Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

Published: 2024-11-25 · Archived: 2026-04-05 16:14:33 UTC

APT & Targeted Attacks

Since 2023, APT group Earth Estries has aggressively targeted key industries globally with sophisticated techniques and new backdoors, like GHOSTSPIDER and MASOL RAT, for prolonged espionage operations.

By: Leon M Chang, Theo Chen, Lenart Bermejo, Ted Lee Nov 25, 2024 Read time: 14 min (3744 words)

Summary

-
- Earth Estries, a Chinese APT group, has primarily targeted critical sectors like telecommunications and government entities across the US, Asia-Pacific, Middle East, and South Africa since 2023.
- The group employs advanced attack techniques and multiple backdoors, such as GHOSTSPIDER, SNAPPYBEE, and MASOL RAT, affecting several Southeast Asian telecommunications companies and government entities.
- Earth Estries exploits public-facing server vulnerabilities to establish initial access and uses living-off-the-land binaries for lateral movement within networks to deploy malware and conduct long-term espionage.
- The group has compromised over 20 organizations, targeting various sectors including telecommunications, technology, consulting, chemical, and transportation industries, as well as government agencies and NGOs in numerous countries.
- Earth Estries uses a complex C&C infrastructure managed by different teams, and their operations often overlap with TTPs of other known Chinese APT groups, indicating possible use of shared tools from malware-as-a-service providers.

Since 2023, Earth Estriesopen on a new tab (aka Salt Typhoon, FamousSparrow, GhostEmperor and UNC2286) has emerged as one of the most aggressive Chinese advanced persistent threat (APT) groups, primarily targeting critical industries such as telecommunications and government entities in the US, the Asia-Pacific region, the Middle East, and South Africa. In this blog entry, we will highlight their evolving attack techniques and analyze the motivation behind their operations, providing insights into their long-term targeted attacks.

A key finding from our recent investigation is the discovery of a new backdoor, GHOSTSPIDER, identified during attacks on Southeast Asian telecommunications companies. We will explore the technical details of GHOSTSPIDER, its impact across multiple countries, and interesting findings when we were tracking its command-and-control (C&C) infrastructure. We have also uncovered the group's use of the modular backdoor SNAPPYBEE (aka Deed RAT)open on a new tab, another tool shared among Chinese APT groups.

Furthermore, we discovered that Earth Estries uses another cross-platform backdoor, which we initially identified during our investigation of Southeast Asian government incidents in 2020. We named it MASOL RAT based on its PDB string. We couldn't link MASOL RAT to any known threat group at the time due to limited information. However, this year we observed that Earth Estries has been deploying MASOL RAT on Linux devices targeting Southeast Asian government networks. More details about MASOL RAT will be provided in this blog entry.

Recently, we also noticed that Microsoft has tracked the APT groups FamousSparrow and GhostEmperor under the name Salt Typhoonopen on a new tab. However, we don't have sufficient evidence that Earth Estries is related to the recent news of a recent Salt Typhoon cyberattackopen on a new tab, as we have not seen a more detailed report on Salt Typhoon. Currently, we can only confirm that some of Earth Estries' tactics, techniques, and procedures (TTPs) overlap with that of FamousSparrow and GhostEmperor.

Motivation

We have observed that Earth Esties has been conducting prolonged attacks targeting governments and internet service providers since 2020. In mid-2022, we noticed that the attackers also started targeting service providers for governments and telecommunications companies. For example, we found that in 2023, the attackers had also targeted consulting firms and NGOs that work with the U.S. federal government and military. The attackers use this approach to gather intelligence more efficiently and to attack their primary targets more quickly.

Notably, we observed that attackers targeted not only critical services (like database servers and cloud servers) used by the telecommunications company, but also their vendor network. We found that they implanted the DEMODEX rootkit on vendor machines. This vendor is a primary contractor for the region's main telecommunications provider, and we believe that attackers use this approach to facilitate access to more targets.

Victimology

We found that Earth Estries successfully compromised more than 20 organizations in areas that include the telecommunications, technology, consulting, chemical, and transportation industries, government agencies, and non-profit organizations (NGOs). Victims also came from numerous countries, including:

- Afghanistan
- Brazil
- Eswatini
- India
- Indonesia
- Malaysia
- Pakistan
- The Philippines
- South Africa
- Taiwan
- Thailand
- US
- Vietnam

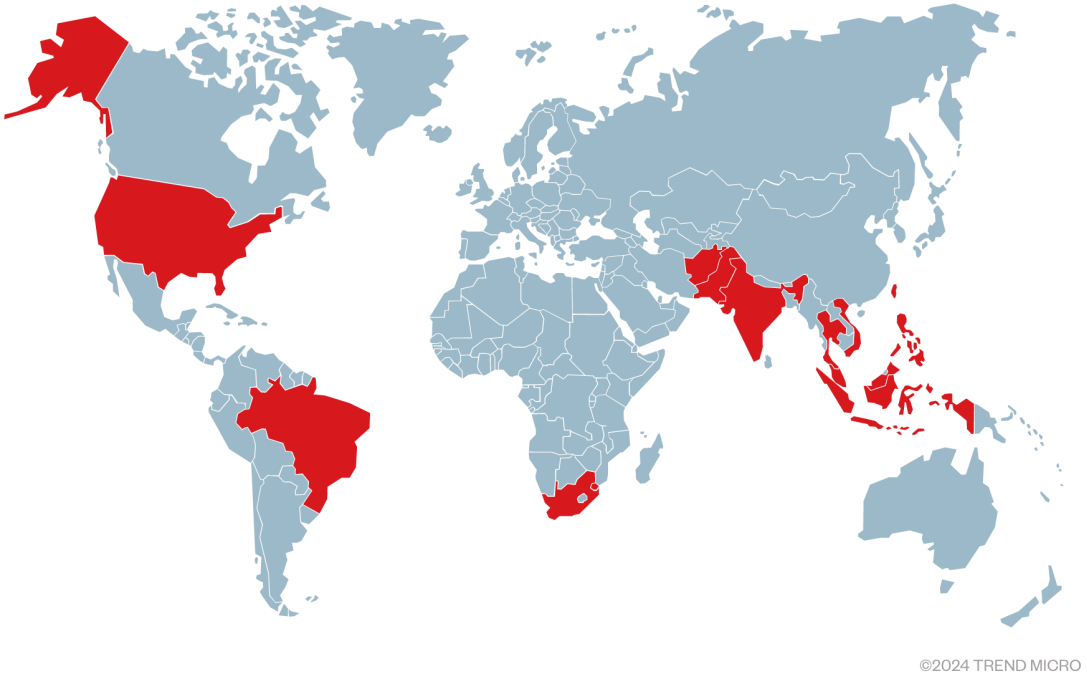

Figure 1. Victimology map of Earth Estries

Initial access

Earth Estries is aggressively targeting the public-facing servers of victims. We have observed them exploiting server-based N-day vulnerabilities, including the following:

Table 1. The list of vulnerabilities exploited by Earth Estries

After gaining control of the vulnerable server, we observed that the attackers leveraged living-off-the-land binaries (LOLBINs) like WMIC.exe and PSEXEC.exe for lateral movement, and deployed customized malware such as SNAPPYBEEopen on a new tab, DEMODEX, and GHOSTSPIDER to conduct long-term espionage activities against their targets.

