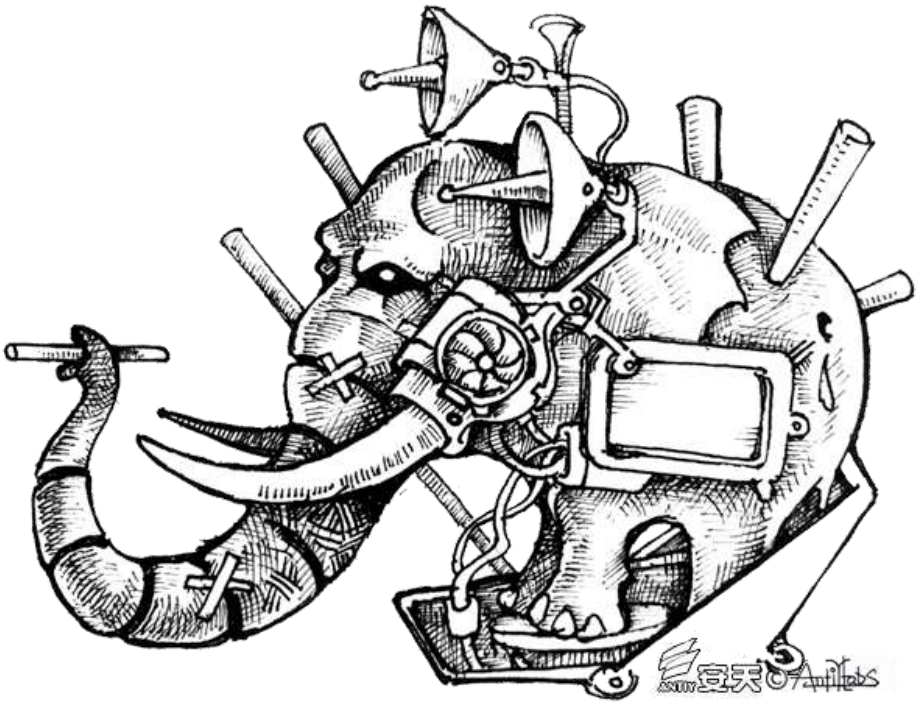
Continued Phishing Attempts Against Endpoint Targets

——Recent Sample Analysis of the "BITTER" Attack Group

Antiy CERT

The original report is in Chinese, and this version is an AI-translated edition.



First published: 2025-05-22 14:15

This version was updated: 2025-05-22 14:15

Scan the QR Code to Get the Latest Report

1 Overview

Since 2012, Antiy Security Research and Emergency Response Center (Antiy CERT) has been continuously paying attention to and analyzing cyber attack activities from the South Asian subcontinent, attributing related organizations and naming the most active organization as White Elephant [1]. We found that there are multiple active organizations in this geo-security direction that are frequently active. Since 2016, Antiy has successively released reports such as "Hidden Elephants" and "Operation PaperFolding", and named several attack organizations such as "White Elephant", "BITTER", "Dark Elephant", "Young Elephant" and "Confucian Elephant". Among them, the "BITTER" organization, also known as "Manlinghua", is a national-level APT organization with a South Asian geopolitical background, just like the White Elephant. Its attack activities can be traced back to 2013. Its attack targets have long focused on government agencies, military enterprises, energy and scientific research institutions in China, Pakistan and other countries, aiming to steal sensitive political, military and technological intelligence. Recently, Antiy CERT has discovered that the organization has been active, delivering various payloads via emails, attempting to attack relevant units and personnel in my country, with the intention of gaining persistent control over target information systems and stealing sensitive information.

This report focuses on the attack waves carried out by the "BITTER" organization in early 2025, analyzes its attack tactics and techniques, and focuses on analyzing its attack weapon samples to provide a reference for domestic users and neighboring countries to improve their prevention capabilities.

2 Phishing Email Analysis

Attackers used Internet email accounts to send a large number of spear-phishing emails in early 2025. One typical phishing email had the subject "Ministry of Foreign Affairs Document" and carried two malicious attachments.

