Earth Estries Targets Government, Tech for Cyberespionage

trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

August 30, 2023

APT & Targeted Attacks

We break down a new cyberespionage campaign deployed by a cybercriminal group we named Earth Estries. Analyzing the tactics, techniques, and procedures (TTPs) employed, we observed overlaps with the advanced persistent threat (APT) group FamousSparrow as Earth Estries targets governments and organizations in the technology sector.

By: Ted Lee, Lenart Bermejo, Hara Hiroaki, Leon M Chang, Gilbert Sison August 30, 2023
Read time: (words)

Earlier this year, we discovered a new cyberespionage campaign by a hacker group we named Earth Estries. Based on our observations, Earth Estries has been active since at least 2020. We also found some overlaps between the tactics, techniques, and procedures (TTPs) used by Earth Estries and those used by another advanced persistent threat (APT) group, FamousSparrow.

From a general overview of the tools and techniques used in this ongoing campaign, we believe the threat actors behind Earth Estries are working with high-level resources and functioning with sophisticated skills and experience in cyberespionage and illicit activities. The threat actors also use multiple backdoors and hacking tools to enhance intrusion vectors. To leave as little footprint as possible, they use PowerShell downgrade attacks to avoid detection from Windows Antimalware Scan Interface's (AMSI) logging mechanism. In addition, the actors abuse public services such as Github, Gmail, AnonFiles, and File.io to exchange or transfer commands and stolen data.

This active campaign targets organizations in the government and technology industries based in the Philippines, Taiwan, Malaysia, South Africa, Germany, and the US. We detail our findings and technical analysis in this entry to guide security teams and organizations in reviewing the status of their respective digital assets and for them to enhance their existing security configurations.

Infection vector

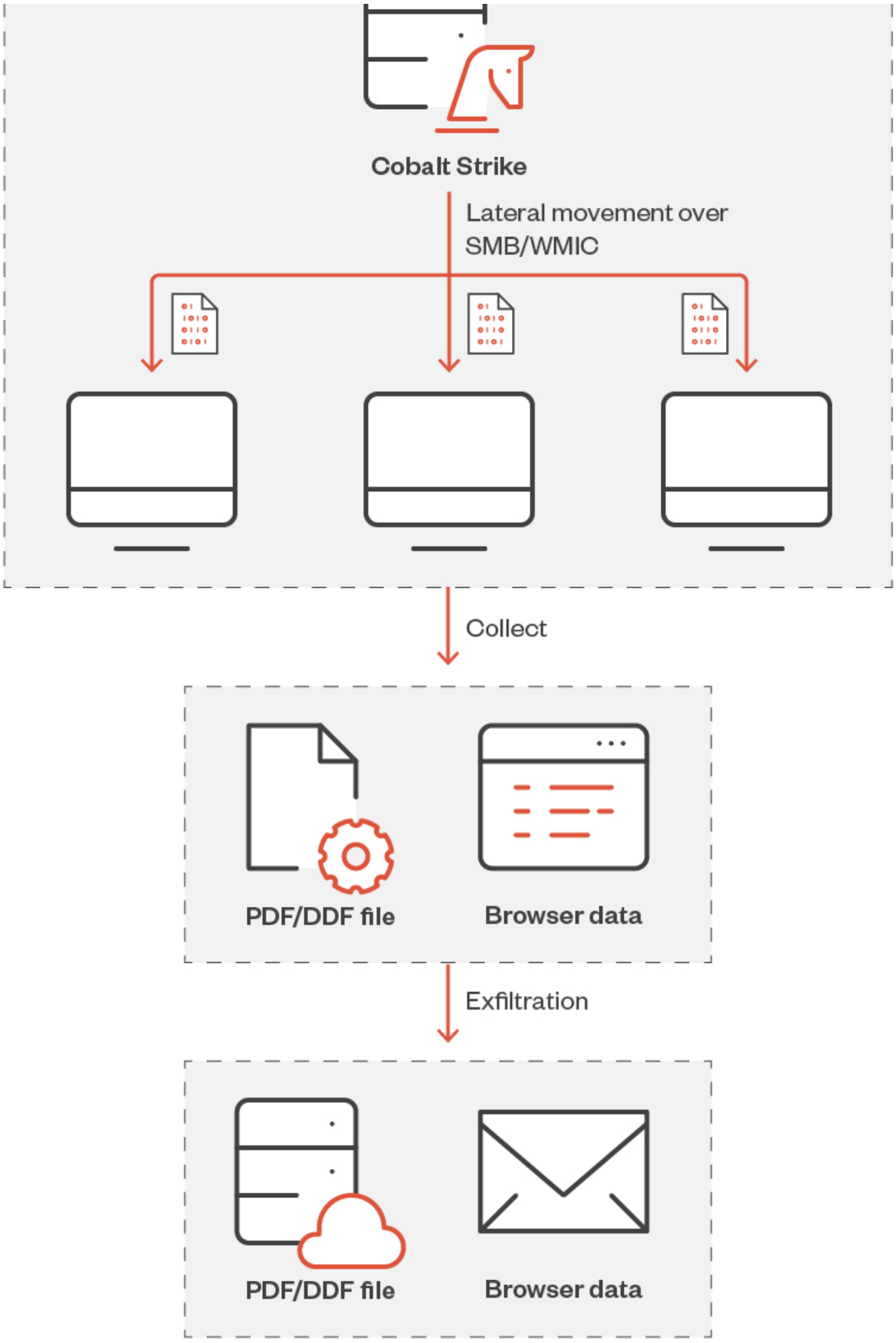


Figure 1. The attack routine of Earth Estries

We found Earth Estries compromising existing accounts with administrative privileges after it successfully infected one of the organization's internal servers. By installing Cobalt Strike on the system, the actors behind Earth Estries were able to deploy more pieces of malware and perform lateral movement. Through the Server Message Block (SMB) and WMI command line (WMIC), the threat actors propagated backdoors and hacking tools in other machines in the victim's environment. At the end of each round of operations in a series of deployments, they archived the collected data from a specified folder. According to our samples and analysis, the threat actors targeted PDF and DDF files, which the actors uploaded to online storage repositories AnonFiles or File.io using *curl.exe*.

