Understanding
Your Opponent Attack Profiling

Moonbeom, Park
Deputy General Researcher
TTPA of South Korea

Yongjun, Park
Manager, Incident Investigation Part
FSI-CERT
Who are we?
Introduction

• Moonbeom, Park
• TTPA (Trust Third Party Agency) of South Korea
• Deputy General Researcher
• Hacking & Analysis, Digital Forensic & Profiling
• Ekoparty, TROOPERS, HITCON, VXCON and RedPill
Introduction

- Yongjun Park
- CERT, Financial Security Institute
- Manager
- Incident Response and Threat Intelligence for Financial Industry in Korea
- Always welcome International cooperation and research
Attack Profiling
Attack Profiling

- Goal
  - Understand attacker’s TTPs and forecast next target and plan
    - Invest resource in particular area and reinforce monitoring to reduce damage of attack
  - Trace Actor and Group
    - Incident investigation for different incident
    - Analyze connection and similarity between incidents

A part of incident response and investigation procedure
Attack Profiling

- Common Factors
  - Tactics
  - Code
  - Server, IP and domain
  - Tools and Exploits
  - Language and sentence
  - A bit of data using incident could help to profile
Case study for tactics and plan

Profiling
DD4BC DDoS to Financial Service

- DD4BC (DDoS for Bitcoin)
  - DDoS Attacked to Banks and Securities In South Korea
  - Initial DDoS (NTP, SSDP, other Amplification and Reflection)
    + Sending Black Mail (Asking Bitcoin and warning massive DDoS bigger than Initial attack)
  - DDoS on every Friday target to Financial Institution.
  - Which bank will be a next Target
Government run Banks

Nationwide Banks

Regional Local Banks

Foreign Banks

Not a good target

Market Leader. But, not included

Regional Business. Small Market

IT System located in Foreign Country
DD4BC DDoS to Financial Service

• Find Next Target

  • Target Banks were Regional local bank, not a major and market leading bank… why?
  
  • They have huge targets in worldwide
    - How they can find information for their target company and system
    - Guess it, no partner, find general information
**Answer is Wikipedia**

List of banks in South Korea

This is a list of South Korean banks. The parenthesized number is the bank number.

This list is incomplete; you can help by expanding it.

Central bank

- Bank of Korea (001)

Government-run banks

- KDB Financial Group
  - Korea Development Bank (002)
  - Industrial Bank of Korea (003)
  - Korea Eximbank (008)

Nationwide banks

- Citigroup Korea
  - Citibank Korea (027)
- Hana Financial Group
  - Hana Bank KEB Hana Bank (005)(081)
- KB Financial Group
  - KB Kookmin Bank (004)
- Standard Chartered
  - Standard Chartered Korea (023)
- Shinhan Financial Group
  - Shinhan Bank (088)
- Woori Financial Group
  - Woori Bank (020)

Local banks

- DGB Financial Group
  - Daegu Bank (031)
- BNK Financial Group
  - Busan Bank (032)
  - Kyongnam Bank (039)
- JB Financial Group
  - Kwangju Bank (034)
  - Jeonbuk Bank (037)
- Shinhan Financial Group
  - Jeju Bank (ko) (035)
Next Attack, in trouble?

- Target were moving to Securities Institutions, BAD...
- There was no Wikipedia page for Securities, 2nd BAD... But,
- There is no partner in South Korea. But, need general information.
DD4BC DDoS to Financial Service

- Google(Securities in Korea)

Korea Investment & Securities (KIS)
www.koreaholdings.com/eng/sub/sub1.html
Korea Investment & Securities Co., Ltd. (KIS) was re-formed in June 2005 through the merger of the former Korea Investment & Securities Co. (KITC) with Dongwon Securities. ... The merger has allowed KIS to develop a well-balanced revenue structure consisting of asset management ...
You've visited this page 3 times. Last visit: 8/3/16

KSD(Korea Securities Depository)
https://www.ksd.or.kr/eng/index.home
KSD, Participating in Hyperledger Blockchain Project 2016 08 09; Settlement status of foreign securities
(2016 first half) 2016 08 03; KSD Newsletter Volume 108 ...