Campaign overview

Our analysis suggests that Earth Estries is a well-organized group with a clear division of labor. Based on observations from multiple campaigns, we speculate that attacks targeting different regions and industries are launched by different actors. Additionally, the C&C infrastructure used by various backdoors seems to be managed by different infrastructure teams, further highlighting the complexity of the group's operations.

Campaign Alpha

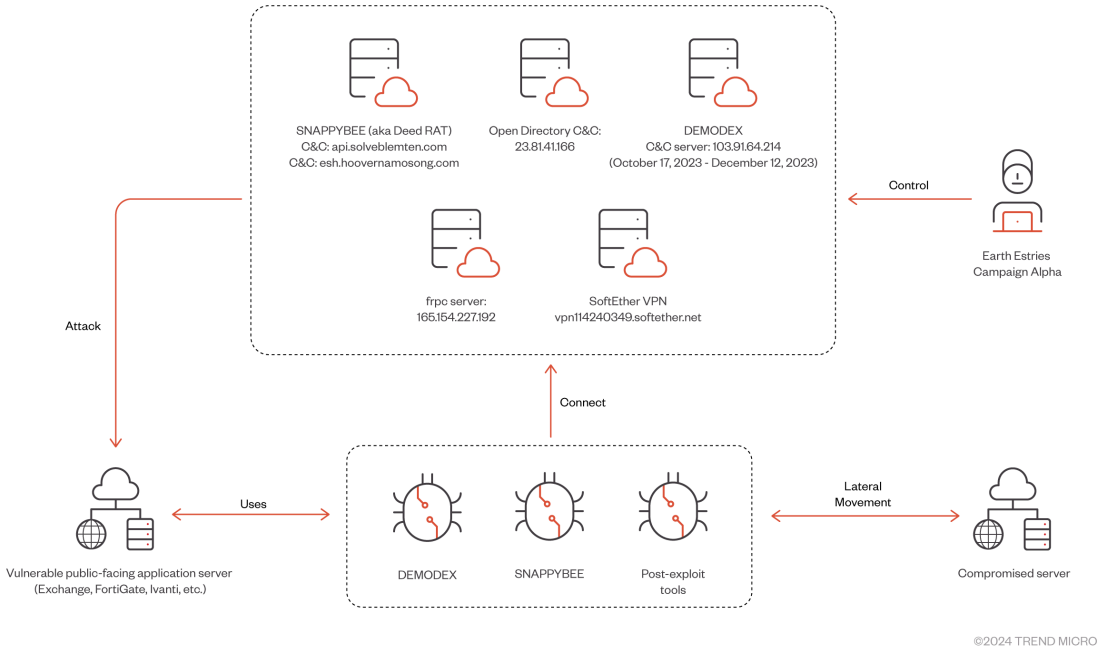

Figure 2. Campaign Alpha overview

In the attacks we observed last October targeting the Taiwanese government and a chemical company, we found that the attackers downloaded malicious tools from their C&C server (23.81.41[.]166). While investigating the download site (23.81.41[.]166), we found more interesting samples on the C&C server which had an open directory on port 80.

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

Figure 3. The C&C with open directory vulnerability

The notable samples are listed in Table 2 below, based on our monitoring from October 2023 to April 2024.

File	Description
sql.toml	frpc config (C&C server: 165.154.227[.]192)
onedrived.zip	Contains the PowerShell script ondrived.ps1.
Nsc.exe	The first SNAPPYBEE sample set (SNAPPYBEE C&C 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 C&C domain: esh.hoovernamosong[.]com)
Others	Open-source hacktools like frpc, NeoReGeorg tunnel, and fscan.

Table 2. Notable samples

Here is a summary of notable findings:

- The frpc C&C 165.154.227[.]192 could be linked to an SSL certificate (SHA256: 2b5e7b17fc6e684ff026df3241af4a651fc2b55ca62f8f1f7e34ac8303db9a31) previously used by ShadowPad, which is another shared tool among several Chinese APT groups. In addition, the C&C IP address was also mentioned in a Fortinet reportopen on a new tab and indicators of compromiseopen on a new tab related to the Ivanti exploit.
- **We observed the TTPs used by onedrived.ps1 are similar to those of GhostEmperoropen on a new tab's first-stage PowerShell dropper. The only difference is that the strings are encoded using base64 algorithm in this new variant.**
- **Based on our analysis, although the two sets of samples used different DLL hijacking combinations and decoding algorithms to decrypt the payload, we found that the backdoor characteristics matched those of the previous SNAPPYBEE. (We identified that the decrypted shellcode module header signature is 0xDEED4554 and the Main/Root module ID is still 0x20, can be seen in Figure 4).**