We also noted that the threat actors regularly cleaned their existing backdoor after finishing each round of operation and redeployed a new piece of malware when they started another round. We believe that they do this to reduce the risk of exposure and detection.

Backdoor and hacking tools

We observed the threat actors using various tools in this campaign, including information stealers, browser data stealers, and port scanners, among others. In this section, we focus on newly discovered and noteworthy toolsets and discuss their technical details.

Zingdoor

Zingdoor is a new HTTP backdoor written in Go. While we first encountered Zingdoor in April 2023, some logs indicate that the earliest developments of this backdoor took place in June 2022. However, it had rarely been seen in the wild and had only been observed being used in a limited number of victims, likely as a newly designed backdoor with cross-platform capabilities. Zingdoor is packed using UPX and heavily obfuscated by a custom obfuscator engine.

We noted that Zingdoor adopts anti-UPX unpacking techniques. Generally, the magic number of UPX is "UPX!", but in this case it was modified to "MSE!", and the UPX application cannot unpack this modified file. This technique is easy and in internet of things (IoT) types of malware, but it is considered rare in APT activities.

Zingdoor was disguised as mpclient.dll and designed to run via DLL sideloading by abusing Windows defender binary MsSecEs.exe. Upon running the executable, Zingdoor registers the current parent process as a Windows service with the name "MsSecEsSvc" for persistence and starts it. As a service process, Zingdoor connects and waits for a command from the command-and-control (C&C) server. Based on the functions defined in the backdoor, it supports the following capabilities:

- Get system information

- Get Windows service information
- Disk management (file upload/download, file enumeration)
- Run arbitrary commands

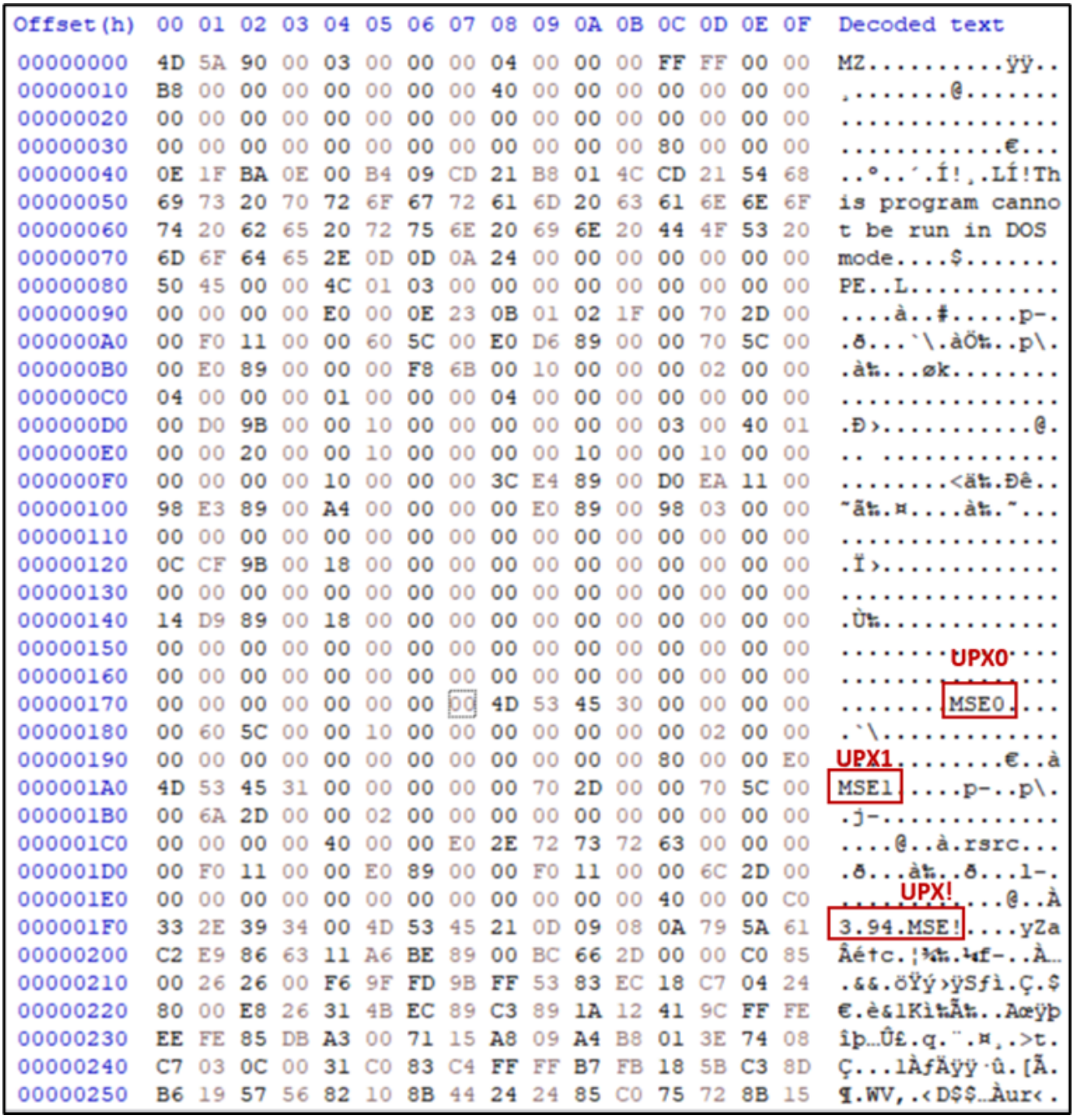


Figure 2. Modified UPX header for anti-UPX unpacking technique

TrillClient

TrillClient toolset is an information stealer designed to steal browser data, and is packed in a single cabinet file (.cab) and extracted through the utility application *expand.exe*. The CAB file contains a TrillClient installer and a stealer. Based on different arguments, the installer performs the following behaviors:

