Perfect Smoke and Mirrors of Enemy:

Following Lazarus group by tracking DeathNote campaign

Seongsu Park,
Lead security researcher @ GREAT

Seongsu Park

- Kaspersky, Global Research and Analysis Team
- Lead security researcher
- Tracking targeted attacks focused on APAC
- Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

Who is Lazarus?

Adversary

Lazarus

a.k.a Hidden Cobra, Zinc

Published by Novetta in 2014

Victim

Financial profit

Cyber espionage

Data theft

Capability

Various infection vectors

Multi-stage components

Several malware clusters

Infrastructure

Compromised server

Commercial hosting service

Origin of DeathNote

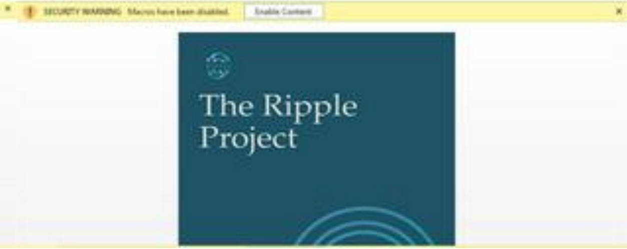
Manuscrypt

- Old Lazarus malware
- Connect to SPE hacking
- Had been used for several years without significant updates.

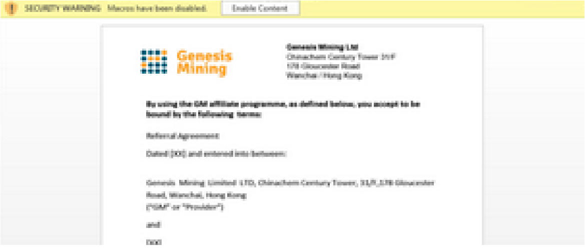
DeathNote (a.k.a DreamJob)

- Came across an updated version of the initial downloader.
- Implemented new techniques.
- Since Oct 2018

Oct 2019. Beginning of tracking DeathNote



The Ripple Project



Genesis Mining Ltd
Chinachem Century Tower 31/F
178 Gloucester Road
Wanchai / Hong Kong

By using the GM affiliate programme, as defined below, you accept to be bound by the following terms:

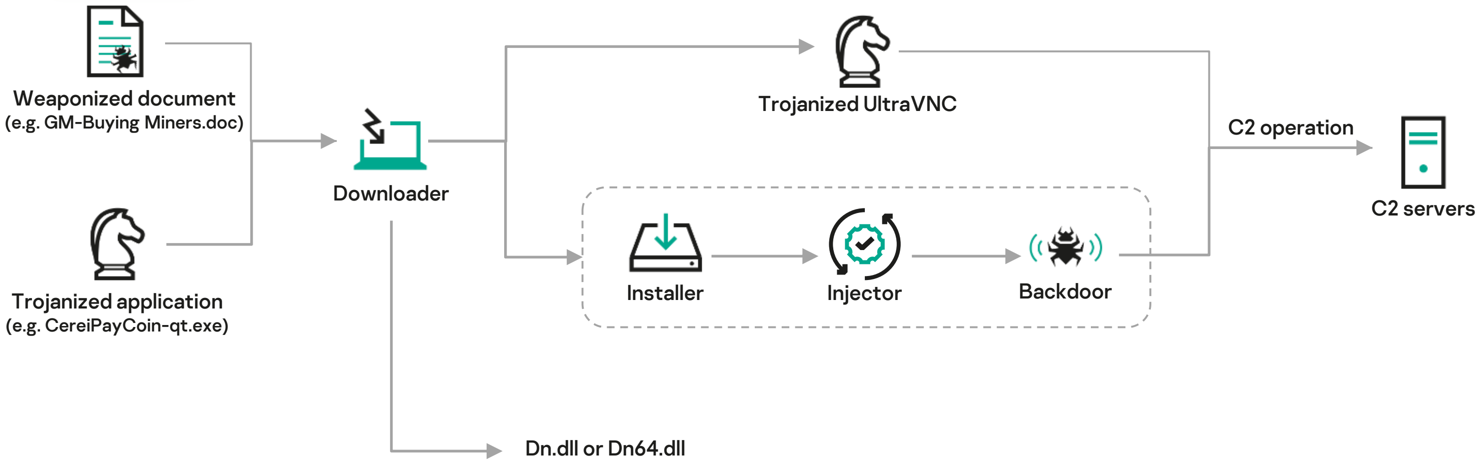
Referral Agreement

Dated [XX] and entered into between:

