

侵入後に使ったツール

```
C:\Users\user05> BrowserPasswordDump.exe
```

```
*****
```

```
Browser Password Dump v3.5 by SecurityXploded
```

```
http://securityxploded.com/browser-password-dump.php
```

```
*****
```

Browser	Username	Password	Website URL
Google Chrome	hoge@hogehogehoge.com	54321	http://213.149.189.100
Firefox	user123	testpass	http://www.100.100.100.100
Firefox	chama	1111	http://www.100.100.100.100
Firefox	guest	password	http://hoge.com
Internet Explorer	guest	testpwd1	http://www.100.100.100.100
Internet Explorer	user789	123456	http://www.100.100.100.100

```
C:\Users\%username%\AppData\Local\Thunderbird\Profiles\%profile%\mail_noArgv_final.exe
```

```
C:\Users\%username%\AppData\Local\Thunderbird\Profiles\%profile%\mail_noArgv_final.exe > type result.log
```

```
=====
Name           : test
Application    : Thunderbird
Email          : test@demo.com
Server         : 192.168.1.100
Server Port    :
Secured        : No
Type           : POP3
User           :
Password       :
Profile        :
Password Strength : Medium
SMTP Server    :
SMTP Server Port :
=====
```

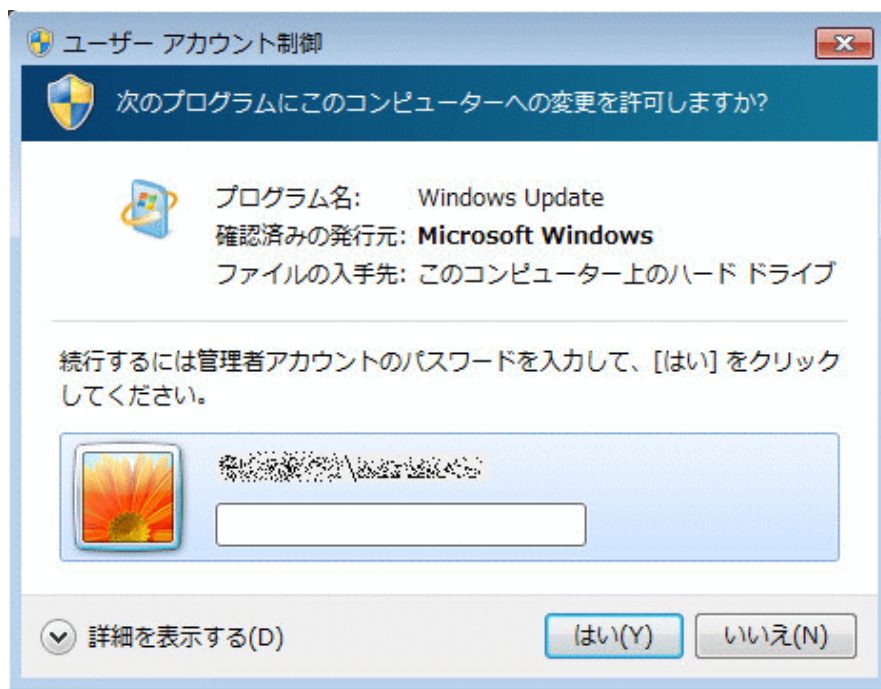
```
C:¥Users¥user05¥Desktop¥hoge>gp.exe
```

```
Authentication Id:0;107180  
Authentication Package:Kerberos  
Primary User:user05  
Authentication Domain:██████████
```

```
* User: user05  
* Domain: ██████████  
* Password: user05
```

- ファイル名: gp.exe、Gp64.exe、mimikatz.exe、mimikat.exe
- Mimikatzと呼ばれるパスワードダンプツールがカスタマイズされていた。
- Mimikatz以外のパスワードダンプツールも使われた。
 - wce.exe - Windows Credential Editor
 - gse_se.exe - gsecdump
 - QuarksPwDump.exe - Quarks PwDump

- ファイル名: msver.exe
- 偽のUAC(ユーザアカウント制御)ポップアップを表示し、パスワードの入力を促す。
- 入力されたパスワードは ps.txt へ書き込まれる。