Table 1. TrillClient arguments and behaviors

Argument	Description
-install	Installs itself as Windows service Net Connection
-start {victim id}	• Creates a victim list based on the input victim ID (File name: *7C809B4866086EF7FB1AB722F94DF5AF493B80DB*) • Launches the TrillClient stealer through starting services
-remove	Cleans up the installation (Deletes the service)

As TrillClient is a custom browser data stealer written in Go, it is heavily obfuscated by a custom obfuscator for anti-analysis. Once launched, it looks for the victim list, *7C809B4866086EF7FB1AB722F94DF5AF493B80DB* created by the installer. Afterward, it connects to a GitHub repository to retrieve the command for the next set of actions. The repository address is hard-coded in the malware as follows: *hxxps://raw[.]githubusercontent[.]com/trillgb/codebox/main/config.json.*

Figure 3. Sample content of “config.json”

Value.name is the victim ID, while value.value is a command. After receiving this configuration, TrillClient looks for its own victim ID in the value.name list, and performs malicious activities based on the command defined by value.value. TrillClient supports the following commands:

Table 2. TrillCient commands and functions

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)

TrillClient steals the sensitive data found in the following directories:

- %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*

The collected data will be temporarily copied to *<%TEMP%\browser_temp_data<RANDOM>>*, archived usingthe .tar command, and encrypted with an XOR algorithm. Then the collected data will be sent to the threat actor's email account *trillgamby@gmail[.]com* over SMTP (Simple Mail Transfer Protocol). Another noteworthy capability of TrillClient is its ability to update its version. As the value of "version" defined in the downloaded config is newer than the current version number, it will download the newer one from the GitHub repository and update itself.

HemiGate

HemiGate is a backdoor used by Earth Estries. Like most of the tools used by this threat actor, this backdoor is also executed via DLL sideloading using one of the loaders that support interchangeable payloads. *K7AVMScn.exe* from K7 Computing is the sideloading host utilized by this backdoor, while the loader poses as *K7AVWScn.dll*. The main backdoor is an encrypted file named *taskhask.doc*, and another encrypted file named *taskhask.dat* serves as the configuration file.

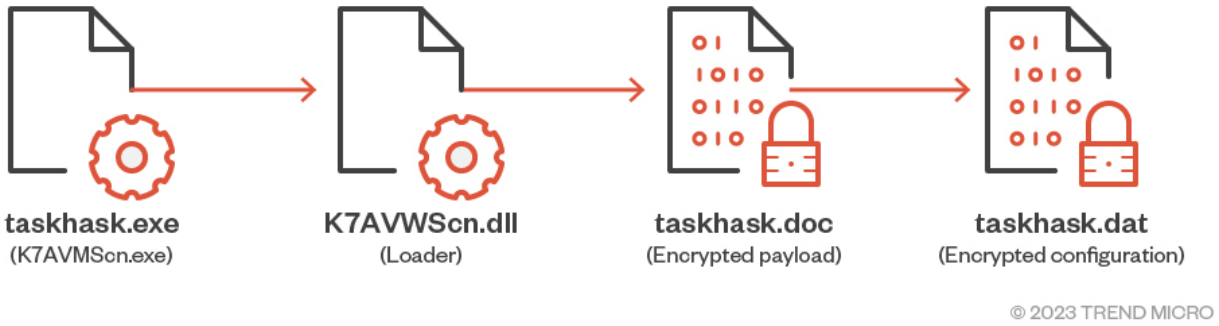


Figure 4. HemiGate sideloading sequence

HemiGate communicates to its C&C server over port 443 and performs a connection via proxy if required by the environment. The C&C server is retrieved from the configuration file, which mainly contains C&C server and port combinations. The config file is decrypted using RC4 encryption with the key *4376dsygdYTFde3*. This RC4 key is also used in other encryption/decryption functions performed by the backdoor in most of its routines. Communication with the server is performed using POST method, using the following predefined header:

```
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
```

Figure 5. HemiGate communication header

HemiGate executes in three instances:

- First instance. This instance is launched without any parameter. Its main purpose is to install startup mechanisms and execute the second instance. This instance will terminate once its purpose is finished.
    - Startup 1. An entry in the autostart registry named “Windrive” is created.
    - Startup 2. A service called “Windrive” with the full service name “Windows Drive Security” is created as another startup mechanism.

- Second instance: Executed with the */a* argument, this instance is responsible for reading the config file and communicating with the C&C server. It also serves as the launcher and will communicate with the third instance via named pipes. In addition, the second instance performs the following functions:
    - Updates the configuration
    - Receives the data captured by the keylogger function via pipe and logs it into a file
    - Serves as watchdog for the third instance
    - Directly executes backdoor commands if the parameter is satisfied or if the pipe communication fails
    - Passes backdoor command execution to the third instance if the parameter from the C&C is true and the pipe communication is successful
    - Executes a full uninstall if the command is received from the C&C
- **Third instance.** This instance is launched with the */u <PID of instance 2>* argument. The following are its two main functions:
    - Executes the keylogger routine and passes captured data to the second instance via pipe communication

        Keylogger communication is done via *\\[.]\pipe\Key[500]*
    - Opens a pipe to receive and executes commands passed by the second instance