Genesis Mining Limited LTD, Chinachem Century Tower, 31/F,178 Gloucester Road, Wanchai, Hong Kong
("GM" or "Provider")

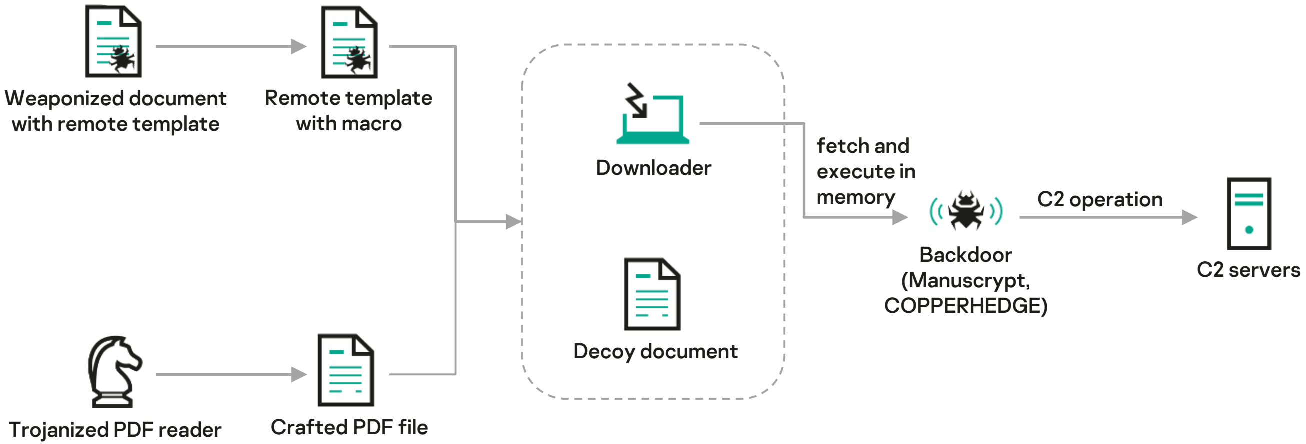
and

[XX]



Apr 2020. Shifting focus to the defense industry

US-ROK Relations and Diplomatic Security
한미관계와 외교안보
BOEING
Description
2020
Lockheed Martin Corporation
LOCKHEED MARTIN



Weaponized document with remote template

Remote template with macro

Downloader

Decoy document

fetch and execute in memory

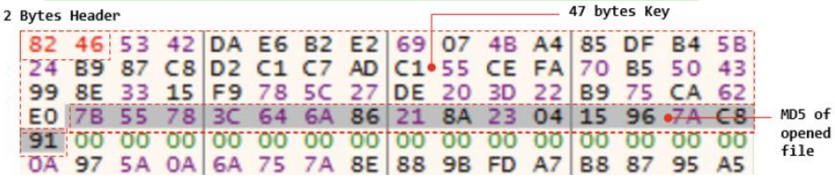
Backdoor (Manuscrypt, COPPERHEDGE)