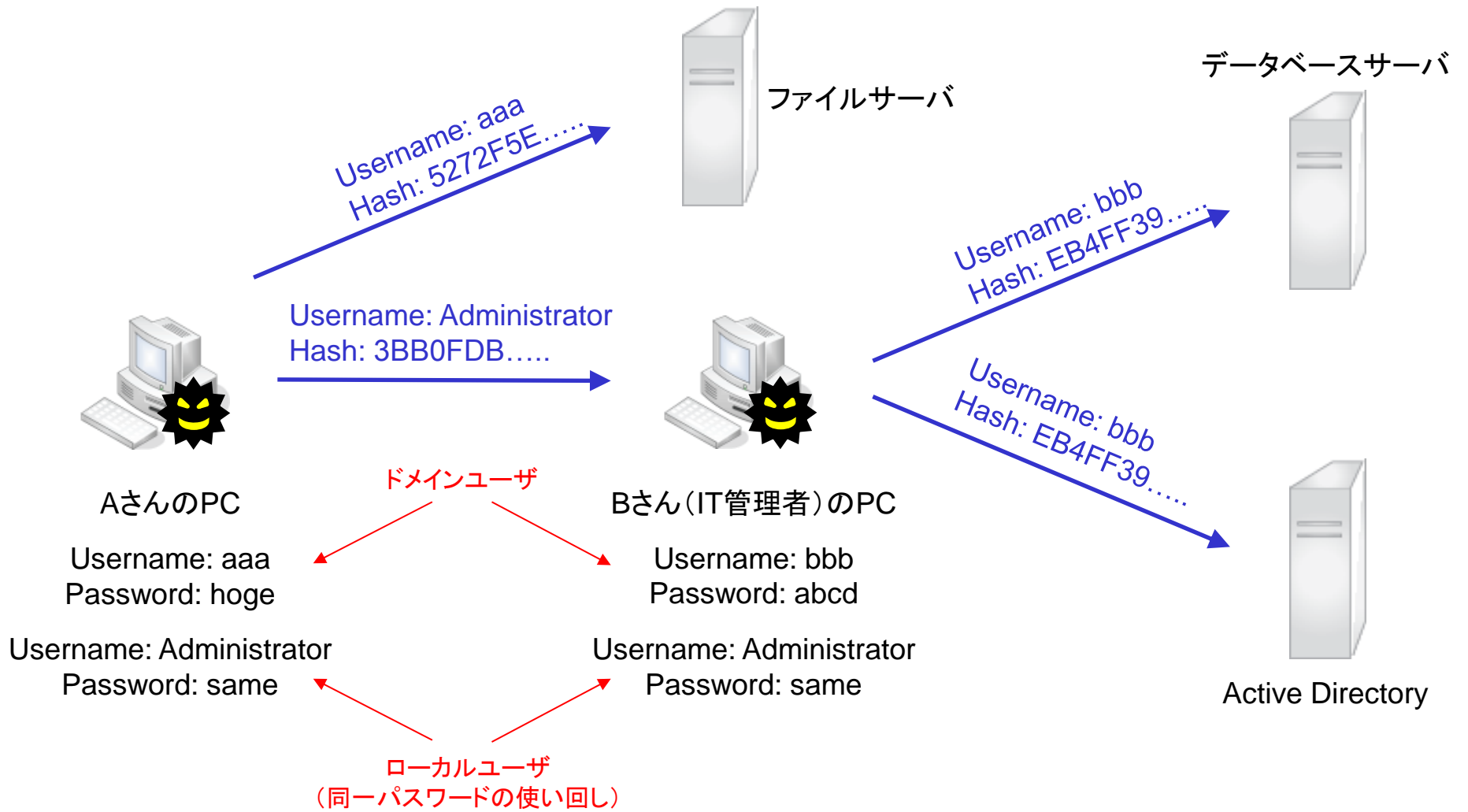


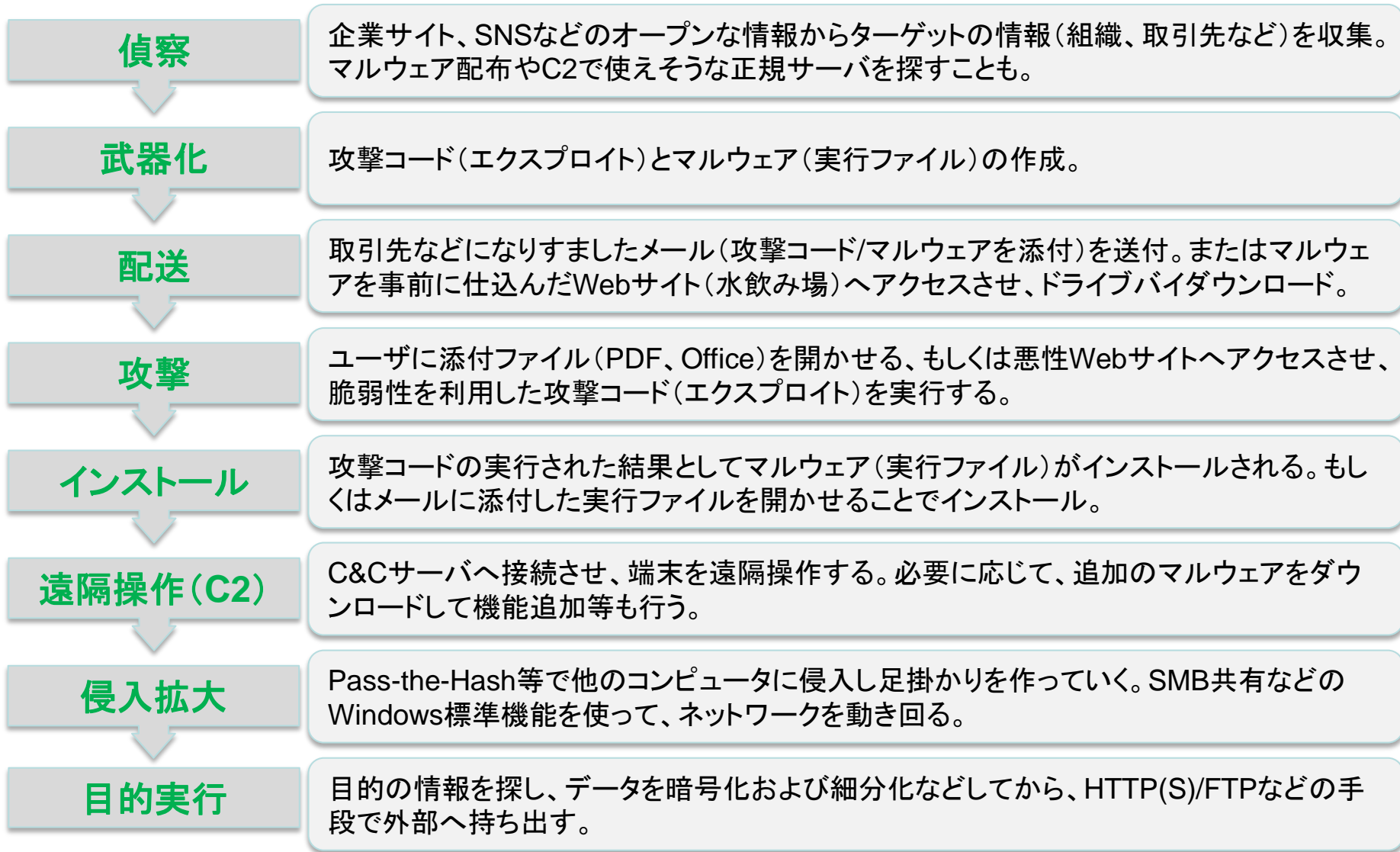
```
C:\Users\user05\Desktop\hoge>ms14-068.exe -u user05@xxxxxxxxxx.jp -s S-1-5-21-xxxxxxxxxx-12  
[+] Building AS-REQ for AD01... Done!  
[+] Sending AS-REQ to AD01... Done!  
[+] Receiving AS-REP from AD01... Done!  
[+] Parsing AS-REP from AD01... Done!  
[+] Building TGS-REQ for AD01... Done!  
[+] Sending TGS-REQ to AD01... Done!  
[+] Receiving TGS-REP from AD01... Done!  
[+] Parsing TGS-REP from AD01... Done!  
[+] Creating ccache file 'TGT_user05@xxxxxxxxxx.jp.ccache'... Done!
```

- Kerberos認証の脆弱性 (MS14-068 / KB3011780)
- ドメインコントローラへの攻撃
- 権限昇格が可能 (ドメイン管理者の権限を奪取)

■ Pass-the-Hash

- 他のシステムへハッシュのみを渡し、認証を突破して侵入する。





企業の為の サイバーセキュリティ Workshop

～攻撃者を知り、

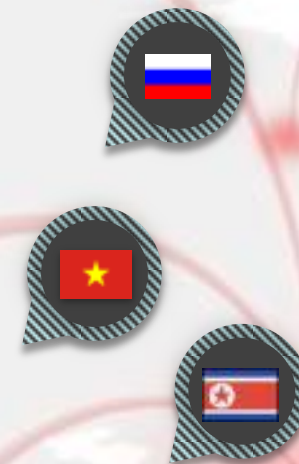