        Commands are received via *\\[.]\pipe\<username>\[<session number>]*

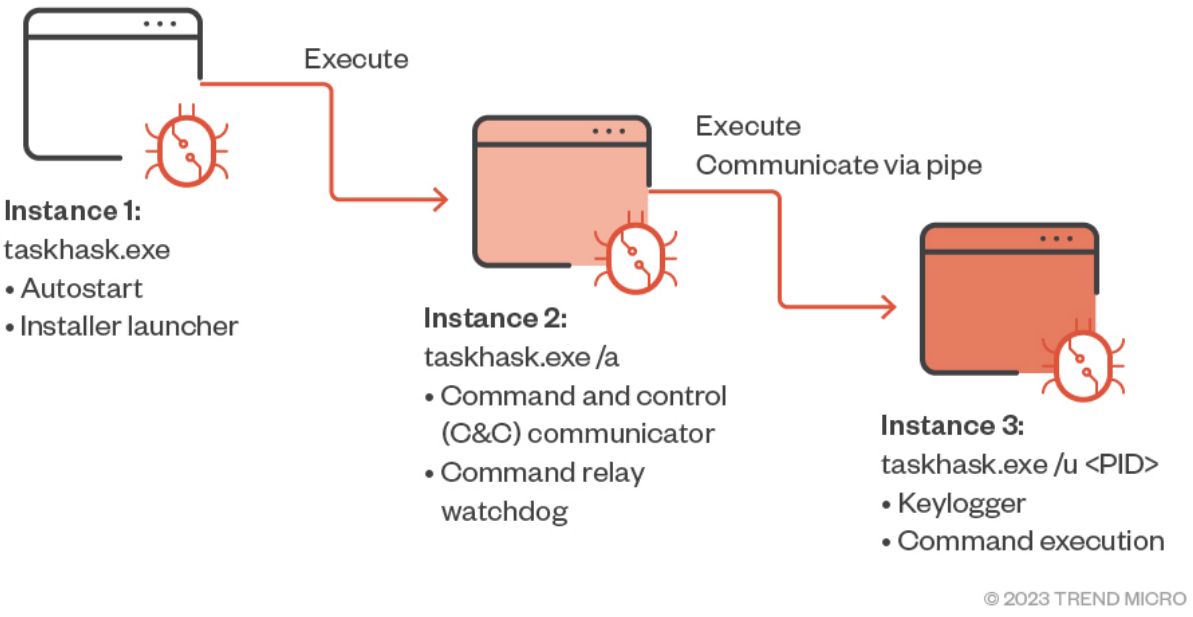


Figure 6. HemiGate process tree

The keylogger feature utilizes a non-interactive static control window by creating a window with a predefined “static” class. A timer function is then used alongside a keyboard hook to log the keystrokes on an active window continuously, so long as the window remains active. The keystroke is logged using the following structure:

- User: Active user at the time of logging
- Title: Active window title
- Time: Time of the keystroke log (format: dd/mm hh:mm:ss)
- Key: Logged keystrokes

Aside from the keylogger, the following features are also available:

- Directory monitoring: Sets a directory notification handle to receive notifications for added files, deleted files, changes in files, and file name changes (records old and new names) in the target directory. The changes recorded are stored in the file named “fm.”
- File content read/write: Allows to write contents to a target file or to read the contents of the target file.
- File operations: Performs operations like enumerate drives, move, copy, rename, or delete files, create directories, or open files using their default applications.
- Shell: Launches an interactive command shell.
- CMD: Executes a command via cmd (one-time execution).
- Screenshot: Takes a screenshot of the active desktop window.
- Process monitor: Enumerates currently running processes and allows the termination of a target process.

Heavy use of DLL sideloading

We observed that Earth Estries relies heavily on DLL sideloading to load various tools within its arsenal. Aside from the backdoors previously mentioned, this intrusion set also utilizes commonly used remote control tools like Cobalt Strike, PlugX, or Meterpreter stagers interchangeably in various attack stages. These tools come as encrypted payloads loaded by custom loader DLLs.

A notable feature of the loaders used is that the decryption key is in the encrypted payload. We observed that this intrusion set utilizes the same loader file while loading a different payload in the same target environment.

During our investigation, we learned several sideloading combinations used by Earth Estries and enumerate them in the following table:

Table 3. Legitimate executables and sideloaded DLLs abused by Earth Estries

Affected vendor	**Legitimate executables**	**Sideloaded DLL**
Canon Inc.	*ijplmui.exe*	*IJPLMCOM.dll*
Brother Industries Ltd (Signer: Dell Inc.)	*brdifxapi.exe*	*brlogapi.dll / brlogapi64.dll*
IObit Malware Fighter	*imfsbCrypto.exe*	*imfsbDll.dll*

K7 Computing Pvt Ltd	*K7AVMScn.exe*	*K7AVWScn.dll*
K7 Computing Pvt Ltd	*K7TSVlog.exe*	*K7UI.dll*
K7 Computing Pvt Ltd	*K7SysMon.EXE*	*K7SysMn1.dll*
Microsoft Corporation	*iisexpresstray.exe*	*mscoree.dll*
Netgate Technologies s.r.o.	*seanalyzertool.exe*	*msimg32.dll*
Oracle Corporation	*jps.exe*	*jli.dll*
iTop Inc. (Signer: Orange View Ltd)	*graphics-check.exe* (renamed as *sfc.exe* by attacker)	*dxgi.dll*
Xanasoft.com	*SandboxieBITS.exe*	*SbieDll.dll*

By and large, the DLL sideloading attacks we've observed are against older versions of legitimate files, some even a decade old, in a bid to convert them into LOLBins. Attackers are using this opportunistic tactic in the hopes of them being ignored by security products. This situation makes it even more important to implement version controls and application baselines to detect anomalies and prevent attackers from gaining footholds in the enterprise environment.

