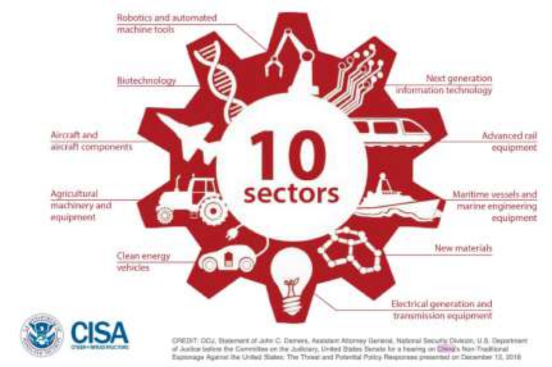
AI鑑識調查應用於半導體的APT - 勒索軟體只是煙霧彈
サイバー攻撃におけるAIフォレンジック - ランサムウェアカムフラージュ

C.K. Chen, Senior Researcher, CyCraft

U.S DoJ: China Wants What We Have

- U.S. Department of Justice
- U.S. Cybersecurity and Infrastructure Security Agency
  - Awareness Briefing – Chinse Cyber Activity Targeting Managed Service Provider
- Made in China 2025


Robotics and automated machine tools
Biotechnology
Next generation information technology
Aircraft and aircraft components
10 sectors
Advanced rail equipment
Agricultural machinery and equipment
Maritime vessels and marine engineering equipment
Clean energy vehicles
New materials
Electrical generation and transmission equipment
CISA

CREDIT: DOJ, Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice before the Committee on the Judiciary, United States Senate for a hearing on China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses presented on December 12, 2018

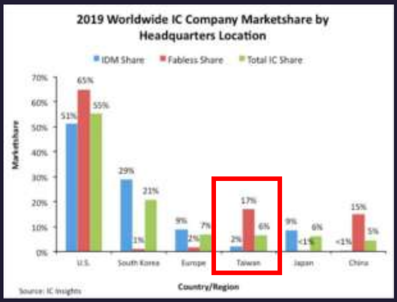
U.S.-China Trade War Hobbles China's Semiconductor Industry Ambitions And Rattles Stocks

- US-China Trade War
  - U.S. restricts sales of critical chip-manufacturing gear to China.

https://www.investors.com/

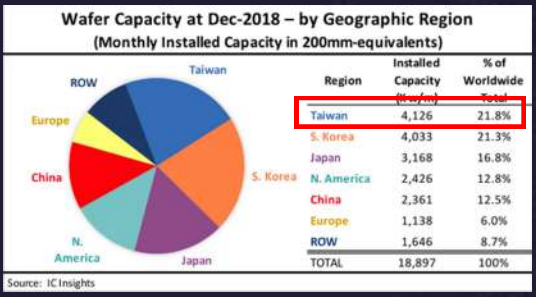
Taiwan's Importance in the Semiconductor Landscape

- 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



2019 Worldwide IC Company Marketshare by Headquarters Location

Source: IC Insights



Wafer Capacity at Dec-2018 – by Geographic Region
(Monthly Installed Capacity in 200mm-equivalents)

Region	Installed Capacity (K w/m)	% of Worldwide Total
Taiwan	4,126	21.8%
S. Korea	4,033	21.3%
Japan	3,168	16.8%
N. America	2,426	12.8%
China	2,361	12.5%
Europe	1,138	6.0%
ROW	1,646	8.7%
TOTAL	18,897	100%

Source: IC Insights

- "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

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: > 8 semiconductor vendors were attacked

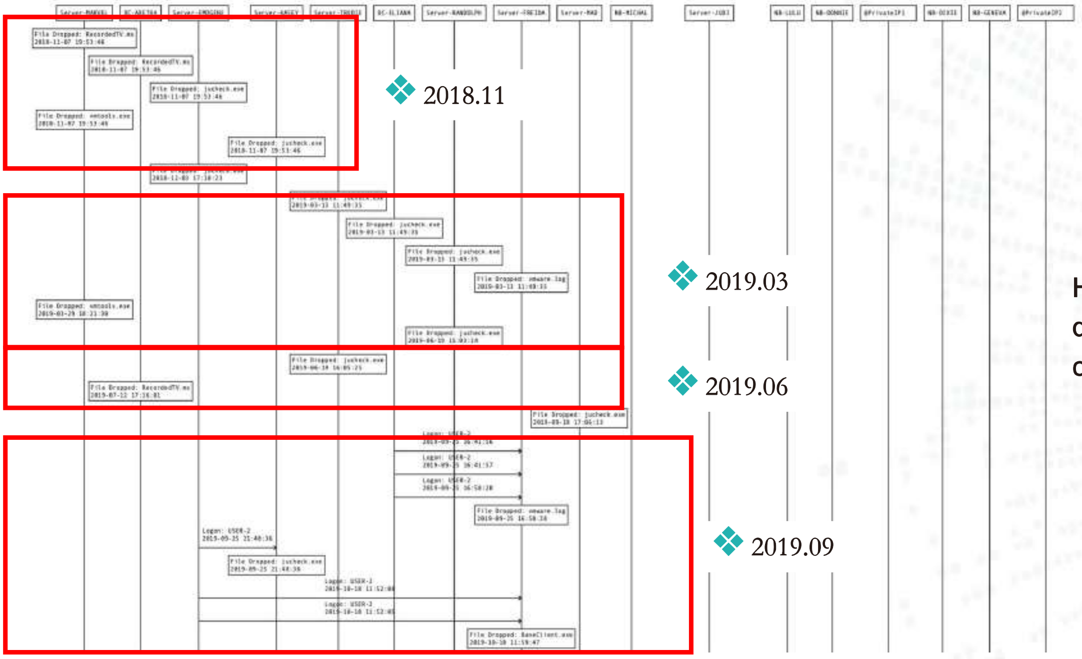
After our white paper was published, the received feedback revealed that more than 8 vendors were targeted by the same threat actor.