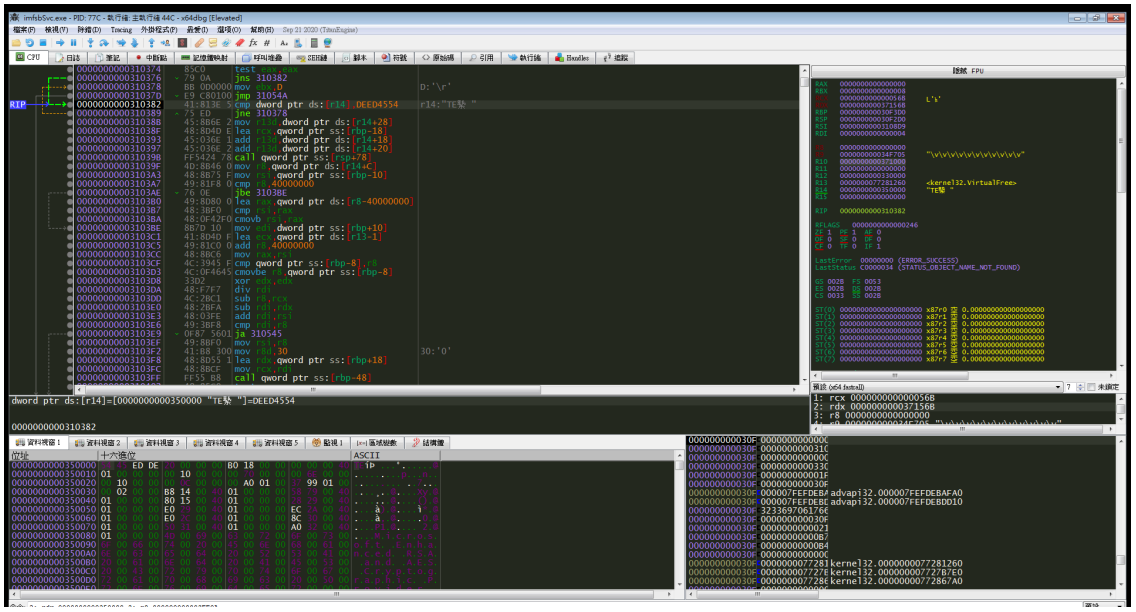

Figure 4. The analysis screenshot of SNAPPYBEE

DEMODEX rootkit infection chain

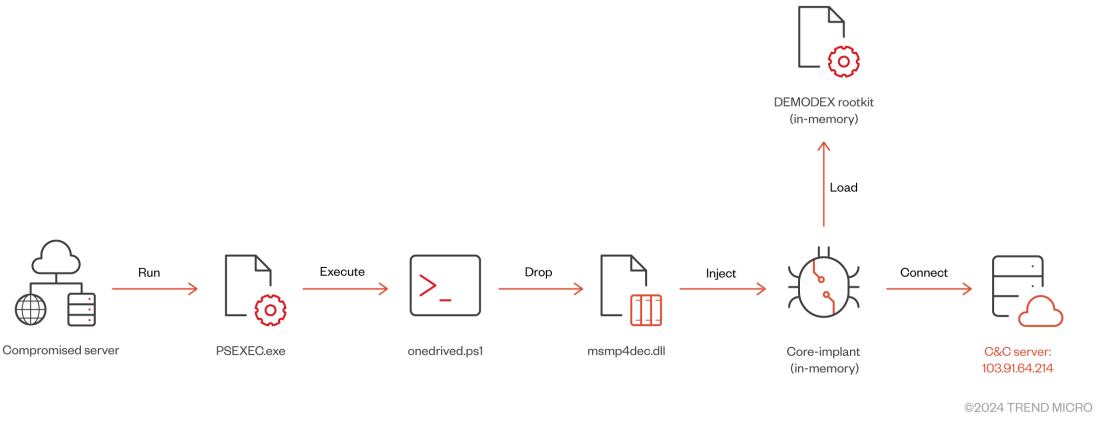

Figure 5. The infection chain of DEMODEX rootkit

There are two requirements to analyze the DEMODEX rootkit:

1. The first-stage PowerShell script requires a decryption key as an argument.
2. The second-stage service loader uses the computer name as the AES decryption key.

Based on our telemetry, we discovered that the attacker used PSEXEC.exe to execute the following commands to install the DEMODEX rootkit:

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

Notably, we discovered that all components related to the DEMODEX rootkit use control flow flattening techniques to increase the difficulty of analysis (Figure 6).

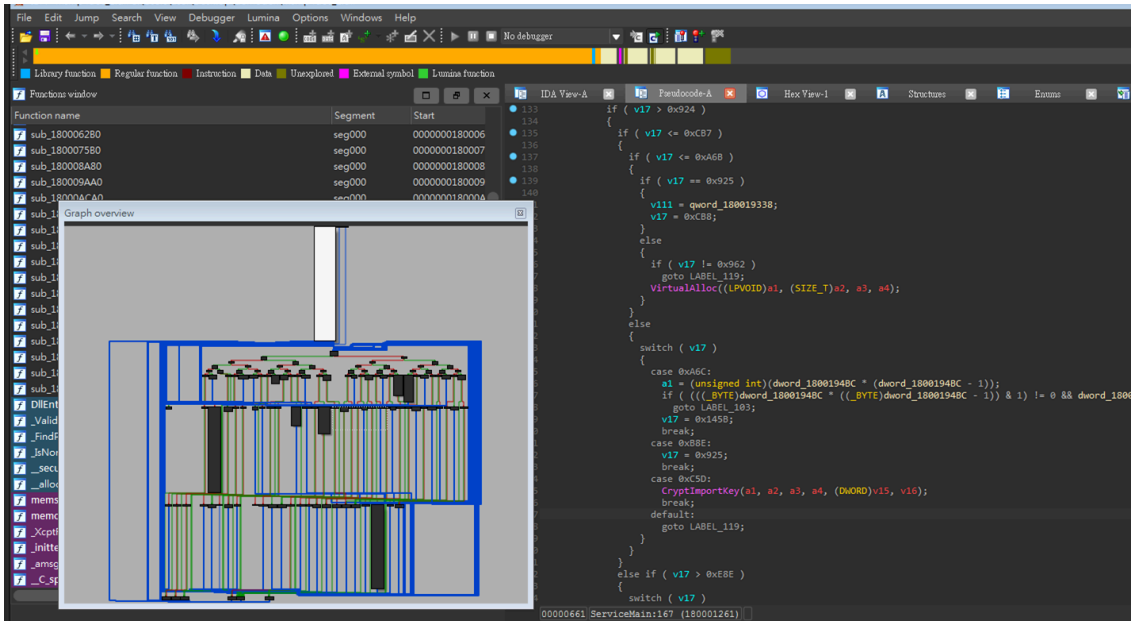

Figure 6. DEMODEX Anti-analysis techniques (control flow flattening)

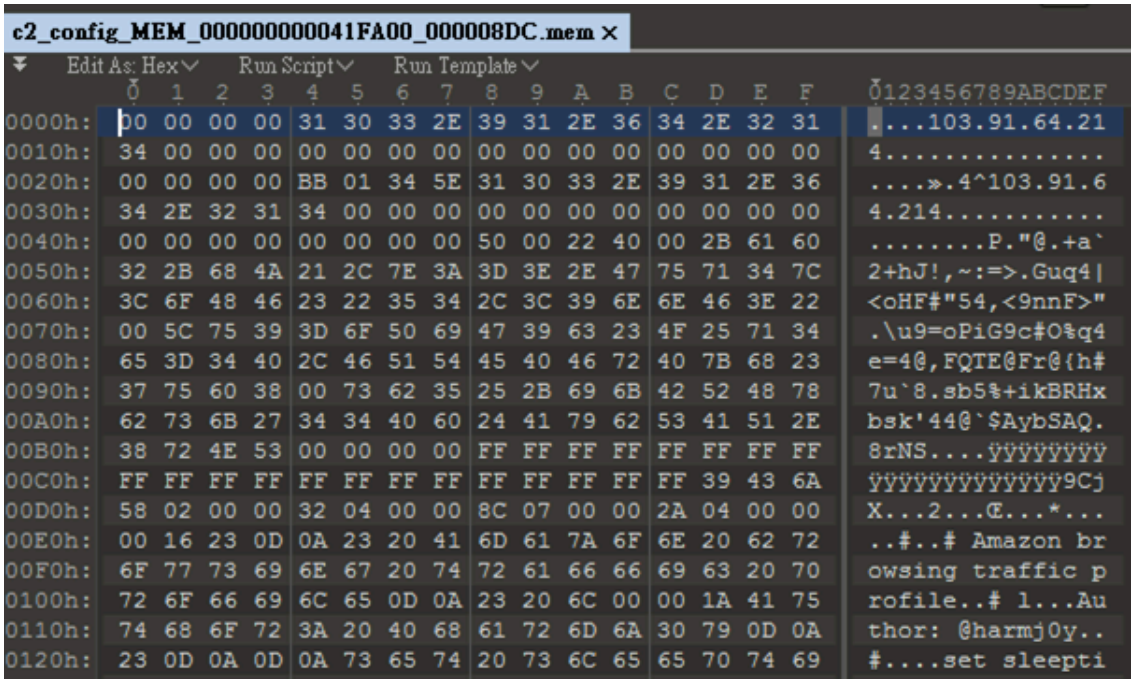

Figure 7. Core-implant malware configuration (C&C: 103.91.64[.]214)