C&C server infrastructure

We observed that some of the Cobalt Strike implants Earth Estries used utilized Fastly CDN service to hide the actual IP address. We've also previously observed the use of Fastly CDN in other campaigns by some APT41-related groups such as Earth Longzhi and GroupCC.

Looking into other Earth Estries' C&C activities observed from their victims' environments, we discovered some notable pieces of data in the registrant information as follows:

Table 4. Information on C&C activities referenced with WHOIS protocol

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

The domains observed in Table 4 were observed from real incidents. According to public repositories, those C&C domains share the same registrant information. We infer that the domains have preferences when it comes to registrant information. In addition, these domains share similar C&C address formats, some of which we observed while tracking their operations. While our investigation is ongoing to determine whether these domains and registrant data are related to the threat actors, we do know that these pieces of information can be used to pivot other related C&C domains, likely used by the same group.

Based on the registrant information, we found more records of the old domain registered by the threat actors.

Table 5. History of registered domains following the keyword “De Wang Mao Yi You Xian Gong Si”

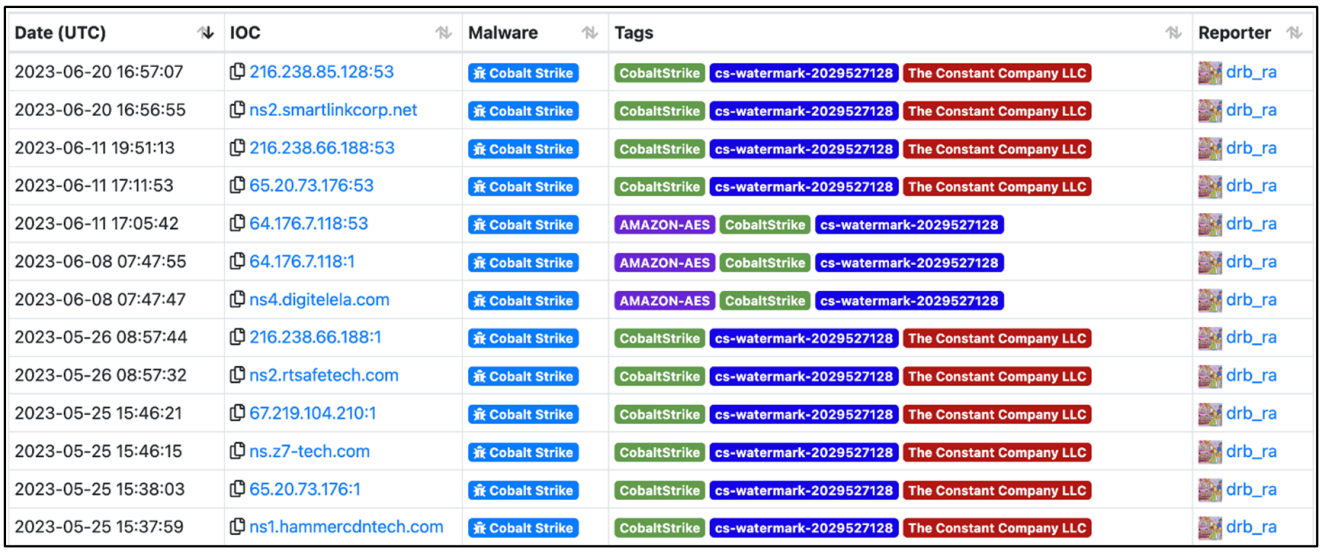
Domain keyword search: "De Wang Mao Yi You Xian Gong Si"		
Domain	**Registered/First seen**	**Expires/ Last seen**
rtsafetech.]com	Oct 8, 2022	Oct 8, 2023
keyplancorp[.]com	Dec 22, 2021	Dec 16, 2023
trhammer[.]com	Sep 5, 2022	Jul 12, 2023 (Last seen)
rthtrade[.]com	Nov 23, 2021	Nov 23, 2023
smartlinkcorp[.]net	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)

Table 6. History of registered domains following the keyword “3280132818@qq.com”

Domain keyword search: “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

Checking all the domains, we observed that *smartlinkcorp[.]net* yielded the most information from public repositories and the threat intelligence community. Digging into the domain, we discovered a record of a related subdomain, "*ns2.smartlinkcorp[.]net*". In addition, Cobalt Strike was once hosted on *ns2.smartlinkcor[.]net* with the watermark *2029527128*. Based on the watermark, we found more related domains and IP records.



Date (UTC)	IOC	Malware	Tags	Reporter
2023-06-20 16:57:07	216.238.85.128:53	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-06-20 16:56:55	ns2.smartlinkcorp.net	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-06-11 19:51:13	216.238.66.188:53	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-06-11 17:11:53	65.20.73.176:53	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-06-11 17:05:42	64.176.7.118:53	Cobalt Strike	AMAZON-AES CobaltStrike cs-watermark-2029527128	drb_ra
2023-06-08 07:47:55	64.176.7.118:1	Cobalt Strike	AMAZON-AES CobaltStrike cs-watermark-2029527128	drb_ra
2023-06-08 07:47:47	ns4.digitelela.com	Cobalt Strike	AMAZON-AES CobaltStrike cs-watermark-2029527128	drb_ra
2023-05-26 08:57:44	216.238.66.188:1	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-05-26 08:57:32	ns2.rtsafetech.com	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-05-25 15:46:21	67.219.104.210:1	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-05-25 15:46:15	ns.z7-tech.com	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-05-25 15:38:03	65.20.73.176:1	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra
2023-05-25 15:37:59	ns1.hammercdntech.com	Cobalt Strike	CobaltStrike cs-watermark-2029527128 The Constant Company LLC	drb_ra

Figure 7. Cobalt Strike records found

From these Cobalt Strike records, we noticed two new domains, *digitelela[.]com* and *z7-tech[.]com*, which we did not observe in our initial investigations. We then found another domain set possibly used by the threat actors based on the registrant information.