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

The APT on the important vendors were precise and well-coordinated. 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


Server-MARVEL
DC-ARETHA
Server-EMOGENE
Server-ANSEY
Server-TREDIE
DC-ILIANA
Server-RANDOLPH
Server-FREIDA
Server-MAD
NB-MICHAL
Server-JUDI
NB-LULU
NB-DONNIE
@PrivateIP1
NB-DIXIE
NB-GENEVA
@PrivateIP2
File Dropped: RecordedTV.ms 2018-11-07 19:53:46
File Dropped: RecordedTV.ms 2018-11-07 19:53:46
File Dropped: jucheck.exe 2018-11-07 19:53:46
File Dropped: vmtools.exe 2018-11-07 19:53:48
File Dropped: jucheck.exe 2018-11-07 19:53:46
File Dropped: jucheck.exe 2018-12-03 17:10:23
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: vmware.log 2019-03-13 11:49:33
File Dropped: vmtools.exe 2019-03-29 18:21:38
File Dropped: jucheck.exe 2019-06-19 15:03:18
File Dropped: jucheck.exe 2019-06-18 16:05:25
File Dropped: RecordedTV.ms 2019-07-12 17:16:01
File Dropped: jucheck.exe 2019-09-18 17:06:13
Logon: USER-2 2019-09-25 16:41:16
Logon: USER-2 2019-09-25 16:41:57
Logon: USER-2 2019-09-25 16:58:28
File Dropped: vmware.log 2019-09-25 16:58:38
Logon: USER-2 2019-09-25 21:40:36
File Dropped: jucheck.exe 2019-09-25 21:48:36
Logon: USER-3 2019-10-18 11:52:08
Logon: USER-3 2019-10-18 11:52:45
File Dropped: BaseClient.exe 2019-10-18 11:59:47

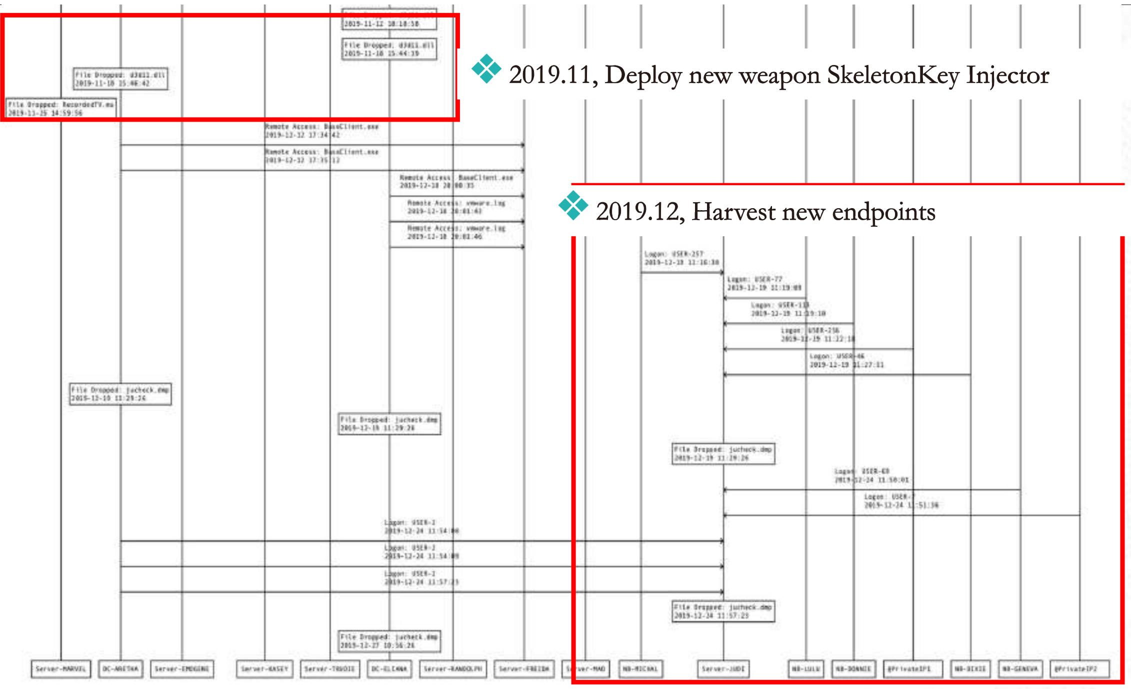
2018.11

2019.03

2019.06

2019.09

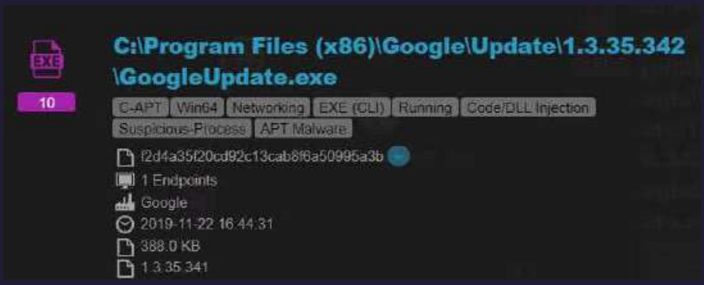
Hacker returns on a quarterly basis to collect new data.