C&C infrastructure activities

While tracking the C&C infrastructure of the aforementioned backdoor, we found the following notable findings:

1. We found that one of the SNAPPYBEE C&C domains, api.solveblemten[.]com, has WHOIS registration information that overlaps with some indicators of compromise (IOCs) mentioned in Mandiant's UNC4841 reportopen on a new tab. Based on our research, we believe that these related C&C domains were likely registered by the same provider and shared them in different operations. However, we don't have sufficient evidence to consider UNC4841 as one of the subgroups related to Earth Estries.

2. Another SNAPPYBEE C&C domain (esh.hoovernamosong[.]com) resolved to a C&C IP address (158.247.222[.]165), which could be linked to a SoftEther domain (vpn114240349.softether[.]net). Therefore, we believe the threat actor also used SoftEther VPN to establish their operational networks, making it more difficult to track their activities.
3. Notably, we discovered and downloaded victim data from the SNAPPYBEE C&C (158.247.222[.]165) with an open directory on 8000 port this February. Based on our analysis, we believe the victim data was exfiltrated from a US NGO. Most of the victim data is composed of financial, human resources, and business-related documents. It's worth noting that the attacker also collected data related to multiple military units and federal government entities.

Post-exploitation findings

In this campaign, we observed that the attackers primarily used the following LOLbin tools to gather endpoint information and perform lateral movement to gain access to more compromised machines.

Tools	Description
frpc related	• WMIC.exe /node:<REDATED> /user:<REDATED> /password:<REDATED> process call create "cmd.exe /c expand c:/windows/debug/1.zip c:/windows/debug/notepadup.exe • cmd.exe /c ping 165.154.227.192 -n 1 > c:\Windows\debug\info. • cmd.exe /c c:/windows/debug/win32up.exe -c c:/windows/debug/sql.toml • cmd.exe /c wevtutil qe security /format:text /q:\"Event[System[(EventID=4624)]\" > c:\windows\debug\info.log
ps.exe (PSEXEC.exe)	• C:\Windows\assembly\ps.exe /accepteula \\<REDATED> -u <REDATED> -p <REDATED> -s cmd /c c:\Windows\assembly\1.bat • WMIC.exe /node:<REDATED> /user:<REDATED> /password:<REDATED> process call create "cmd.exe /c c:\Windows\debug\1.bat""

Table 3. LOLbin tools used to gather endpoint information and perform lateral movement

Campaign Beta

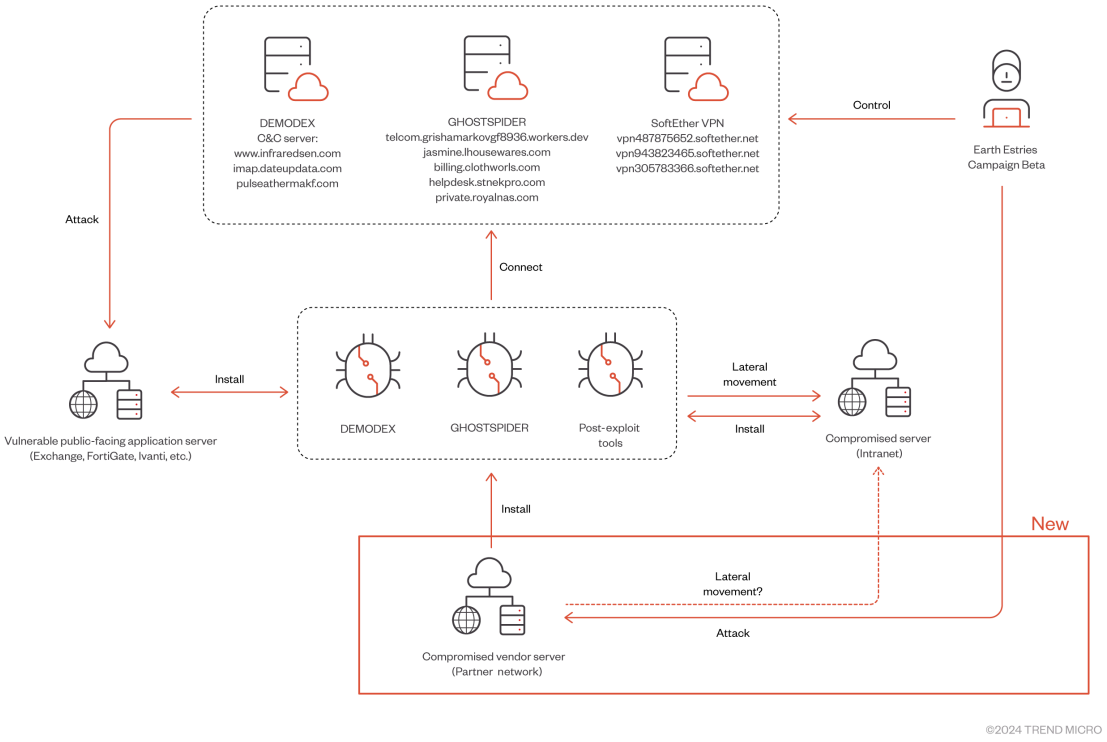

Figure 8. Campaign Beta overview

In this section, we will introduce Earth Estries' long-term attacks on telecommunications companies and government entities. According to our research, most of the victims have been compromised for several years. We believe that in the early stages, the attackers successfully obtained credentials and control target machines through web vulnerabilities and the Microsoft Exchange ProxyLogon exploit chain. We observed that for these long-term targets, the attackers primarily used the DEMODEX rootkit to remain hidden within the victims' networks. Notably, in a recent investigation into attacks on telecommunications companies in Southeast Asia, we discovered a previously undisclosed backdoor; we have named it GHOSTSPIDER.

GHOSTSPIDER's technique analysis

GHOSTSPIDER is a sophisticated multi-modular backdoor designed with several layers to load different modules based on specific purposes. This backdoor communicates with its C&C server using a custom protocol protected by Transport Layer Security (TLS), ensuring secure communication.