C2 operation

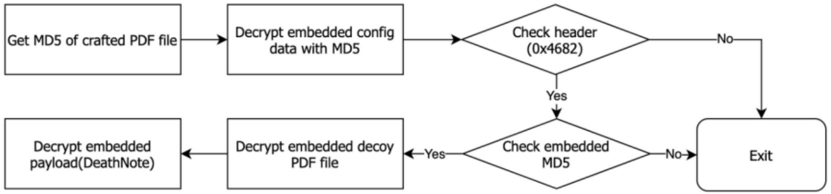
C2 servers

Trojanized PDF reader

Crafted PDF file



```
2 Bytes Header                                  47 bytes Key
82 46 53 42 | DA E6 B2 E2 | 69 07 4B A4 | 85 DF B4 5B
24 B9 87 C8 | D2 C1 C7 AD | C1 55 CE FA | 70 B5 50 43
99 8E 33 15 | F9 78 5C 27 | DE 20 3D 22 | B9 75 CA 62
E0 7B 55 78 | 3C 64 6A 86 | 21 8A 23 04 | 15 96 7A C8   MD5 of
91 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00   opened
0A 97 5A 0A | 6A 75 7A 8E | 88 9B FD A7 | B8 87 95 A5   file
```



Get MD5 of crafted PDF file

Decrypt embedded config data with MD5

Check header (0x4682)

No

Yes

Check embedded MD5

Yes

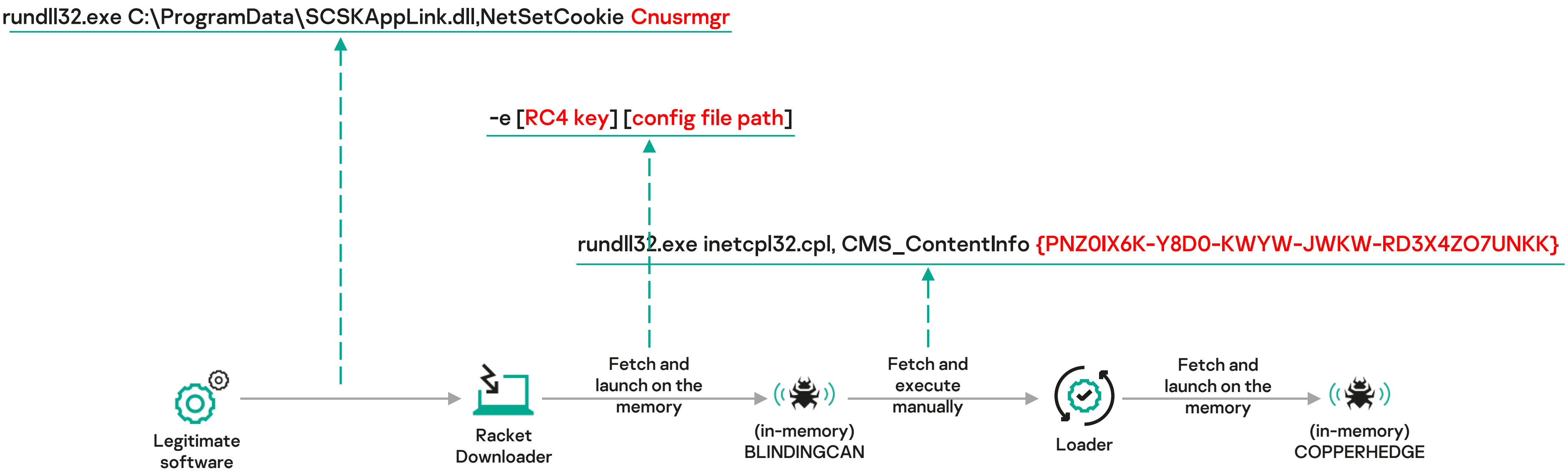
No

Decrypt embedded decoy PDF file

Decrypt embedded payload(DeathNote)