- 2019.11, Deploy new weapon SkeletonKey Injector
- 2019.12, Harvest new endpoints

THREAT-1

Disguised Google Chrome APT Malware



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

10

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

f2d4a35f20cd92c13cab8f6a50995a3b

1 Endpoints

Google

2019-11-22 16:44:31

388.0 KB

1.3.35.341

- **Cannot be effectively detect by AV**
  - In VirusTotal and our own intelligence system CyberTotal, this malware is unseen by all vendors
- C&C Server (Google Cloud Platform)
  - chrome-applatnohp.appspot.com
  - ussdns04.heketwe.com
  - ussdns02.heketwe.com
  - ussdns01.heketwe.com

Appear Date: 2019-11-12

Backdoor: CobaltStrike

Overwrite GoogleUpdate

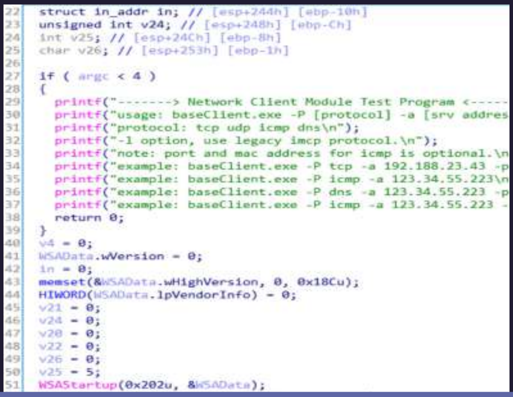
No CTI/VT Information

Discovered in 3+ Comapny

RAT、Command & Control

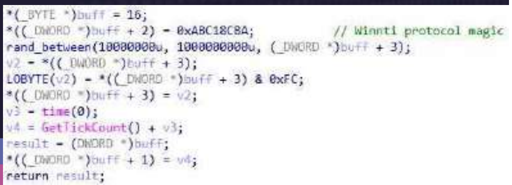
THREAT-2

Customize Probing Tools & Backdoor



```
struct in_addr in; // [esp+244h] [ebp-10h]
unsigned int v24; // [esp+248h] [ebp-Ch]
int v25; // [esp+24Ch] [ebp-8h]
char v26; // [esp+253h] [ebp-1h]

if ( argc < 4 )
{
  printf("-------> Network Client Module Test Program <-----
  printf("usage: baseClient.exe -P [protocol] -a [srv addres
  printf("protocol: tcp udp icmp dns\n");
  printf("-1 option, use legacy imcp 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
  printf("example: baseClient.exe -P icmp -a 123.34.55.223\n
  printf("example: baseClient.exe -P dns -a 123.34.55.223 -p
  printf("example: baseClient.exe -P icmp -a 123.34.55.223 -
  return 0;
}
v4 = 0;
WSAData.wVersion = 0;
in = 0;
memset(&WSAData.wHighVersion, 0, 0x18Cu);
HIWORD(WSAData.lpVendorInfo) = 0;
v21 = 0;
v24 = 0;
v20 = 0;
v22 = 0;
v26 = 0;
v25 = 5;
WSAStartup(0x202u, &WSAData);
```

- MD5
  - A8559c4bcd299125036583febe1a53fb
- We thought baseClient.exe in our public report was a network probing tool
  - It's actually Winnti backdoor



```
*(_BYTE *)buff = 16;
*((_DWORD *)buff + 2) = 0xABC18CBA;           // 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;
```

Appear Date: 2019-11-12

Unknow Source, Maybe Develop by Attackers

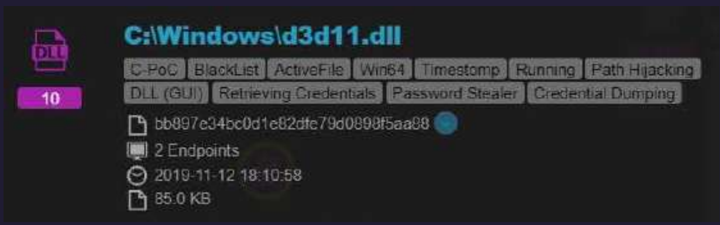
No information in VirusTotal/CTI

Discover in 3+ HSPB Company

Discovery、Recon

THREAT-3

Powerful Credential Hacking Tool



DLL

10

C:\Windows\d3d11.dll

C-PoC | BlackList | ActiveFile | Win64 | Timestomp | Running | Path Hijacking | DLL (GUI) | Retrieving Credentials | Password Stealer | Credential Dumping

bb897e34bc0d1e82dfe79d0898f5aa88

2 Endpoints

2019-11-12 18:10:58

85.0 KB

- File name (DLL Hijacking)
  - C:\Windows\d3d11.dll
  - C:\Windows\wlanapi.dll
- Malware analysis
  - Some code is copied from Dumpert https://github.com/outflankl/Dumpert
  - Weaponize with Skeleton-Key functions，source code from mimikatz
  - Infect and modify LSASS KDC service in DC, implant NTLM hash
    - bd1558807bc500596758364919068dbe

Modified LSASS Memory to implant Skeleton key，any account could login with the pw!