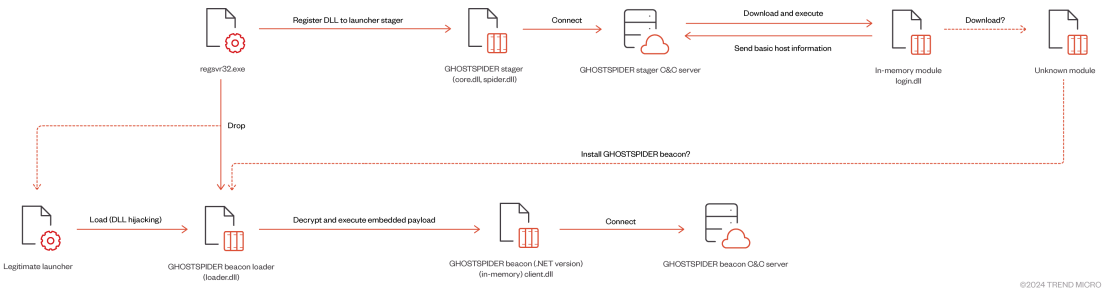

Figure 9. The GHOSTSPIDER infection flow

Initial infection and stager deployment

Based on our telemetry, we observed that the threat actor installs the first-stage stager via regsvr32.exe, which is used to install a DLL (with export names such as core.dll or spider.dll) as a service. The stager is designed to check for a specific hostname hard-coded in the DLL, ensuring that it only runs on the targeted machine. 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) to load and execute in memory. This login module collects basic information about the infected endpoint and sends it back to the stager's C&C server. After this initial phase, the stager enters a polling mode, waiting for the threat actor's next payload.

Beacon loader deployment

On the infected endpoint, the threat actor deploys a legitimate executable file alongside a malicious DLL file for DLL search order hijacking. This malicious DLL, another GHOSTSPIDER module known as the beacon loader (DLL export name: loader.dll), is used to launch the beacon payload in memory. A scheduled task is created to launch the executable. The beacon loader contains an encrypted .NET DLL payload (DLL export name: client.dll), which is decrypted and executed in memory.

Communication protocol

The communication requests that are used by the GHOSTSPIDER stager follow a common format. A connection ID is placed in the HTTP header's cookie as “phpsessid”. The connection ID is calculated using CRC32 or CRC64 with UUID4 values. Figure 10 shows an example of a stager's first request to the C&C server.

```
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....*.
```

Figure 10. Example of a stager's first request to the C&C server

Here is an example of a decrypted response:

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

The 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

Beacon communication and command codes

Like the stager, the GHOSTSPIDER beacon uses an almost identical format to communicate with the beacon C&C server to receive command codes.

Table 4 outlines the command codes supported by the GHOSTSPIDER beacon.

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)

Table 4. Command codes supported by the GHOSTSPIDER beacon

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.

This modular design significantly enhances the backdoor's flexibility and adaptability, as individual components can be deployed or updated independently based on the attacker’s evolving needs. Additionally, it complicates detection and analysis, as analysts are forced to piece together a fragmented view of the malware’s full functionality. By isolating different capabilities across separate modules, GHOSTSPIDER not only reduces its footprint, but also makes it challenging to construct a comprehensive understanding of its operation and overall objectives.

The new DEMODEX infection flow

This year, we observed that the attackers used another variant of DEMODEX. In this new installation flow, the attackers no longer use a first-stage PowerShell script to deploy the additional needed payload. Instead, the required registry data (the encrypted configuration and the shellcode payload) for installation are bundled in a

CAB file. The CAB bundle will be deleted after installation is finished. This approach ensures that, even after we collected the first-stage PowerShell script, the analysis cannot proceed due to the lack of additional information. We found a report published by another vendor that mentions findings consistent with our observations.