Table 2-12executable files

Attack time	Early 2025
Attack intent	Continuous control and secret theft
Bait type	CHM Help File
Attack method	Spear phishing emails, CHM help file bait
Weapons and equipment	Remote control Trojans , secret stealing Trojans

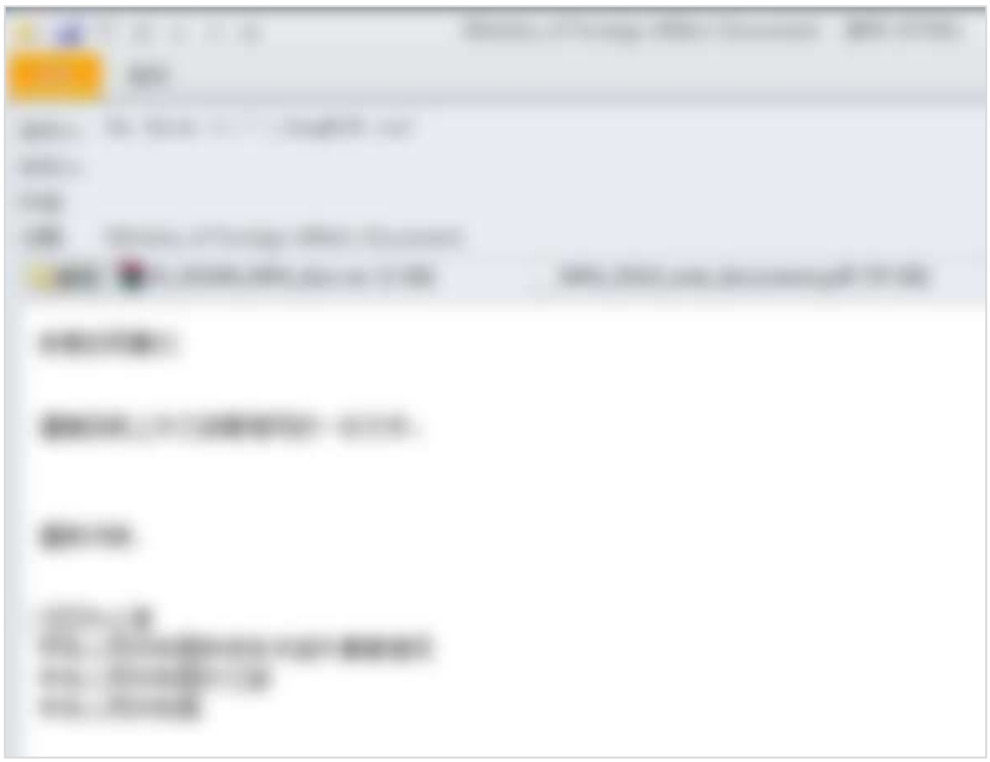


Figure 2-1 2

2.1 Attachment 1: Compressed File

Table 2-3Malicious email attachment 1

Virus name	Trojan/Win32.Agent
Original file name	03_2024N_MFA_doc.rar
MD5	F26C1083B42ADECBBEF7108D1C2A798C
File size	2.79 KB (2,866 bytes)
File format	Archive/ Eugene_Roshal.RAR [:Roshal ARchive]
Last content modification time	October 24 , 2024 14:48:12
Decompression password	None
Include file content	03_2024N_MFA_doc.chm

One of the attachments carried in the phishing email is in the form of a compressed package, which is in the form of a CHM help document after decompression. After the victim opens it, a scheduled task will be added to execute the PowerShell command regularly, thereby obtaining a persistent entry.

Table 2-4Malicious CHM documents

Virus name	Trojan / HTML.Agent [Downloader]
Original file name	03_2024N_MFA_doc.chm
MD5	4B91AB01AD75B5485D4F8D33FA3C0AFF
File size	10.5 KB (10,756 bytes)
File format	Document/Microsoft.CHM[:Microsoft Compiled HTML Help]
Timestamp	October 24 , 2024 14:48:12

CHM (Compiled HTML Help) [3]help document format developed by Microsoft for the Windows platform. It integrates HTML pages, images, CSS style sheets and script resources into a single file (.chm suffix) based on a compound document structure through the LZX compression algorithm. It has both high compression rate and fast retrieval characteristics. It implements structured navigation through a directory tree (.HHC) and an index (.HHK), and supports JavaScript, ActiveX controls and ms -its: protocol hyperlinks. It can dynamically execute scripts or call system functions. Therefore, it is widely used in software help systems (such as Office), e-books and technical document distribution. However, because CHM relies on the Windows native parser hh.exe to run, attackers often abuse its script execution capabilities (such as launching malicious code through WScript.Shell) and use the trust of the file format to disguise as legitimate documents to spread malicious payloads.