Appear Date: 2019-11-12

Hacker Develop，From Mimikatz & Dumpert

Only Target DC Server

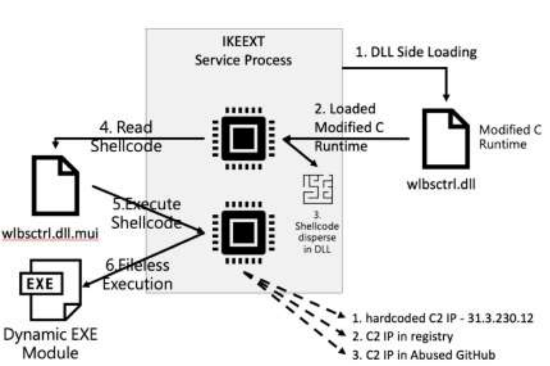
New malware, 0 in VirusTotal

Discover in 2 IC Design Vendors

Lateral Movement、 Persistence

THREAT-4

The Same Backdoor as CCleaner Attack



- File name
  - wlbsctrl.dll
  - 6376a3469c9fb1bb8326e7af734e01d1
- Malware analysis
  - Inserting tiny malign code into benign software
  - non-continuous
  - Indirect call to memory allocation APIs
  - Multiple method to hide/get C2 address

Appear Date: 2020-10-08

Hacker Develop · Same backdoor in CCleaner

Supply Chain Attack

Trick to confuse Anti-Virus

Discover in 1 Vendors

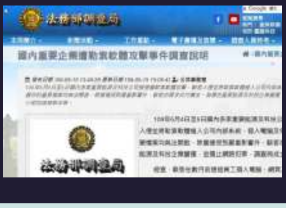
Persistence · Command and Control

APT 41 Targeting Taiwan Critical Infrastructure

- Significant attack to energy sector. Halt down the service of many gas stations.
- CPC - Taiwan Chinese Petroleum Company

2020.05.05

2020.05.15

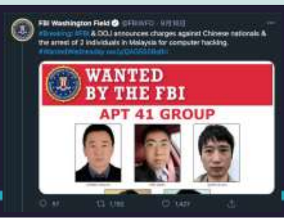


法務部調查局

國內重要企業遭勒索軟體攻擊事件調查說明

[illegible]

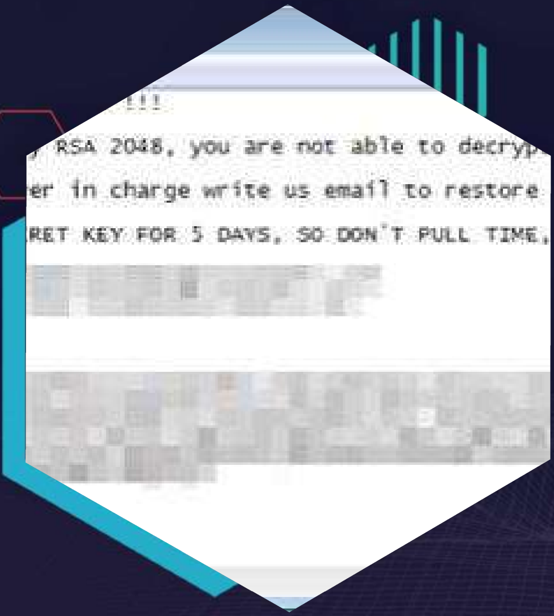
2020.09.16



FBI Washington Field

#Breaking: #FBI & DOJ announces charges against Chinese nationals & the arrest of 2 individuals in Malaysia for computer hacking.

2020.09.18



!!!

RSA 2048, you are not able to decryp

er in charge write us email to restore

RET KEY FOR 5 DAYS, SO DON'T PULL TIME,

[redacted]

[redacted]

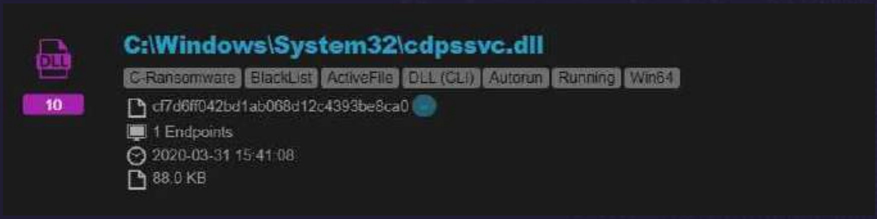
Ransomware? No! It's just a smokescreen

- We found the other variant in VirusTotal, which doesn't leave decryption message
- Not delete shadow volume, leave chance for recovery.
- Launch attack just before TW presidential inauguration.

Remnant Evident: Malware

- Before our IR service, most endpoints are already reinstalled.
- Keep the crime scene is quite important.