Table 7. Registered domains' histories following the keyword "3087384364@qq[.]com"

Domain keyword search: "*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.

Like the domain sets we found listed in Table 4, there are several common pieces of information, such as the country registration derived under these domains and subdomains. Specifically, the domains follow a *ns{number}.{domain}* format and are designed for a Cobalt Strike beacon to send and receive commands via DNS tunneling.

- *cdn-xxxxx.{domain}*
- *cdnxxxxxxxx.{domain}*
- *xxxxxx.ns1.{domain}*
- *xxxxxx.ns2.{domain}*
- *xxxxxx.ns3.{domain}*
- *xxxxxx.ns4.{domain}*

Analyzing the preceding C&C domains and the resolved IP addresses, we found their C&C servers hosted on virtual private server (VPS) services located in different countries. We summarize the distribution of C&C servers here:

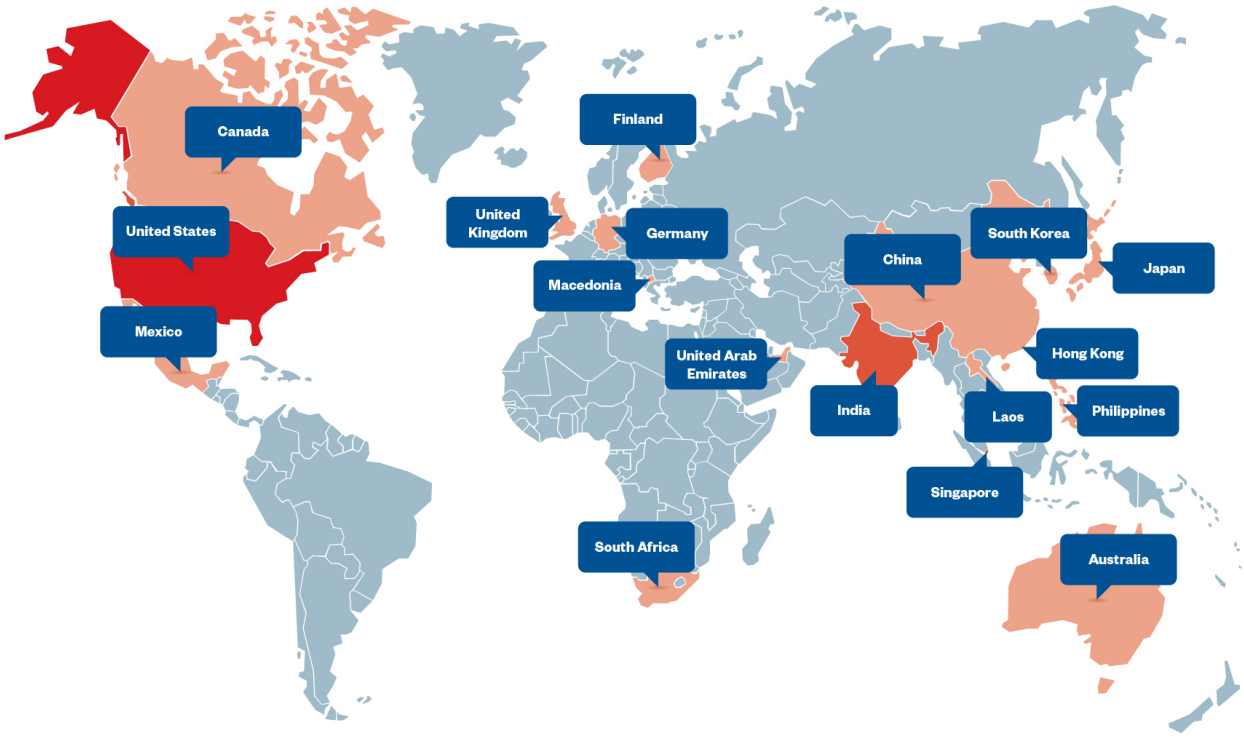


Figure 8. Heat map distribution of C&C server services used by Earth Estries

Victimology

Based on our investigation, Earth Estries focuses its attack targeting and attempts on government-related organizations and technology companies in the Philippines, Taiwan, Malaysia, South Africa, Germany, and the US. We also observed the network traffic to C&C servers in Canada and the occurrence of toolset detections in India and Singapore, making these regions potentially highly affected regions. Organizations in the identified countries should not only reexamine their systems for possible intrusions and unauthorized traffic exchanges but also reinforce their existing security measures.