Exit

Jun 2021. Expanded target, adopted new infection vectors

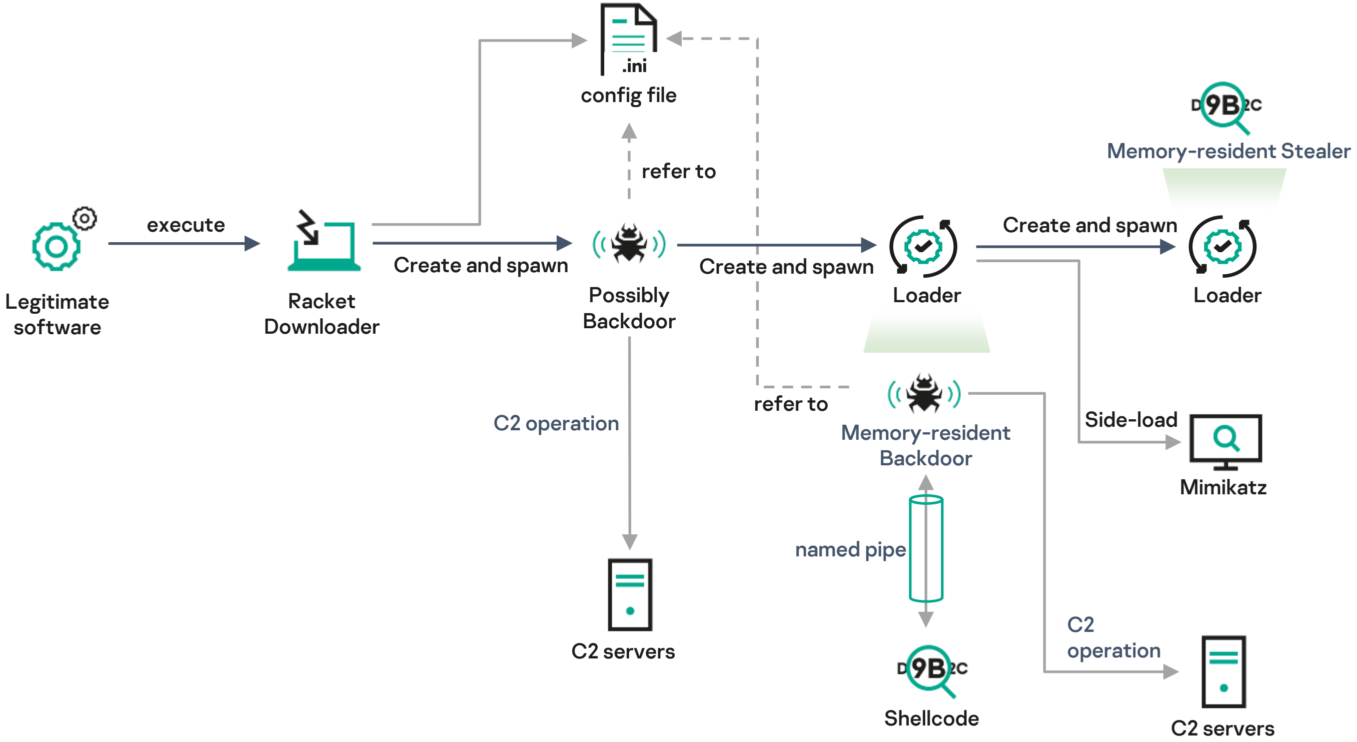


```
rundll32.exe C:\ProgramData\SCSKAppLink.dll,NetSetCookie Cnusrmgr
```