2020-04-27 01:39:23



C:\Windows\System32\cdpssvc.dll

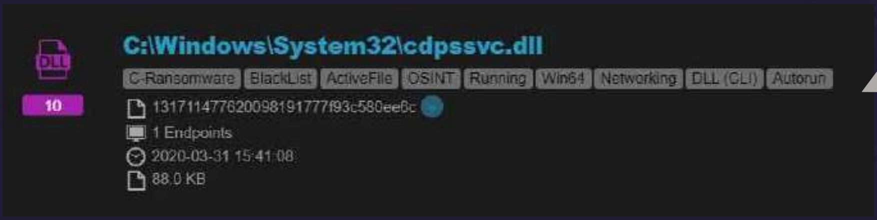
cf7d6ff042bd1ab068d12c4393be8ca0

1 Endpoints

2020-03-31 15:41:08

88.0 KB

2020-04-29 02:19:24



C:\Windows\System32\cdpssvc.dll

1317114776200981917771f93c580ee6c

1 Endpoints

2020-03-31 15:41:08

88.0 KB

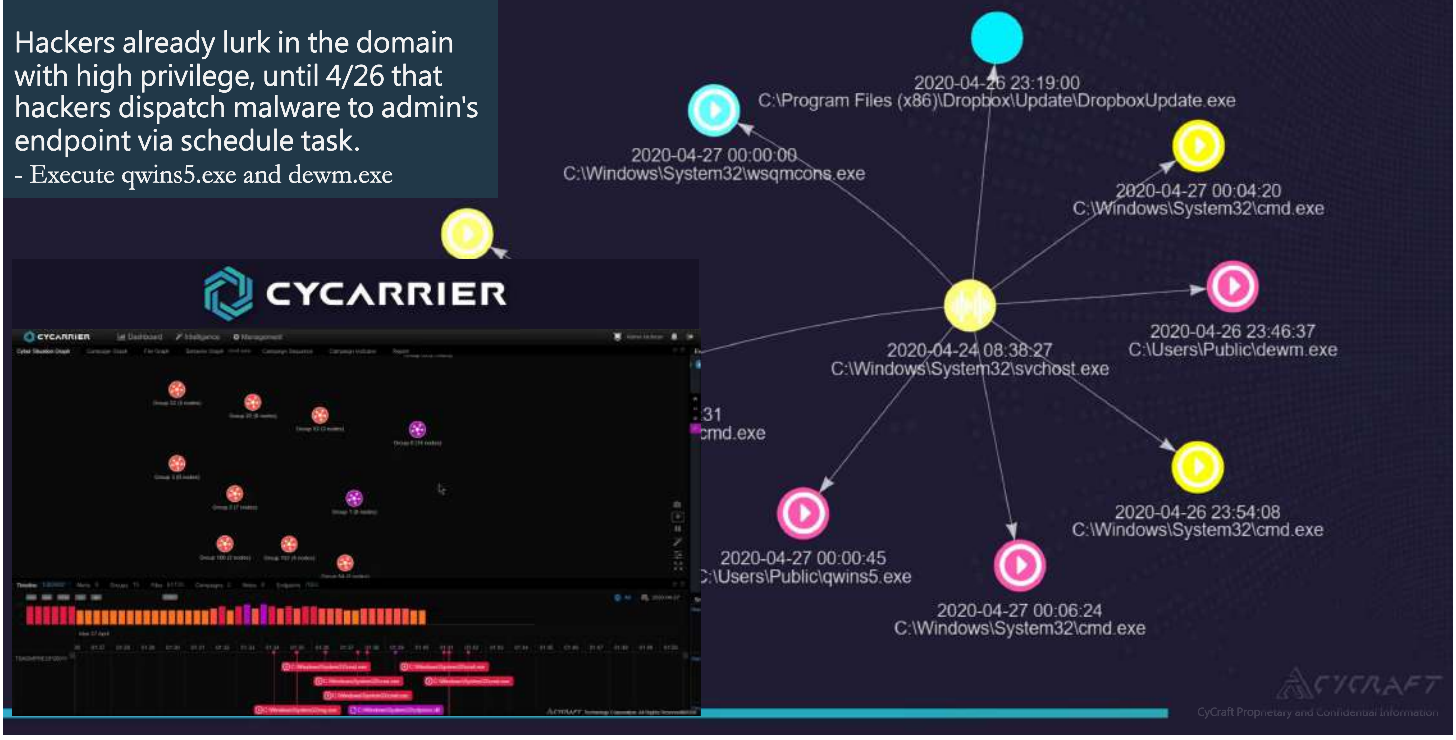
Discover identical malware and C2 as describing in public report

64.64.234.24
104.233.224.227

MIS312_NB
2020-04-26 23:48:31

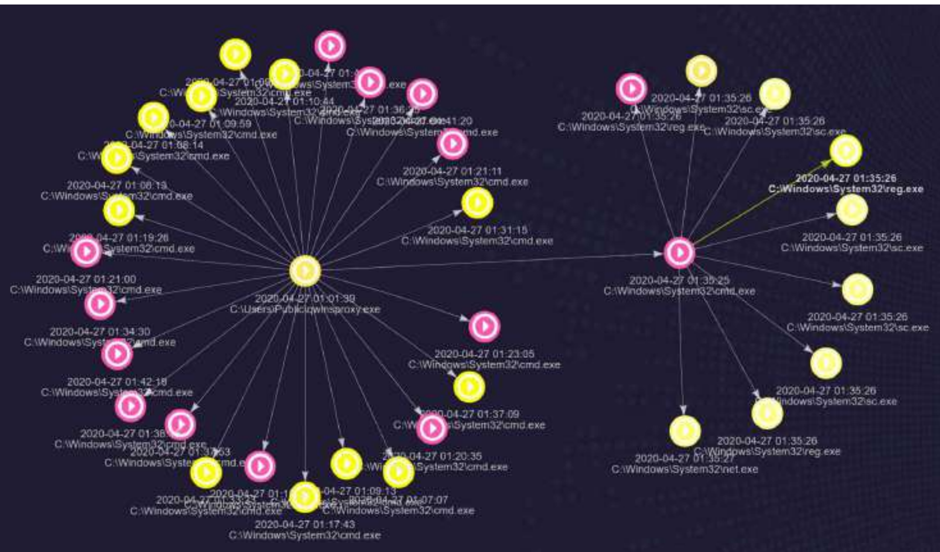
Hackers already lurk in the domain with high privilege, until 4/26 that hackers dispatch malware to admin's endpoint via schedule task.