In this incident, the attacker embedded a malicious script in the CHM help document. After the CHM was opened, a scheduled task named ChromeCrashReport was created and executed every 15 minutes. The online packet generated by the scheduled task carried the host information to request the C2 server (**** centrum.com) and accepted the instructions issued by the server. The issued instructions were stored in the Public user document, named fc.cdt , and executed through cmd.

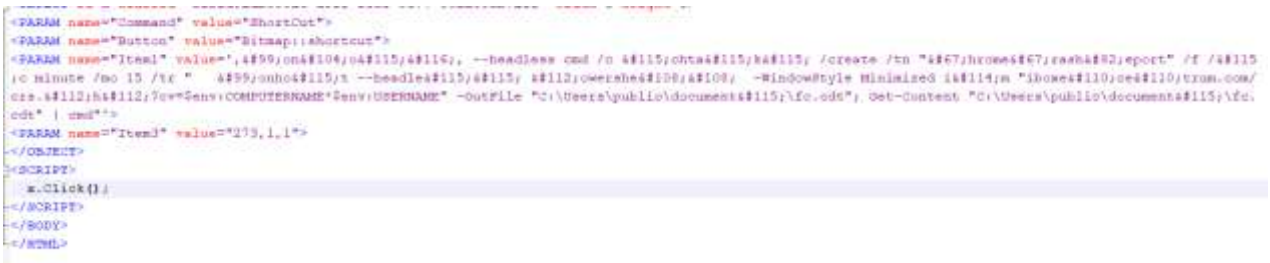
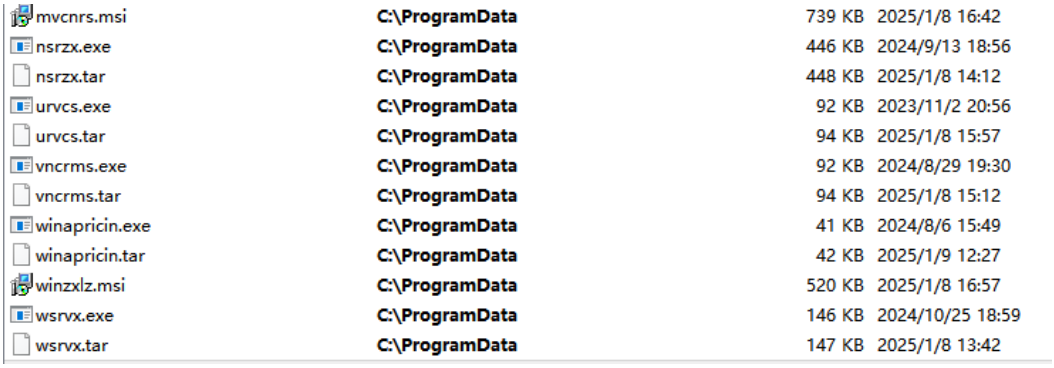


Figure 2-3Malicious script in CHM

Through continuous monitoring and analysis, it was found that the attack organization used fc.cdt to download compressed packages and decompress and execute them, and would download subsequent attack payloads in the ProgramData directory.