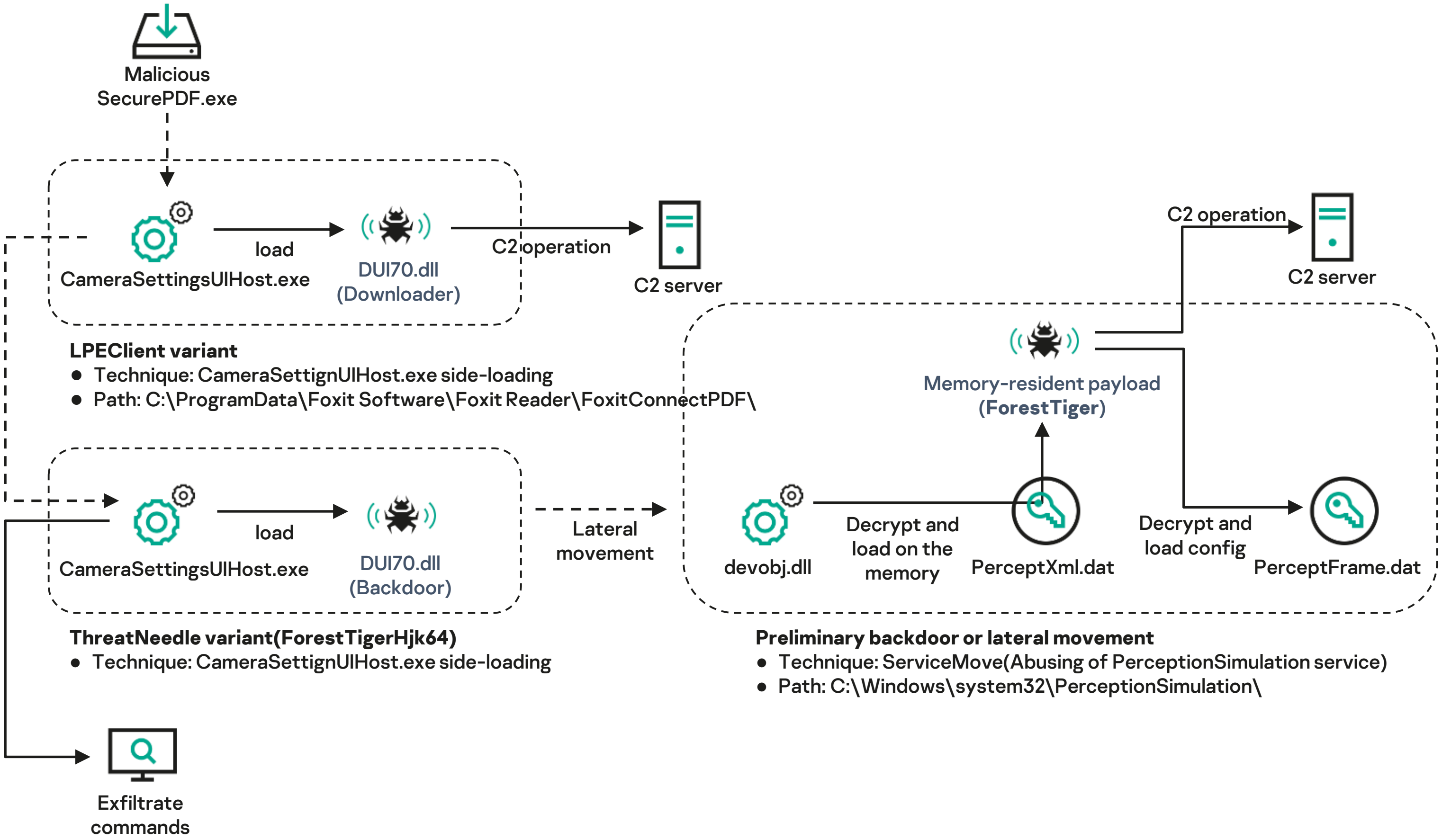
```
-e [RC4 key] [config file path]
```

```
rundll32.exe inetcpl32.cpl, CMS_ContentInfo {PNZ0IX6K-Y8D0-KWYW-JWKW-RD3X4ZO7UNKK}
```

March 2022. Same method with elaborate infection scheme



July 2022. Same method with elaborate infection scheme



Malicious SecurePDF.exe

CameraSettingsUIHost.exe

load

DUI70.dll (Downloader)

C2 operation

C2 server

LPEClient variant

- Technique: CameraSettignUIHost.exe side-loading
- Path: C:\ProgramData\Foxit Software\Foxit Reader\FoxitConnectPDF\

CameraSettingsUIHost.exe

load

DUI70.dll (Backdoor)

Lateral movement

ThreatNeedle variant(ForestTigerHjk64)