- Execute qwins5.exe and dewm.exe


2020-04-26 23:19:00
C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
2020-04-27 00:00:00
C:\Windows\System32\wsqmcons.exe
2020-04-27 00:04:20
C:\Windows\System32\cmd.exe
2020-04-26 23:46:37
C:\Users\Public\dewm.exe
2020-04-24 08:38:27
C:\Windows\System32\svchost.exe
31
cmd.exe
2020-04-26 23:54:08
C:\Windows\System32\cmd.exe
2020-04-27 00:00:45
C:\Users\Public\qwins5.exe
2020-04-27 00:06:24
C:\Windows\System32\cmd.exe
CYCARRIER

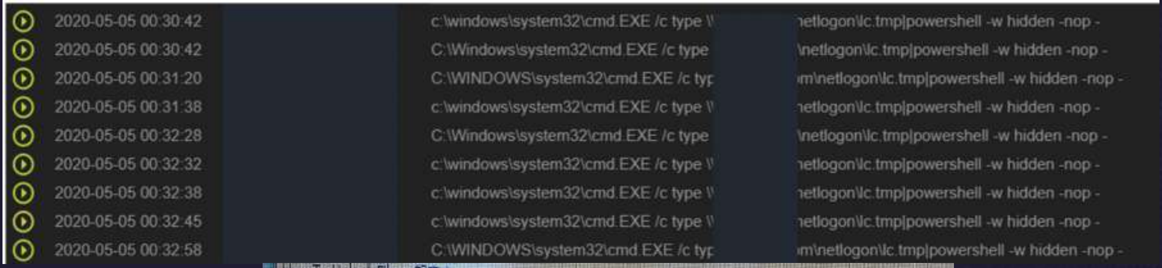
MIS201_NB
2020-04-27 01:01:39

Install Malware CDPSSVC.DLL

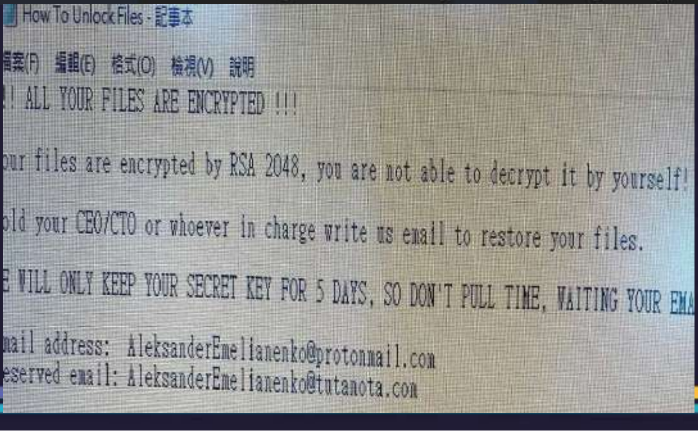

2020-04-27 01:01:39
C:\Users\Public\qwinsproxy.exe
2020-04-27 01:09:59
C:\Windows\System32\cmd.exe
2020-04-27 01:08:14
C:\Windows\System32\cmd.exe
2020-04-27 01:08:19
C:\Windows\System32\cmd.exe
2020-04-27 01:10:44
C:\Windows\System32\cmd.exe
2020-04-27 01:36:20
2020-04-27 01:41:20
C:\Windows\System32\cmd.exe
2020-04-27 01:21:11
C:\Windows\System32\cmd.exe
2020-04-27 01:31:15
C:\Windows\System32\cmd.exe
2020-04-27 01:19:26
C:\Windows\System32\cmd.exe
2020-04-27 01:21:00
C:\Windows\System32\cmd.exe
2020-04-27 01:34:30
C:\Windows\System32\cmd.exe
2020-04-27 01:42:18
C:\Windows\System32\cmd.exe
2020-04-27 01:23:05
C:\Windows\System32\cmd.exe
2020-04-27 01:37:09
C:\Windows\System32\cmd.exe
2020-04-27 01:36
C:\Windows\System32\cmd.exe
2020-04-27 01:37:53
C:\Windows\System32\cmd.exe
2020-04-27 01:20:35
C:\Windows\System32\cmd.exe
2020-04-27 01:33:33
C:\Windows\System32\cmd.exe
2020-04-27 01:09:13
2020-04-27 01:07:07
C:\Windows\System32\cmd.exe
2020-04-27 01:17:43
C:\Windows\System32\cmd.exe
2020-04-27 01:35:25
C:\Windows\System32\cmd.exe
2020-04-27 01:35:26
C:\Windows\System32\reg.exe
2020-04-27 01:35:26
C:\Windows\System32\sc.exe
2020-04-27 01:35:26
C:\Windows\System32\sc.exe
2020-04-27 01:35:26
C:\Windows\System32\reg.exe
2020-04-27 01:35:26
C:\Windows\System32\sc.exe
2020-04-27 01:35:26
C:\Windows\System32\sc.exe
2020-04-27 01:35:26
C:\Windows\System32\sc.exe
2020-04-27 01:35:26
C:\Windows\System32\reg.exe
2020-04-27 01:35:27
C:\Windows\System32\net.exe

```
• C:\WINDOWS\system32\cmd.exe /C C:\WINDOWS\system32\install.bat
• reg add "HKLM\SYSTEM\CurrentControlSet\Services\CDPSsvc\Parameters" /v "ServiceDll" /t REG_EXPAND_SZ /d
  "c:\windows\system32\\cdpssvc.dll" /f
• C:\WINDOWS\system32\cmd.exe /C del c:\users\public\qwinsproxybyp.dll
• sc create "CDPSsvc" binPath= "C:\WINDOWS\system32\svchost.exe -k CDPSsvc" type= share start= auto error= ignore
  DisplayName= "Connected Devices Platform Service"
• C:\WINDOWS\system32\cmd.exe /C del c:\windows\system32\normnfa.nls
```