mvcnrs.msi	C:\ProgramData	739 KB	2025/1/8 16:42
nsrzx.exe	C:\ProgramData	446 KB	2024/9/13 18:56
nsrzx.tar	C:\ProgramData	448 KB	2025/1/8 14:12
urvcs.exe	C:\ProgramData	92 KB	2023/11/2 20:56
urvcs.tar	C:\ProgramData	94 KB	2025/1/8 15:57
vncrms.exe	C:\ProgramData	92 KB	2024/8/29 19:30
vncrms.tar	C:\ProgramData	94 KB	2025/1/8 15:12
winapricin.exe	C:\ProgramData	41 KB	2024/8/6 15:49
winapricin.tar	C:\ProgramData	42 KB	2025/1/9 12:27
winzxlz.msi	C:\ProgramData	520 KB	2025/1/8 16:57
wsrvx.exe	C:\ProgramData	146 KB	2024/10/25 18:59
wsrvx.tar	C:\ProgramData	147 KB	2025/1/8 13:42

Figure 2-4Attack payload delivered by the attacker

2.2 Attachment 2: PDF Document

Another attachment carried by the phishing email is in the form of a PDF document, in which a malicious script is inserted. When the PDF document is clicked, the embedded malicious script will be run and the attacker will be redirected to the phishing website set up by the attacker. The malicious link in the script is in the form of a short link, and the service pointed to by the current short link has been stopped. The parsing result of the short link shows that the destination address service is suspected to be used for phishing attacks against mailboxes, and the target address is: https:// **** filedownload.com/mail.I29.com.session.expired/mod_prc.login.again. The link uses longer characters and uses fake email address characters in the middle to deceive the target of the attack.

Table 2-5Phishing email attachment 2

Virus name	Trojan/ PDF.Agent [Phishing]
Original file name	MFA_2024_note_document.pdf
MD5	86EF4F713FFAA1810067ED609AD32055
File size	69.5 KB (71,247 bytes)
File format	Document/Adobe.PDF [:AdobeReader -1.5]

Figure 2-56

3 Attack Payload Analysis

In our analysis of this wave of attacks by the organization, Antiy found that it mainly delivered four types of attack payloads, namely: remote control Trojan wmRAT[4], remote control Trojan MiyaRAT[5]new remote control Trojan [6], and a new Python secret stealing Trojan. The first two are remote control Trojan programs frequently used by the organization. wmRAT is named after the first two letters of the sample name "wmservice.exe" when it was first discovered, and MiyaRat is named because the sample PDB path contains a string such as Miya1.1_client.pdb. The C# remote control Trojan is a new Trojan that has been modified and upgraded, and the Python secret stealing Trojan is a newly discovered secret stealing Trojan. Both are named according to their development languages.

3.1 wmRAT Remote Control Trojan: mvcnrs.msi

The wmRAT remote control Trojan is a malicious code used to collect information, perform file operations, and execute commands on the target during an attack. 3.1, 3.2, and 3.3are all remote control Trojans of the same wmRAT family with different configurations.

Table 3-1 2sample tags

Virus name	Trojan/Win32.WmRAT[APT] [7]

Original file name	mvcnrs.msi
MD5	B4A8C113A24A2878DBCBE911EE7CED9B
Processor architecture	Intel 386 or later processors
File size	739.00 KB (756,736 bytes)
File format	Archive/Microsoft.MSI
Timestamp	2024:08:08 13:03:06 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

MSI (Microsoft Software Installer) [8]files are installation packages defined by Microsoft and are parsed and installed through Windows Installer. They reuse the OLE (Object Linking and Embedding) compound document format defined by Microsoft for earlier versions, so their file header |D0 CF 11 E0| is also consistent with OFFICE files. Since MSI files are parsed by Widows Installer and the installation instructions defined in them are executed, they are not only widely used by Microsoft and other software vendors to release software or provide upgrade patches, but are also used by attackers to package and run malicious code.

In order to evade detection, this sample uses the MSI format to package its core payload. After running, it will release files in the C:\Windows\Installer directory and run. The information of the released files is shown in the following table.