- Technique: CameraSettignUIHost.exe side-loading

Exfiltrate commands

C2 operation

C2 server

Memory-resident payload **(ForestTiger)**

devobj.dll

Decrypt and load on the memory

PerceptXml.dat

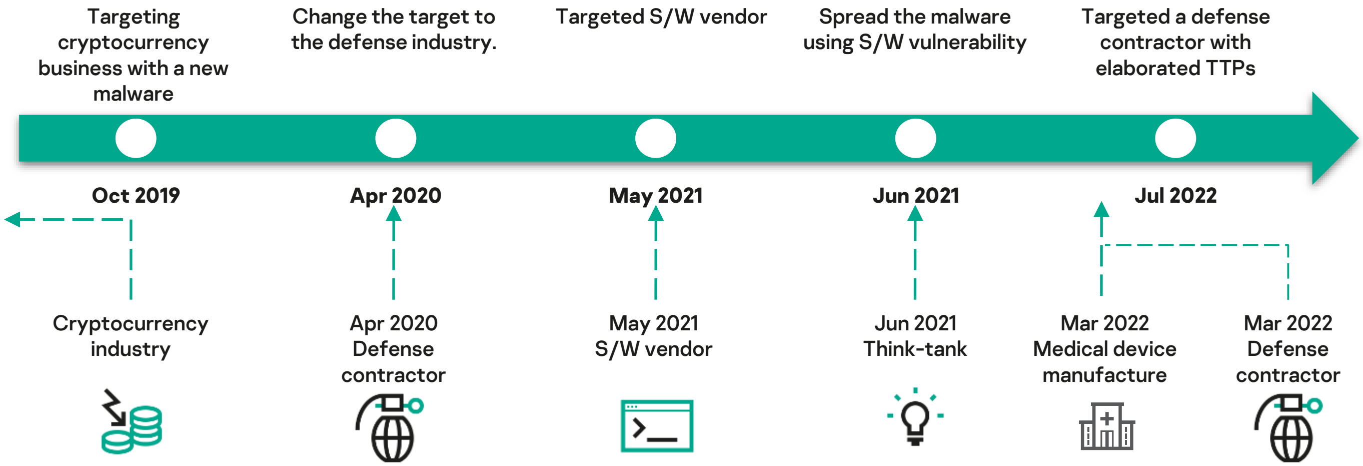
Decrypt and load config

PerceptFrame.dat

Preliminary backdoor or lateral movement

- Technique: ServiceMove(Abusing of PerceptionSimulation service)
- Path: C:\Windows\system32\PerceptionSimulation\

Chronicle of DeathNote cluster



Targeting cryptocurrency business with a new malware

Change the target to the defense industry.