5/4~5 – Launch the Ransomware



```
2020-05-05 00:30:42  [redacted]  c:\windows\system32\cmd.EXE /c type \  [redacted]  netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:30:42  [redacted]  C:\Windows\system32\cmd.EXE /c type   [redacted]  \netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:31:20  [redacted]  C:\WINDOWS\system32\cmd.EXE /c typ    [redacted]  m\netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:31:38  [redacted]  c:\windows\system32\cmd.EXE /c type \  [redacted]  netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:32:28  [redacted]  C:\Windows\system32\cmd.EXE /c type   [redacted]  \netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:32:32  [redacted]  c:\windows\system32\cmd.EXE /c type \  [redacted]  netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:32:38  [redacted]  c:\windows\system32\cmd.EXE /c type \  [redacted]  netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:32:45  [redacted]  c:\windows\system32\cmd.EXE /c type \  [redacted]  netlogon\lc.tmp|powershell -w hidden -nop -
2020-05-05 00:32:58  [redacted]  C:\WINDOWS\system32\cmd.EXE /c typ    [redacted]  m\netlogon\lc.tmp|powershell -w hidden -nop -
```



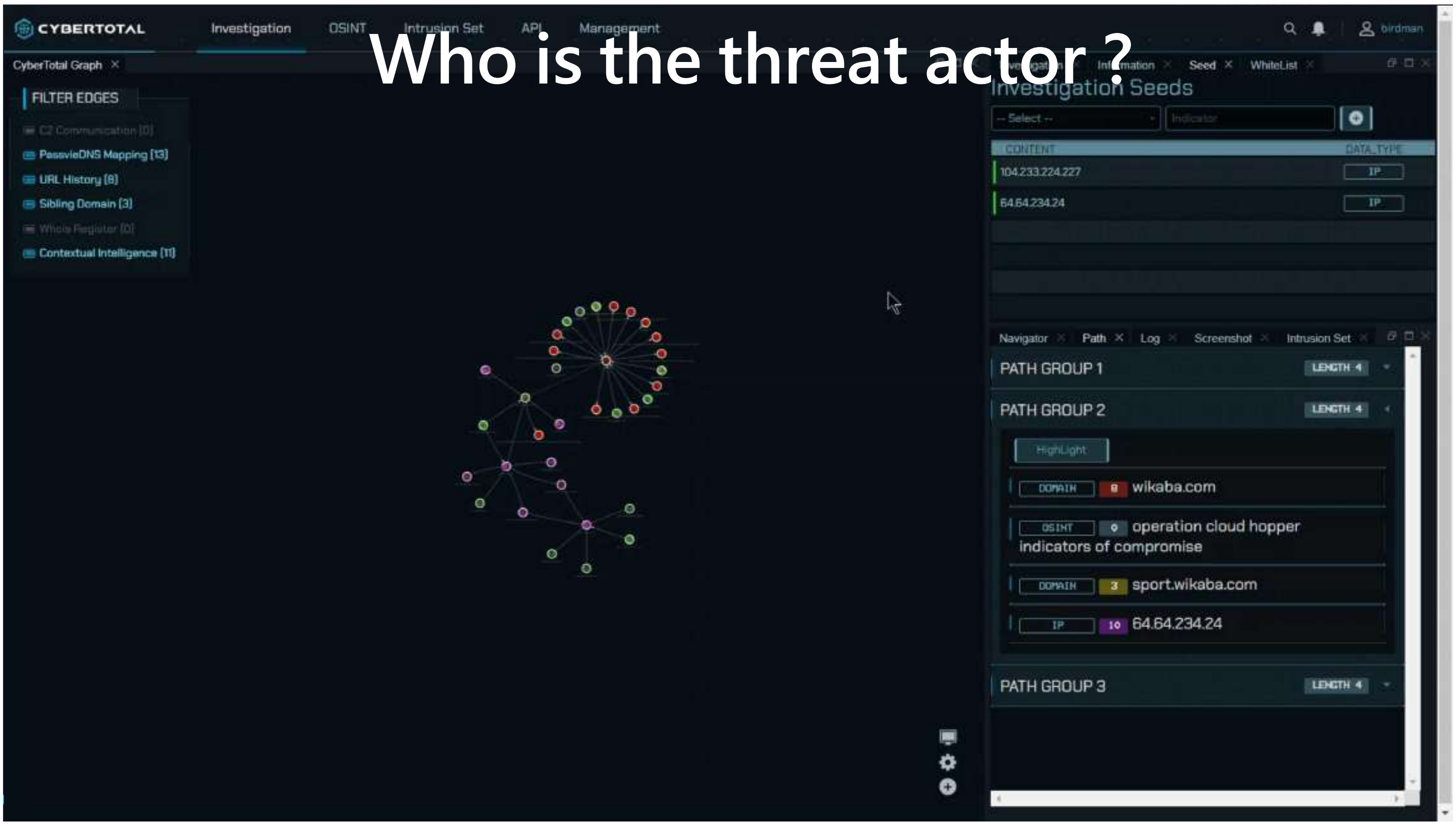
How To Unlock Files - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

```
!! ALL YOUR FILES ARE ENCRYPTED !!!

our files are encrypted by RSA 2048, you are not able to decrypt it by yourself!

old your CEO/CTO or whoever in charge write us email to restore your files.

E WILL ONLY KEEP YOUR SECRET KEY FOR 5 DAYS, SO DON'T PULL TIME, WAITING YOUR EMA

mail address:  AleksanderEmelianenko@protonmail.com
eserved email: AleksanderEmelianenko@tutanota.com
```

Incident Timeline

日曜日	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
4/26 First observed Hacker activity	4/27 1st round backdoor install	4/28 Hacker's day off	4/29 2ND round backdoor install	4/30 Hacker's day off	5/1 Labor day TW Holiday	5/2 Weekend
5/3 Weekend Hacker prepare to attack	5/4 ⚠ Compromised !!	5/5 ⚠ Compromised !!	5/6 Reinstall Systems Chunghwa Telecom Incident Notification	5/7 Reinstall Systems	5/8 Reinstall Systems	5/9
5/10	5/11	5/12	5/13	5/14	5/15 Report from MJIB	5/16

Who is the threat actor ?