BNP Paribas Securities Korea - BNP Paribas South Korea
www.bnpparibas.co.kr › Home › Corporates & Institutions
BNP Paribas Securities Korea provides financial investment services for Local and Foreign Institutional Investors, Corporates, and Financial Institutions.

Banks and Securities Firms List - South-Korea - korea4expats
www.korea4expats.com/article-list-banks-securities-korea.html
Mar 19, 2014 - Following is a list of banks and financial institutions in Korea.

NH Investment & Securities - NH농협금융
www.nhfgroup.com/Eng/affiliates/subsidiary_4.aspx
Greeting, 김험규, NH Investment & Securities has been leading the Korean securities industry by performing a pivotal role in the growth and development of the ...

Mirae Asset Securities
securities.miraeasset.co.kr/eng/jsp/main.jsp
contact us; site map; korea; company; business ... Korea NDR (April, 2013) · · Korea NDR (December, 2012) · · UBS Conference (June, 2012). ©1997 to 2008 ...
Case study for Code Profiling
APT to IT Solution Provider

- Compromised IT solution providers and exploit 0-day of solution for massive attack
  - Detected Malware code-sign with legitimate certificate
  - Well known IT solution provider in South Korea
  - Using several 0-day to attack Government, Financial Service, Media, Education, Medical and R&D
APT to IT Solution Provider

Client Security Solution ('B' Solution Provider)

0-day #1

Attacker

'A' Solution Provider

C&C

Canada University(KR)
Kindergarten(KR)
Catholic Broadcasting(KR)

Malware Code-Sign with 'A' solution certificate

'Another Incident'

IT management Solution ('C' Solution Provider)

0-day #2

Scan and Exploit with 0-day #1, #2

Government
Financial
Large Scale Company
others
APT to IT Solution Provider

- Connection with another incident
  - This incident related with APT incident in 2015
    - ADEX (Seoul International Aerospace & Defense Exhibition)
  - Spear-phishing target to ADEX 386 participating company (Military and Defense)
  - Send E-mail include .xls file (Macro downloader) pretended to be a exhibition organizer
APT to IT Solution Provider

- Similarity and common
  - File Delete Command
  - Directory, Registry
  - C&C
  - PDB path
APT to IT Solution Provider

Delete Command
APC to IT Solution Provider

Malware Directory
APT to IT Solution Provider

Registry
APT to IT Solution Provider

C&C server

158.69.

[Map showing location of 158.69, United States, Lake Forest]
APT to IT Solution Provider

PDB Path in PE info
- Debug information
APT to IT Solution Provider

- That’s all?
- More connections?

- Who will attack military and defense company in South Korea
- ADEX incident is related with Sony Picture incident

- Find out connections between incident, and then figure out actor from these connections
National Cyber Warfare Organization
North Korean Cyber Warfare Organization

- Where are South and North now?
  - Spent more than 60 years with cold war since 1950s
  - Both nations use various ways to collect information (espionage agent etc)
  - Recently, hack to collect info.
  - South Korea = well developed with massive IT infrastructures and industries
  - North Korea = categorized as 3rd world nation
North Korean Cyber Warfare Organization

• OOO Lab
  • Specialized in radio disturbance & overseas intelligence group hacking
  • Specialized in public & military sector related information
  • Abuse HWP, PDF, PPT vulnerability
  • Hacked SONY Picture in 2014
  • Hacked Korea Hydro & Nuclear Power Co., Ltd in 2014
  • Many South Korea government agency hacked by OOO Lab
North Korean Cyber Warfare Major Strategy and Method of Attack
North Korean Cyber Warfare Major Strategy and Method of Attack