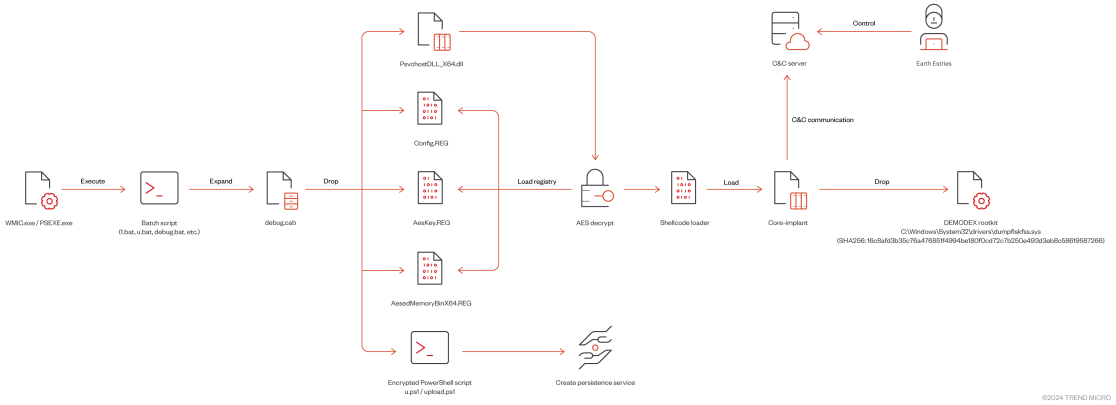

Figure 11. New DEMODEX infection flow

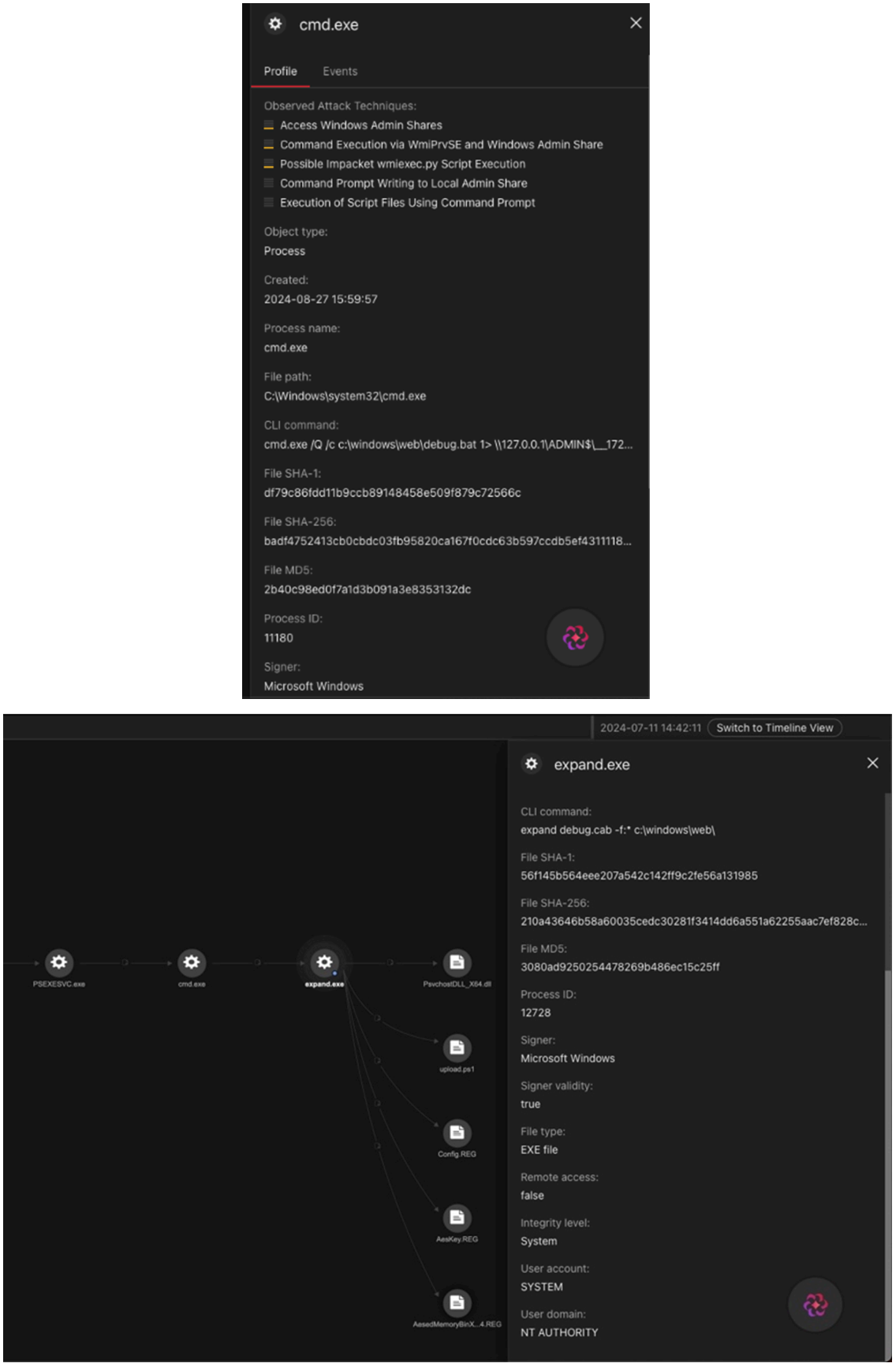

Figure 12. The DEMODEX rootkit installation flow observed in Trend Vision One™

Additional C&C infrastructure analysis

Deploying the MASOL backdoor (aka Backdr-NQ) on a Linux server

While investigating the C&C infrastructure related to Campaign Alpha, we tracked the associated C&C IP (103.159.133[.]251) to a Linux backdoor (name: dash_board, SHA256: 44ea2e85ea6cffba66f5928768c1ee401f3a6d6cd2a04e0d681d695f93cc5a1f). Our analysis confirmed that this sample is linked to the MASOL RAT, which we identified in 2020 and observed being used to target Southeast Asian government entities (Figure 13). Based on the backdoor's PDB string (E:\Masol_https190228\x64\Release\Masol.pdb), we believe the backdoor may have been developed as early as 2019. We observed the new Linux variant of MASOL in the wild after 2021. However, we haven't seen the Windows variant of MASOL after 2021. Currently, we have moderate to high confidence that Earth Estries uses MASOL RAT to target Linux servers within Southeast Asian governments recent years.

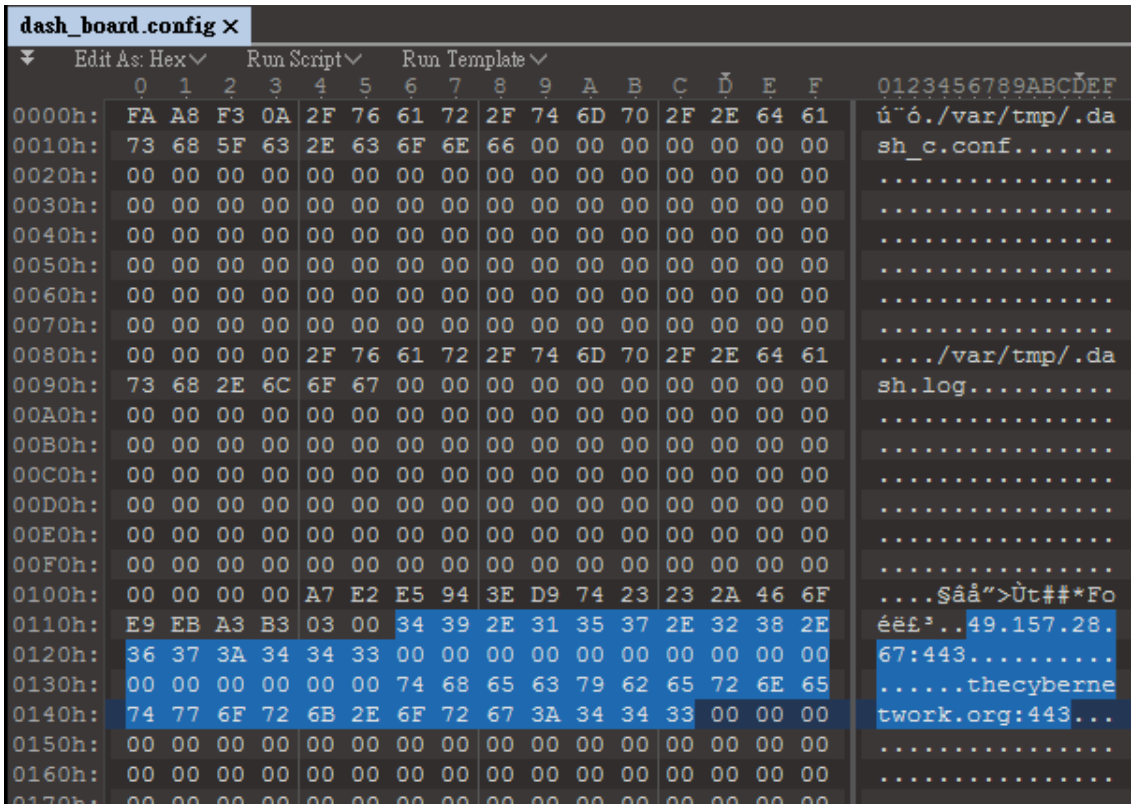

Figure 13. The extracted MASOL RAT malware configuration

Based on the following reasons, we currently only have low confidence that Earth Estries has previously deployed the MASOL RAT through CVE-2022-3236:

- Since August of this year, we have observed a new campaign launched by Earth Estries targeting Southeast Asian governments. Our Deep Discovery Inspector (DDI) detected a compromised Linux server communicating with the MASOL RAT C&C. During the same period, we also observed other compromised hosts within the same organization communicating with the C&C infrastructure associated with the sub-domain of CrowDoor backdooropen on a new tab. We will continue monitoring this ongoing campaign and may provide more details after we have completed our investigation.
- We didn't find any C&C infrastructure that overlaps between our research and the Sophos reportopen on a new tab. Although we only observed limited MASOL RAT IOCs in the wild, we cannot rule out the possibility that MASOL RAT is a shared tool among limited Chinese APT threat groups.