FILTER EDGES

- C2 Communication (0)
- PassiveDNS Mapping (13)
- URL History (8)
- Sibling Domain (3)
- Whois Register (0)
- Contextual Intelligence (11)

Investigation Seeds

-- Select --
Indicator

CONTENT	DATA_TYPE
104.233.224.227	IP
64.64.234.24	IP

PATH GROUP 1 LENGTH 4

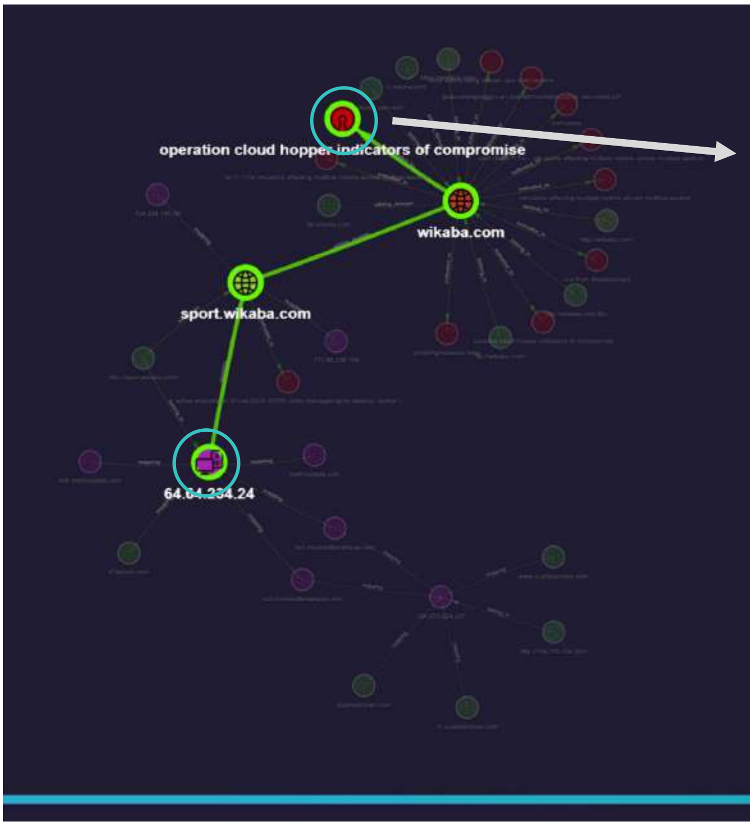
PATH GROUP 2 LENGTH 4

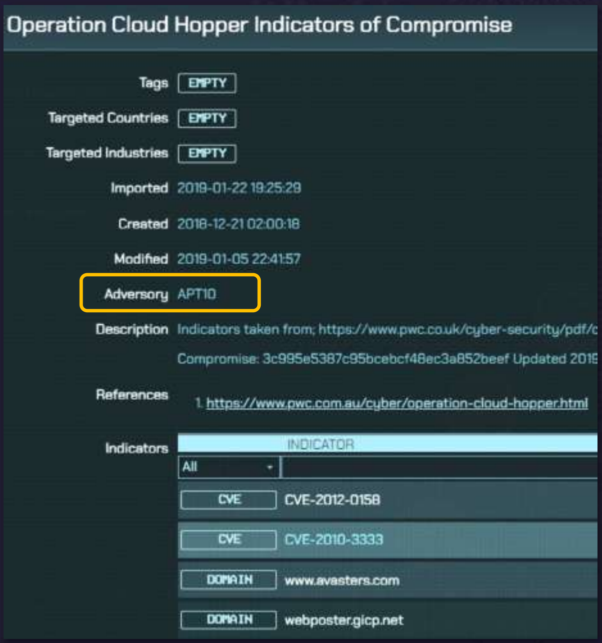
HighLight

- DOMAIN 8 wikaba.com
- OSINT 0 operation cloud hopper indicators of compromise
- DOMAIN 3 sport.wikaba.com
- IP 10 64.64.234.24

PATH GROUP 3 LENGTH 4

AI Auto Reasoning for Threat Actor and Source





Operation Cloud Hopper Indicators of Compromise

Tags	EMPTY
Targeted Countries	EMPTY
Targeted Industries	EMPTY
Imported	2019-01-22 19:25:29
Created	2018-12-21 02:00:18
Modified	2019-01-05 22:41:57
Adversary	APT10
Description	Indicators taken from; https://www.pwc.co.uk/cyber-security/pdf/c Compromise: 3c995e5387c95bcebcf48ec3a852beef Updated 2019
References	1. https://www.pwc.com.au/cyber/operation-cloud-hopper.html

Indicators

INDICATOR	
All	
CVE	CVE-2012-0158
CVE	CVE-2010-3333
DOMAIN	www.avasters.com
DOMAIN	webposter.gicp.net

Q&A