- **Spreading Malicious code using website**
  - Targets are South Korean news media websites
  - Target lists are based on the information of website hits count
  - Technics are Drive by Download & Watering Hole
  - Abuse Active-x vulnerability which most of South Korean website are using
  - Reuse same webshell
  - Use 175.45.000.000
North Korean Cyber Warfare Major Strategy and Method of Attack

- Use Spear Phishing (targeted attack) with HWP 0-day vulnerability
  - HWP (Korean word processor) is most popular word processor in South Korea
  - 0-day vulnerabilities were found when HWP API was released
  - All of South Korean Government/state owned companies are using HWP
  - Hacked South Korean nuclear power plant in Dec. 2014
Case study related North Korea cyber warfare
Case study related North Korea cyber warfare

- Broadcasting station cyber terror (Dark Seoul, 2013. 3)

1. Attack and create Flash 0-Day Exploit page
2. Attack and create Dropper down page
3. Access to Flash 0-Day Exploit page
4. Dropper download and execute
5. Malware upload
6. Execute malware and disk distory 2013. 3. 20. 14:00
7. Transmit malware to internal PC 2013. 3. 20. 08:00
Case study related North Korea cyber warfare

- Sony Pictures Entertainment (2014. 10)

1. Attacker
   - Sending a spear phishing mail attached malware

2. E-mail
   - After opening a mail, being infected malware

3. SPE Staff’s PC
   - Searching shared folder and Cracking id/pass

4. C&C Server (Thailand)
   - Data leaked on infected PC

4. Server
   - Sending C&C server data leaked on infected PC
Case study related North Korea cyber warfare

- Korea nuclear power plant (2014. 12)

1. Attacker
2. HWP include malware
3. 2014. 8. 18 Downloaded from FTP Server
4. HncChecker.exe
5. 2014. 7. 7 Sent E-mail with an attached file (HWP)
6. SKT_N_XXXXXXX.avi
7. Access and control using TeamViewer
   TeamViewer ID: OOOOOOO
8. TeamViewer
9. FTP Server (UK)
10. FTP Server (KR)
11. comaddon.dll
12. Dropper Keylogger Encryptor Decryptor RAT
13. Attacker uploads to FTP Server
Profiling North Korean Cyber Warfare Group
Profiling North Korean Cyber Warfare Group

• Webshell
  • When hacking a web server, same webshell is always involved
  • North Korean hacker uses webshell called “dmc webshell”
  • This webshell is always found in victim web servers of North Korea
  • Developed in PHP language and use encrypted protocol when there is an execution command
Profiling North Korean Cyber Warfare Group
Profiling North Korean Cyber Warfare Group

- IP address that are being used by N.Korea
  - Thailand ISP called “Loxley”
  - Use 5 number of C-Class IP
    - 175.45.176.xxx
    - 175.45.177.xxx
    - 175.45.178.xxx
    - 175.45.179.xxx
    - 210.52.103.xxx
Profiling North Korean Cyber Warfare Group

• IP address that are being used by North Korea

175.45.00.00 - - [07/Jul/2015:17:20:41 +0900] "GET /files/env/list.php HTTP/1.0" 200 10099 "http://www.OOOOO.com/files/env/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 873

175.45.00.00 - - [07/Jul/2015:18:23:47 +0900] "POST /files/env/list.php HTTP/1.0" 200 13583 "http://www.OOOOO.com/files/env/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 30944

175.45.00.00 - - [08/Jul/2015:12:49:26 +0900] "POST /files/env/list.php HTTP/1.0" 200 11312 "http://www.OOOOO.com/files/env/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 29228
Profiling North Korean Cyber Warfare Group

- User Agent information of the N.Korea

- 175.45.17X.000
  - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
  - Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)
  - Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1
  - Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.4 (KHTML, like Gecko) Chrome/16.0.889.0 Safari/535.4
  - Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
  - Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
  - Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.52 Safari/537.4

- 175.45.17X.000
  - Mozilla/4.5 (compatible; HTTrack 3.0x; Windows 98)

- 175.45.17X.000
  - Mozilla/5.0 (Windows NT 6.2; rv:37.0) Gecko/20100101 Firefox/37.0
Profiling North Korean Cyber Warfare Group