Additional GHOSTSPIDER C&C infrastructure

Currently, we do not have sufficient evidence to attribute the DEMODEX rootkit and GHOSTSPIDER as a proprietary backdoor used by Earth Estries. Therefore, we will only list the C&C infrastructure used by two campaigns discussed above in the IOC section. However, we discovered some interesting GHOSTSPIDER C&C infrastructure.

In the certificate used by the GHOSTSPIDER C&C 141.255.164[.]98:2096 (C&C active timeline: August 2, 2024 to August 22, 2024), we found that one of the certificate's alternative names, "palloaltonetworks[.]com", was mentioned in a vendor reportopen on a new tab related to a Inc Ransom attack (Figure 14). Although we haven't observed any GHOSTSPIDER-related incidents that links it to Inc Ransom, based on these OSINT findingsopen on a new tab, it is possible that Earth Estries may use ransomware in their operations for espionage or for financial gain.

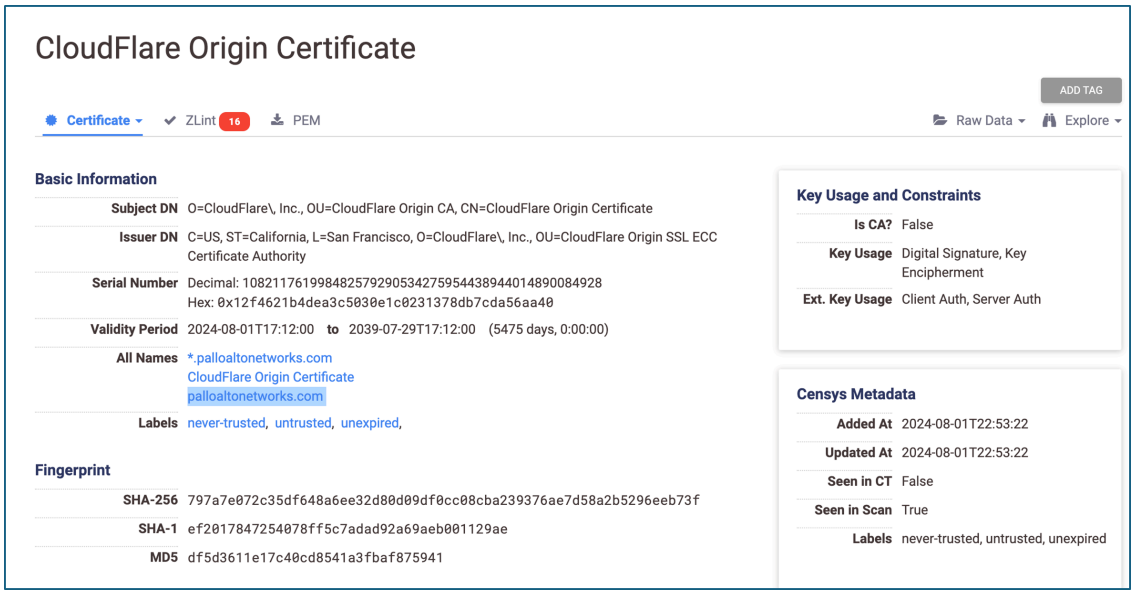

Figure 14. Certificate used by GHOSTSPIDER

Attribution

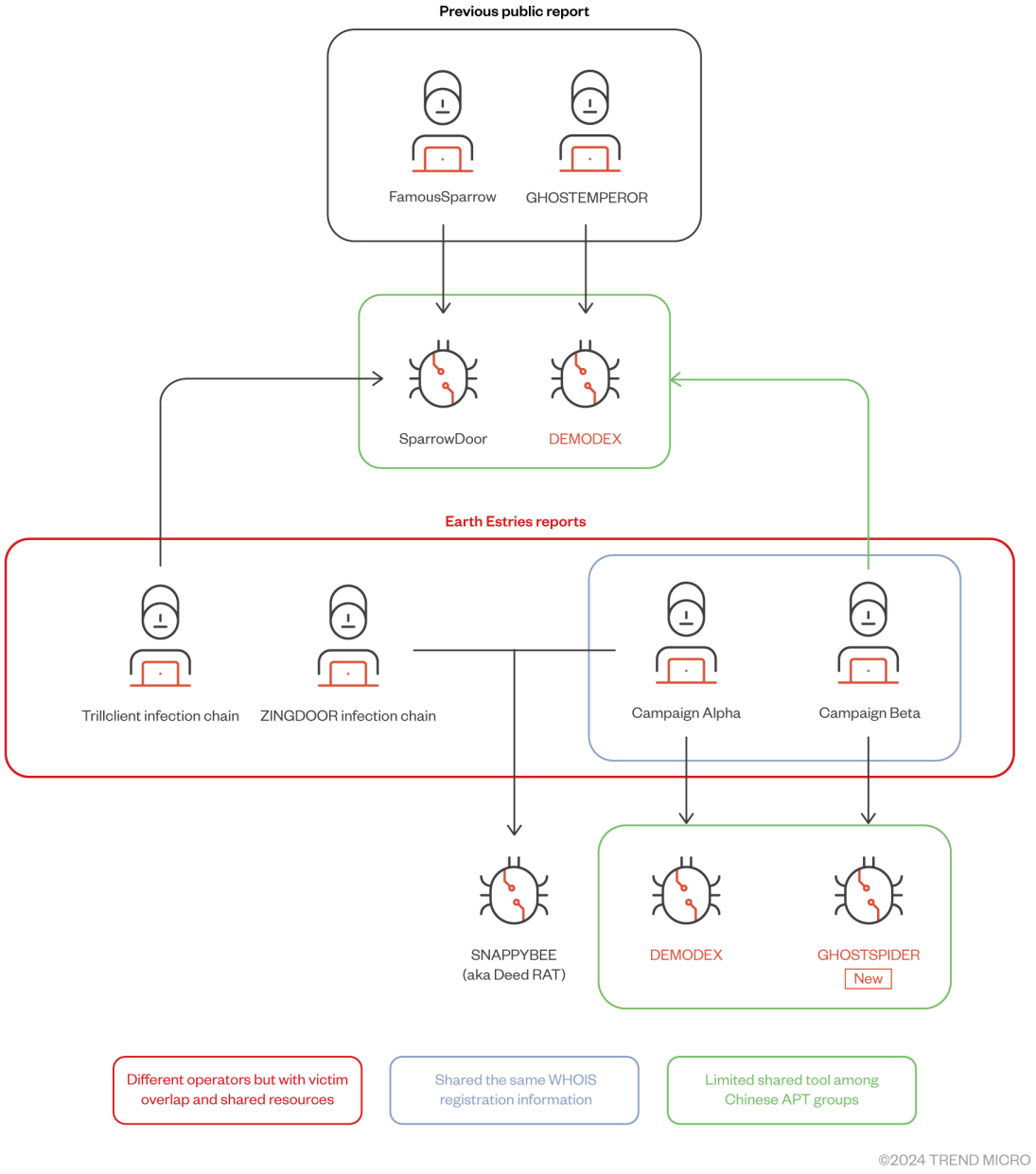

Figure 15. Attribution overview (demonstrates a possible joint operation across different units)