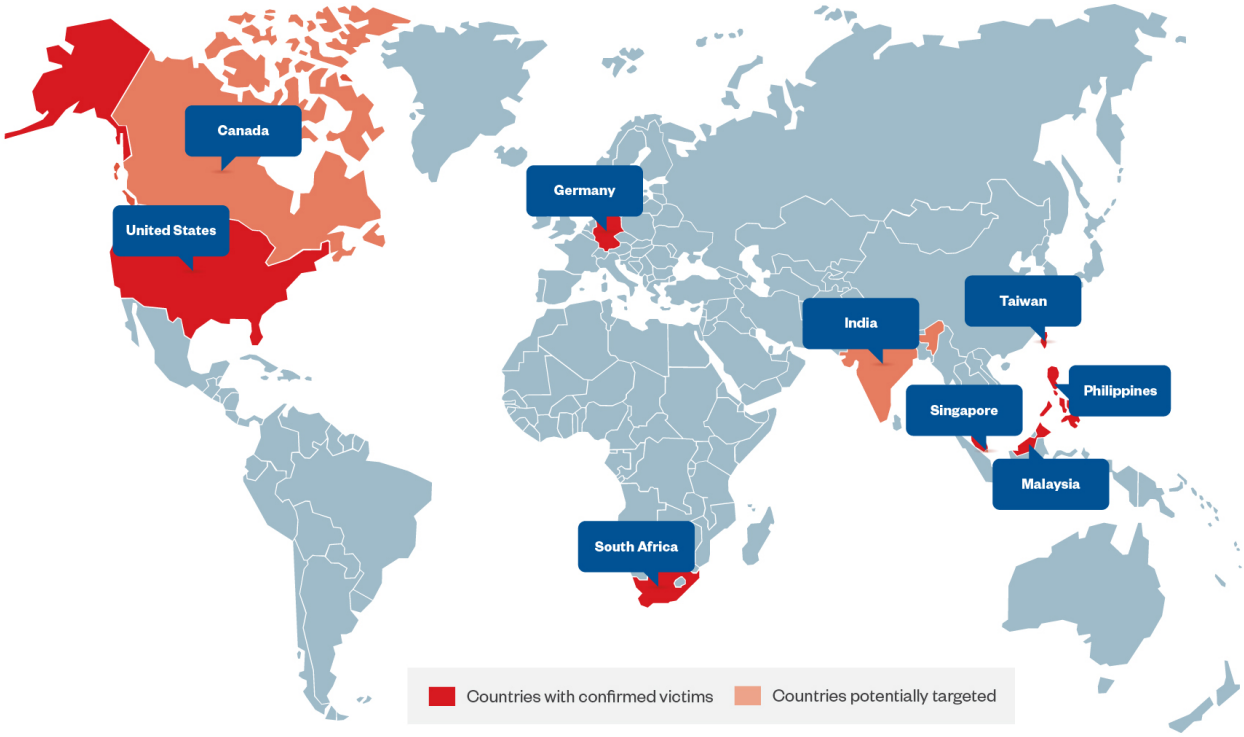


Figure 9. Distribution of targeted and potentially affected countries

Attribution

While tracking the campaign, we noticed the threat actors using “ping” to test if a remote server is available before accessing it. Figure 10 shows one of the tests performed by Earth Estries, at the same time our tracking found that the threat actors tried to see if the remote server with IP address 103.133.137[.]157 is available.

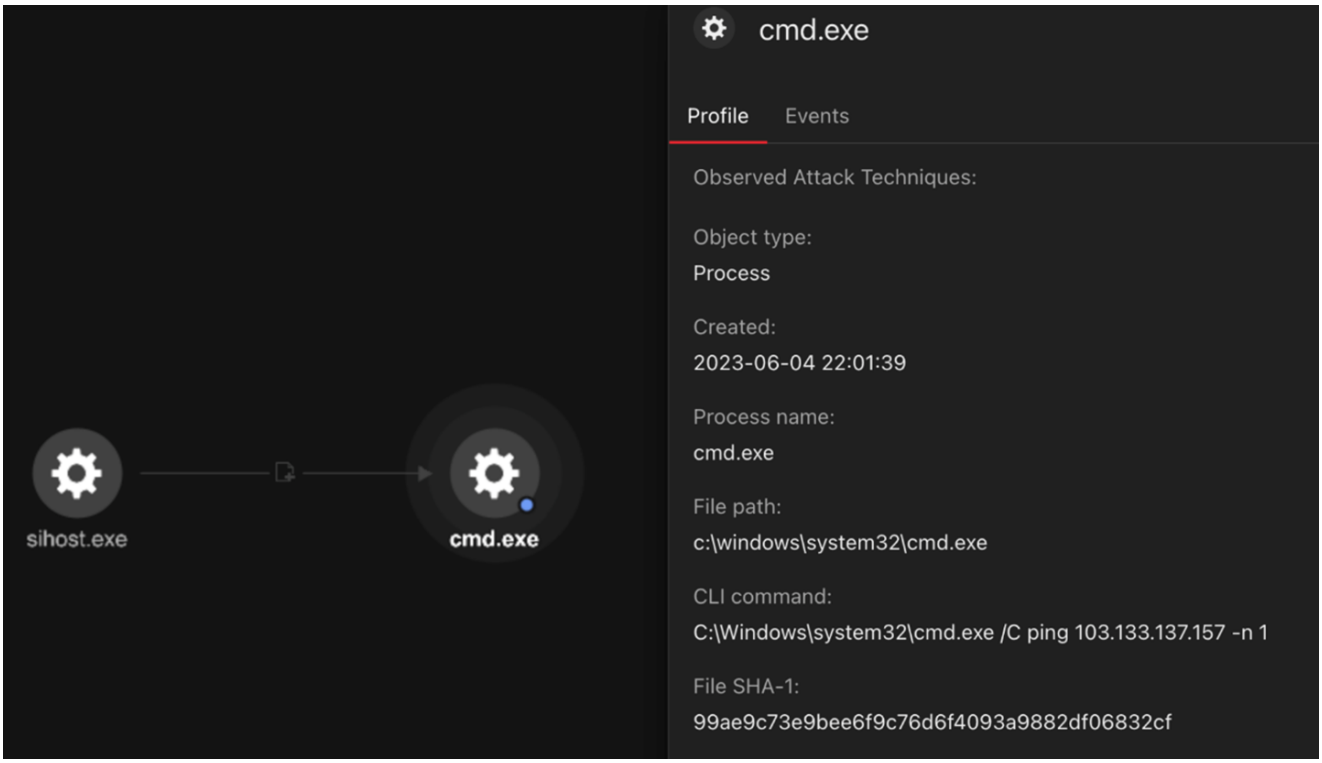


Figure 10. Sample tracking Earth Estries' ping tests (Screenshot taken using Trend Vision One™)

In addition, Earth Estries used some tools and TTPs that overlap with FamousSparrow. We compared the backdoor loader used in this campaign to the loader mentioned in the previous report. As for TTPs, Earth Estries also tends to use .CAB files to deploy their malware and toolset to the victim's environment, which reinforced the tracking we found and initial country reports responsible for the attacks.