自社の弱点を把握して、

対策の本質を捉える！～

攻撃者のTTP (Tactics, Techniques, and Procedures) を理解することで、対策のあるべき姿が見えてくる！

Kill Chainの各フェーズにおける攻撃者のTTPを座学と演習を通して学ぶ！

- 会場：マクニカネットワークス株式会社 神奈川県横浜市港区新横浜 1 - 5 - 5
- 時間：10:00～18:00
- 定員：最大5名まで
- 参加費：¥100,000/人
- 対象者：自社のセキュリティ対策を企画、運用されているエンジニア
- 事前に持つておくべき知識
 - └ ネットワークに関する基本的な知識
 - └ Windowsに関する基本的な知識
 - └ Web、DNS、メールに関する基本的な知識



講師紹介



政本 憲蔵

2000年、マクニカに入社し、WAF、IDS/IPS、暗号製品、標的型攻撃対策ソリューションの設計・導入等の業務に携わる。顧客で見つかった脅威の解析を行う傍ら、セキュリティイベントでの講演やブログでの情報発信を行う。



凌 翔太

クライアントセキュリティ対策製品、IPS/IDSおよびWAFなどのネットワークセキュリティに関する製品を担当する傍ら、マルウェアや脆弱性の研究を実施する。Black Hat USA 2013 & 2014で自作のマルウェア・シミュレータを発表。

ご清聴ありがとうございました。

研究センターのブログをご覧ください。

<http://blog.macnica.net>

重要インシデントの分析や最新セキュリティ技術など、
Actionableな情報を発信！



具体的なセキュリティ対策ソリューションを
取り扱っておりますので、ご相談下さい。