• User Agent information of the N.Korea

- 175.45.000.000
  • Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
  • Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10
  • Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.17) Gecko/2009122116 Firefox/3.0.17
  • Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
  • Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.94 Safari/537.36
Profiling North Korean Cyber Warfare Group

- Malicious code similarity
  - North Korean cyber warfare group reuse previous malicious code
  - Malicious code encryption methods are same
  - System information gathering module codes are same
  - Keylogging module codes are same
  - Malicious code compile routes are very similar
Profiling N.Korean Cyber Warfare Group

- Malicious code reuse

```c
v2 = strchr(a1, 'Wn');
v3 = v2;
if ( v2 )
{
    v4 = v2 - a1;
    strncpy(a2, a1, v2 - a1);
    if ( a2[v4 - 1] == 'Wr' )
    a2[v4 - 1] = 0;
    result = v3[1] != 0 ? (unsigned int)(v3 + 1) : 0
}
else
{
    result = 0;
    strcpy(a2, a1);
}
return result;
```

< 3.20 Cyber terror in 2013 >

```c
v2 = strchr(Source, 'Wn');
v3 = v2;
if ( v2 )
{
    v4 = v2 - Source;
    strncpy(Dest, Source, v2 - Source);
    if ( Dest[v4 - 1] == 'Wr' )
    Dest[v4 - 1] = 0;
    result = v3[1] != 0 ? (unsigned int)(v3 + 1) : 0;
}
else
{
    result = 0;
    strcpy(Dest, Source);
}
return result;
```

< Sony Pictures hacking in 2014 >
Profiling N. Korean Cyber Warfare Group

- Malicious code reuse

```
lea    eax, [ebp+var_16C]
push   eax
push   ebx
lea    eax, [ebp+var_270]
push   offset aPm
push   eax
push   [ebp+Str1]
push   offset aXe
push   offset aCm
push   offset aSD_eScSS21
push   eax
push   var_16h
lea    eax, [ebp+var_24]
push   eax
lea    eax, [ebp+var_68]
push   eax
push   ebx
push   ebx
push   80000000h
push   ebx
lea    eax, [ebp+var_64h]
push   ebx
push   eax
push   ebx
push   ebx
call   dword 40AE68
lea    eax, [ebp+var_16C]
lea    eax, [ebp+var_16C]
push   eax
lea    eax, [ebp+var_64h]
push   [ebp+Str1]
push   offset aXe
push   offset aCm
push   offset aSD_eScSS21
push   eax
push   LPSTR
add    esp, 18h
lea    eax, [ebp+var_68]
push   eax
push   ebx
push   ebx
push   ebx
push   80000000h
push   ebx
push   ebx
lea    eax, [ebp+var_64h]
push   ebx
push   eax
push   ebx
push   ebx
call   dword 40AE68
lea    eax, [esp+80Ch+var_744]
push   edx
push   ebx
push   ebx
push   offset aPm
push   eax
push   [ebp+Str1]
call   dword 419CC0
lea    eax, [esp+88Ch+NewFileName]
push   eax
push   [ebp+Str1]
call   dword 419E8
mov    eax, [esp+88Ch+e]
lea    edx, [esp+88Ch+NewFileName]
push   edx
lea    eax, [esp+88Ch+var_64h]
push   offset aXe
push   offset aC
lea    eax, [esp+88Ch+var_64h]
push   offset aSD_eScSS21
push   eax
push   char *
call   _printf
add    esp, 18h
lea    edx, [esp+88Ch+var_89C]
lea    eax, [esp+88Ch+var_88C]
lea    eax, [esp+88Ch+var_64h]
push   edx
push   eax
push   ebx
push   ebx
push   ebx
push   ebx
push   80000000h
push   ebx
push   ebx
call   dword 419D00
lea    eax, eax
```

< APT Case 1 in 2014 >  < APT Case 2 in Jan 2016 >
THANK YOU!