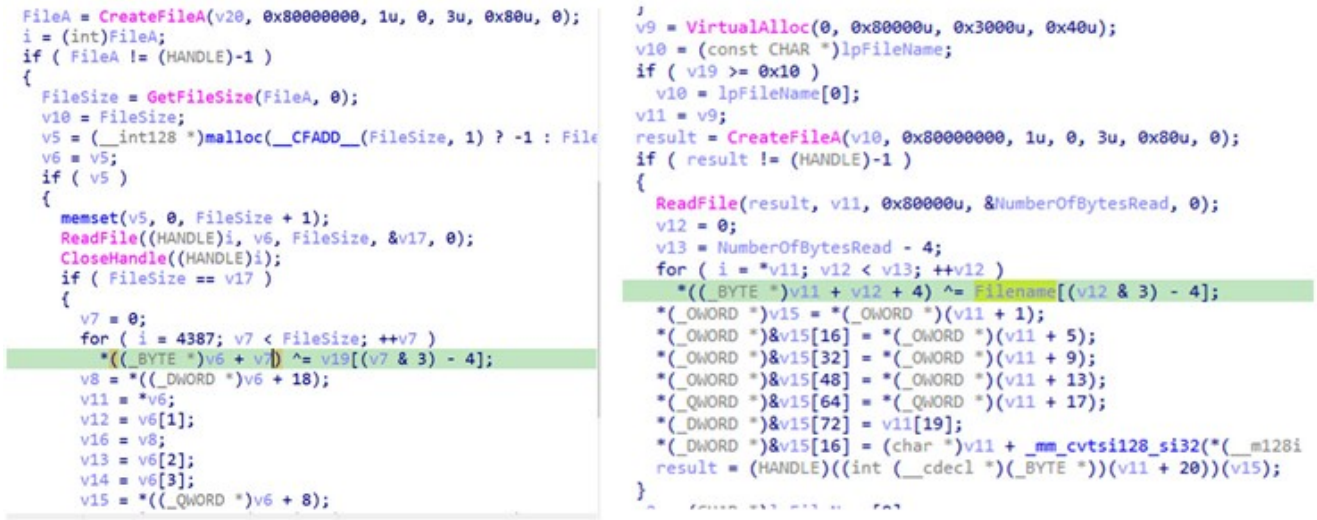


Figure 11. The loader previously mentioned in an earlier report (left), and the loader we observed from the latest campaign (right)

Conclusion

Earth Estries is a sophisticated hacker group that has been active since at least 2020 and that focuses on deploying cyberespionage campaigns. It targets government and technology organizations in various countries and is capable of implementing advanced techniques such as the use of multiple backdoors and hacking tools to gain access to its targets.

By compromising internal servers and valid accounts, the threat actors can perform lateral movement within the victim's network and carry out their malicious activities covertly. The use of Zingdoor as part of the routine to ensure that the backdoor cannot be unpacked easily drive additional challenges for analysts and security teams to make it more difficult to analyze. They also use techniques like PowerShell downgrade attacks and novel DLL sideloading combinations to evade detection. Moreover, the code similarities and TTPs between Earth Estries and FamousSparrow suggests a possible connection between them. Other pieces of evidence, such as tracked IP addresses and common technical formatting themes observed in their operation, indicate strong ties that can be investigated and analyzed further.

Understanding the methods used by Earth Estries can help organizations improve their security measures and protect their digital assets. It is essential for individuals and companies to stay vigilant and take necessary actions to enhance their cybersecurity to safeguard against such cyberespionage campaigns. Trend Vision One™ provides security teams and analysts to visualize all the separate components of the organization from a single platform to monitor and track the tools, behaviors, and payloads as the routine attempts to move and execute in the organization’s networks, systems, and infrastructure while simultaneously detecting and blocking the threats as left of the attack or infection routine as possible.

MITRE ATT&CK

MITRE Tactic	MITRE Technique	Technique ID
Discovery	Account Discovery	T1087
	Domain Trust Discovery	T1482
Execution	Windows Management Instrumentation	T1047
	Command and Scripting Interpreter: PowerShell	T1059.001
	System Services: Service Execution	T1569.002
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002
	Hijack Execution Flow: DLL Side-Loading	T1574.002
	Obfuscated Files or Information: Software Packing	T1027.002
	Obfuscated Files or Information: Command Obfuscation	T1027.010

Defense Evasion	Masquerading: Masquerade Task or Service	T1036.004
	Masquerading: Match Legitimate Name or Location	T1036.005
	Indicator Removal	T1070
	Downgrade Attack	T1562.010
	Access Token Manipulation: Token Impersonation/Theft	T1134.001
Persistence	Scheduled Task	T1053.005
	Boot or Logon Autostart Execution: Registry Run Keys/ Startup Folder	T1547.001
	Create or Modify System Process: Windows Service	T1543.003
	Hijack Execution Flow: DLL Side-Loading	T1574.002
Privilege Escalation	Valid Account	T1078
Collection	Archive Collected Data: Archive via Utility	T1078
	Input Capture: Keylogging	T1056.001
	Screen Capture	T1113
Collection	Application Layer Protocol: Web Protocols	T1071.001
	Application Layer Protocol: DNS	T1071.004
Exfiltration	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002

Indicators of Compromise (IOCs)

Download the list of IOCs here.