In our first Earth Estries blog entryopen on a new tab, we found some TTPs that overlapped between Earth Estries and FamousSparrowopen on a new tab. Since then, we have found the two campaigns that are related to the DEMODEX rootkit mentioned in GhostEmperor report. Since we found that the attacker also used SNAPPYBEE, we suspect that the tools used by Earth Estries might come from different malware-as-a-service (MaaS) providers. We attribute the two campaigns to Earth Estries with high confidence based on the following shared TTPs:

1. Campaign Alpha and Campaign Beta's C&C domain shared the same WHOIS registration information.
2. Both campaigns utilized the DEMODEX rootkit and GHOSTSPIDER.
3. We observed the DEMODEX, SparrowDoor, and CrowDoor used the same C&C infrastructure in the past. Additionally, the C&C 27.102.113[.]240 was mentioned in the FamousSparrowopen on a new tab and GhostEmperoropen on a new tab reports. Therefore, we believe that Earth Estries has used DEMODEX, GHOSTSPIDER, SparrowDoor and CrowDoor. But we're not sure if these customized backdoors are

proprietary tools used by Earth Estries, so some of the C&C infrastructure cannot be attributed to this threat group.

Based on our telemetry, we observed that the Campaign Alpha actors deployed another x86 SNAPPYBEE sample set at %SYSTEMROOT%\assembly\imfsbDll.dll (SHA256: 6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc) and %SYSTEMROOT%\assembly\DgApi.dll (SHA256: 25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b) in their operations on October 10, 2024. We detected the same hashes in two other government entities.

We also found that one of these government entities had been compromised by Earth Estries since 2020. Notably, SNAPPYBEE was deployed in the ZINGDOOR attack chains on October 13, 2024. This is why we believe Earth Estries used distinct C&C infrastructure for different targets, and that the operations might have been launched by different teams. Some of the TTPs differ significantly, even though the same toolset was shared.

It's worth noting that we observed the following C&C infrastructure overlapping across multiple victim environments. First, we found DEMODEX and Cobalt Strike beacon samples in the same infected machine. The DEMODEX C&C domain pulseathermakf[.]com is used by operator of Campaign Beta. The Cobalt Strike beacon C&C cloudlibraries[.]global[.]ssl[.]fastly[.]net (with the sample downloaded from the C&C hxxp://103.159.133[.]205/lib3.cab) and the post-exploitation activity is linked to [TrillClient attack chainsopen on a new tab](), which involve the Hemigate, SparrowDoor, and CrowDoor toolsets.

Next, we found that the DEMODEX C&C domain pulseathermakf[.]com has been used to target a Southeast Asian government agency for several years. However, on August 28, 2024, we detected a network connection to pulseathermakf[.]com from a compromised server belonging to a Southeast Asian telecommunications company (Campaign Beta). We speculate that the attacker may have made a mistake while deploying the backdoor. Currently, we observe that the attacker primarily uses the DEMODEX C&C domains www[.]infraredsen[.]com and imap[.]dateupdata[.]com to target multiple Southeast Asian telecom companies.

During our investigation of Campaign Beta, we discovered the GHOSTSPIDER backdoor. Subsequently, while tracking the C&C infrastructure related to GHOSTSPIDER, we found that the attacker had also tested GHOSTSPIDER on the Campaign Alpha open directory C&C server 23.81.41[.]166.

Basic Information

Subject DN	O=Acme Co
Issuer DN	O=Acme Co
Serial Number	Decimal: 97440775773902486048119504544886212032 Hex: 0x494e692951aae0b10bdbfba9af7cc5c0
Validity Period	2020-01-24T12:00:00 to 2020-01-24T12:00:00 (0:00:00) Expired
All Names	23.81.41.166
Labels	expired, untrusted, self-signed, never-trusted,

Fingerprint

SHA-256	b63c82fc37f0e9c586d07b96d70ff802d4b707ffb2d59146cf7d7bb922c52e7e
SHA-1	7118b65c86bb5ad3e751f900c76bb92c3d3854ba
MD5	5364d44359f6127c5867e73fcd1ac935

Public Key

Key Type	ECDSA (P-256)

Key Usage and Constraints

Is CA?	False
Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Server Auth

Censys Metadata

Added At	2023-11-02T11:20:36
Updated At	2024-01-23T22:43:39
Seen in CT	False
Seen in Scan	True
Labels	expired, untrusted, self-signed, never-trusted

Figure 16. The certificate (SHA256: b63c82fc37f0e9c586d07b96d70ff802d4b707ffb2d59146cf7d7bb922c52e7e) used by GHOSTPSIDER (Campaign Alpha)

Conclusion

Earth Estries is one of the most aggressive Chinese APT groups, primarily targeting critical industries such as telecommunications and government sectors. Their notable TTPs include exploiting known vulnerabilities and using widely available shared tools, such as SNAPPYBEE. Earth Estries conducts stealthy attacks that start from edge devices and extend to cloud environments, making detection challenging. They employ various methods to establish operational networks that effectively conceal their cyber espionage activities, demonstrating a high level of sophistication in their approach to infiltrating and monitoring sensitive targets.

It is crucial for organizations and their security teams to remain vigilant and proactively strengthen their cybersecurity defenses against cyberespionage campaigns. Through technologies like Trend Vision One™open on a new tab, security practitioners can visualize all organizational components from a single platform, enabling them to monitor and track tools, behaviors, and payloads as they navigate their organization's networks, systems, and infrastructure, while simultaneously detecting and blocking threats as early in the attack or infection process as possible.

Trend Micro Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Micro customers can access a range of Intelligence Reports and Threat Insights within Trend Micro Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and better prepared for emerging threats. It offers comprehensive information on threat actors, their malicious activities, and the techniques they use. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and respond effectively to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

- Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

Trend Micro Vision One Threat Insights App

- Threat Actors: Earth Estriesopen on a new tab
- Emerging Threats: Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusiopen on a new tabons

Hunting Queries

Trend Micro Vision One Search App

Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Hunting DEMODEX Malware

```
objectFilePath:"PsvchostDLL_X64.dll" OR
objectFilePath:"AesedMemoryBinX64.REG" OR
objectFilePath:"msmp4dec.dll" OR objectFilePath:"wpccfg.dll" OR
objectFilePath:"dumpfiskfss.sys" OR
objectFilePath:"SstpCfs.dll"
```

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledopen on a new tab.

Yara Rules

Download the YARA rules hereopen on a new tab.

Indicators of Compromise

Download the list of IOCs hereopen on a new tab. This IOC list was last updated on October 31, 2024, during which we observed some of IOCs were still used in the ongoing campaigns. This is not a comprehensive list of IOCs, because most of the related components of DEMODEX and GHOSTSPIDER have different file hashes for different endpoints. We will release more IOCs and hunting queries on the Vision One platform.

Tags