Targeted S/W vendor

Spread the malware using S/W vulnerability

Targeted a defense contractor with elaborated TTPs

Oct 2019

Apr 2020

May 2021

Jun 2021

Jul 2022

Cryptocurrency industry

Apr 2020
Defense contractor

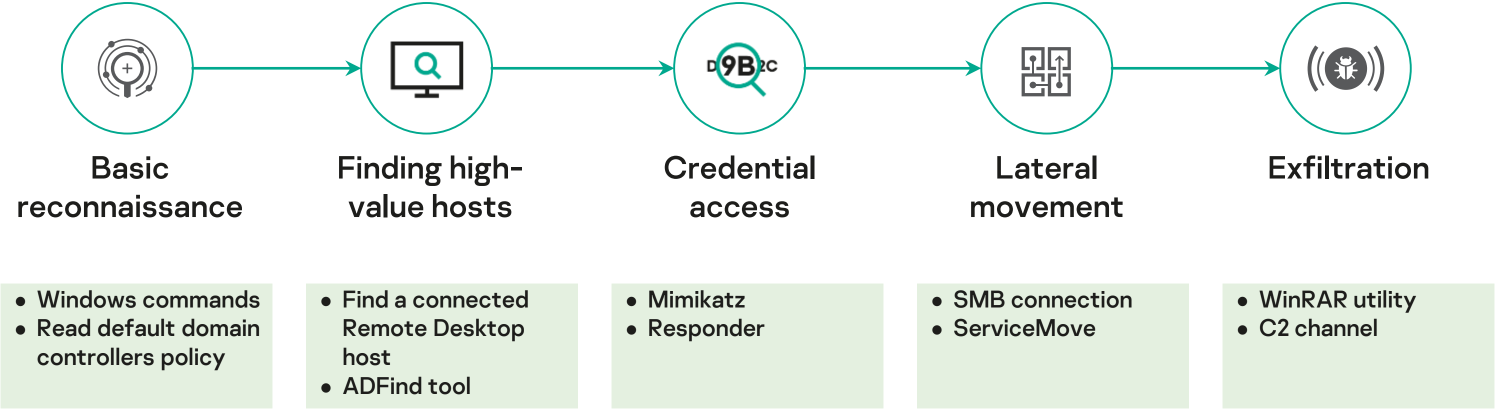
May 2021
S/W vendor

Jun 2021
Think-tank

Mar 2022
Medical device manufacture

Mar 2022
Defense contractor

Post-exploitation



Basic reconnaissance

- Windows commands
- Read default domain controllers policy

Finding high-value hosts

- Find a connected Remote Desktop host
- ADFind tool

Credential access

- Mimikatz
- Responder

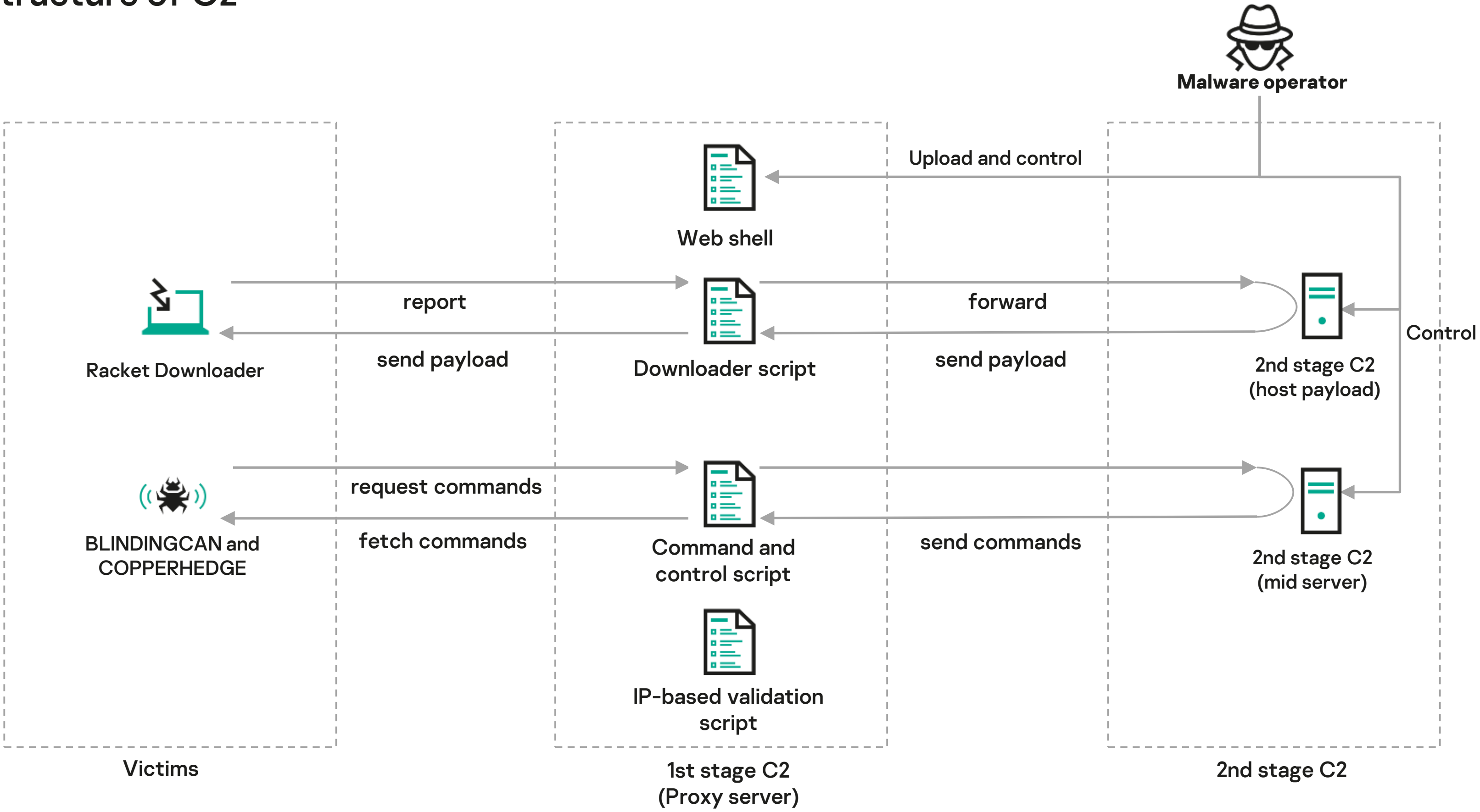
Lateral movement

- SMB connection
- ServiceMove

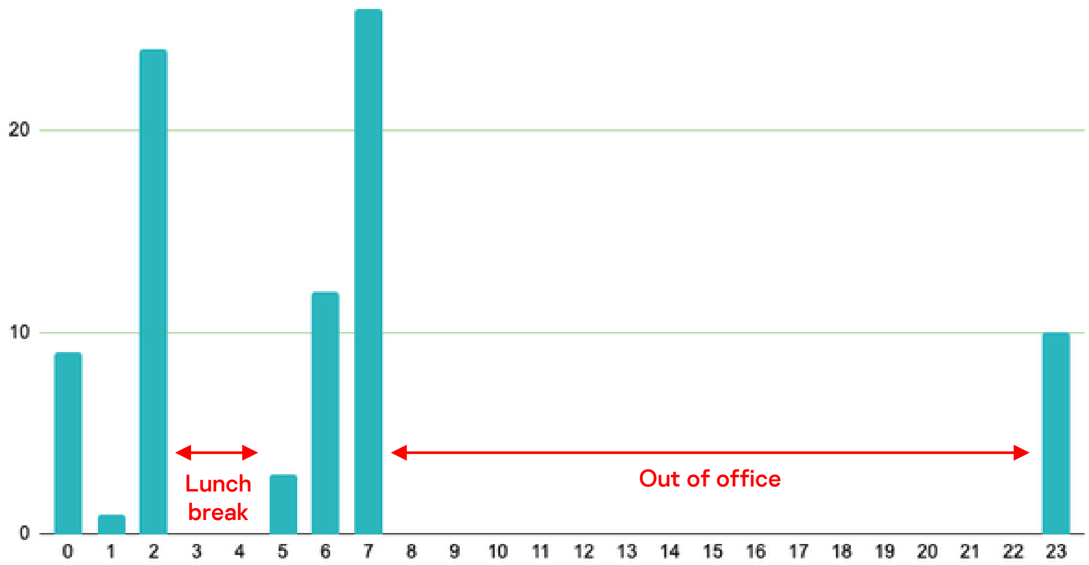
Exfiltration

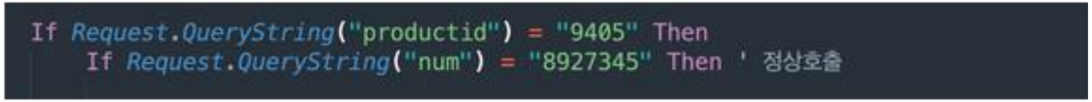
- WinRAR utility
- C2 channel

Structure of C2



Attribution





```
If Request.QueryString("productid") = "9405" Then
    If Request.QueryString("num") = "8927345" Then ' 정상호출
```

Working hours:
GMT+8 or GMT+9 timezone

Language:
Korean-speaking group

Takeaway

Persistent attack and increasing sophistication

- Create malware using open-source software
- Utilized DLL side-loading and BYOVD
- Continuously improve techniques to become more sophisticated.

Full-context based defense is the key

- Hit-and-run style defense never works
- Need to understand full-context of threats
- Diversify defense points

Cooperation with other industry

- Each sector has different strength
- Cooperation is essential to cope with the latest cyber threats

Question?

@unpacker

seongsup4rk@gmail.com