Table 3-3Release file sample tags

Virus name	Trojan/Win32.WmRAT[APT] [7]
Original file name	Binary._ 3A169D0A20F57B076AAB5D938251A2DB
MD5	DC4BA30C67986D6213FCDD40280A4449
Processor architecture	Intel 386 or later processors
File size	91.50 KB (93,696 bytes)
File format	BinExecute /Microsoft.PE[:X86]
Timestamp	2023-11-01 17:55:54 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

After the release sample runs, the delay operation is performed first. 24 sleep functions are executed, each sleep lasts for 100 seconds. And there are actions to apply for memory release.

```
.  E8 A2840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  8B4C24 18        mov ecx,dword ptr ss:[esp+18]
.  51               push ecx
.  E8 91840000      call <JMP.&??_V@YAXPAX@Z>          sleep
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  8B5424 24        mov edx,dword ptr ss:[esp+24]      edx:EntryPoint
.  52               push edx                           edx:EntryPoint
.  E8 80840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  8B4424 20        mov eax,dword ptr ss:[esp+20]
.  50               push eax
.  E8 6F840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  8B4C24 10        mov ecx,dword ptr ss:[esp+10]
.  51               push ecx
.  E8 5E840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  8B5424 14        mov edx,dword ptr ss:[esp+14]      edx:EntryPoint
.  52               push edx                           edx:EntryPoint
.  E8 4D840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  57               push edi
.  E8 40840000      call <JMP.&??_V@YAXPAX@Z>
.  83C4 04          add esp,4
.  6A 64            push 64
.  FFD6             call esi
.  E8 AA010000      call <e.sub_13E1D30>
```

Figure 3-1Delay operation 1

The delay action also includes creating a thread and executing 1000 loops. The function of the loop function has no practical significance.

```
001891FA    BD E8030000      mov ebp,3E8
001891FF    83CF FF          or edi,FFFFFFFF
00189202    E8 39F7FFFF      call e.188940
00189207    66:A1 3CD81B00   mov ax,word ptr ds:[1BD83C]
0018920D    8A0D 3ED81B00    mov cl,byte ptr ds:[1BD83E]
00189213    66:894424 14     mov word ptr ss:[esp+14],ax
00189218    884C24 16        mov byte ptr ss:[esp+16],cl
0018921C    FF15 88D01B00    call dword ptr ds:[<&GetLogicalDrives>]
00189222    894424 18        mov dword ptr ss:[esp+18],eax
00189226    3BC6             cmp eax,esi
00189228    74 57            je e.189281
0018922A    8D9B 00000000    lea ebx,dword ptr ds:[ebx]
00189230    A8 01            test al,1
00189232    74 41            je e.189275
00189234    8D5424 15        lea edx,dword ptr ss:[esp+15]      edx:EntryPoint
00189238    52               push edx                           edx:EntryPoint
00189239    8D4C24 20        lea ecx,dword ptr ss:[esp+20]
0018923D    FF15 40D11B00    call dword ptr ds:[<&??0?$basic_string@
00189243    68 90D81B00      push e.1BD890
00189248    8D4C24 20        lea ecx,dword ptr ss:[esp+20]
0018924C    897424 48        mov dword ptr ss:[esp+48],esi
00189250    FF15 58D11B00    call dword ptr ds:[<&??4?$basic_string@
00189256    8D4424 15        lea eax,dword ptr ss:[esp+15]
0018925A    50               push eax
0018925B    E8 5A0D0000      call <JMP.&??_V@YAXPAX@Z>
00189260    83C4 04          add esp,4
00189263    8D4C24 1C        lea ecx,dword ptr ss:[esp+1C]
00189267    897C24 44        mov dword ptr ss:[esp+44],edi
0018926B    FF15 48D11B00    call dword ptr ds:[<&??1?$basic_string@
00189271    8B4424 18        mov eax,dword ptr ss:[esp+18]
00189275    FE4424 15        inc byte ptr ss:[esp+15]
00189279    D1E8             shr eax,1
0018927B    894424 18        mov dword ptr ss:[esp+18],eax
0018927F    75 AF            jne e.189230
00189281    8D4C24 14        lea ecx,dword ptr ss:[esp+14]
00189285    51               push ecx
00189286    E8 2F0D0000      call <JMP.&??_V@YAXPAX@Z>
```

Figure 3-2Delay operation 2 - a meaningless function that loops 1000 times

The subsequent behavior of the sample is also interspersed with a large number of delayed operations, which will not be described here. The sample then attempts to establish a connection to port 60099 of **** console.com.

```
A1 D43F3F01          mov eax,dword ptr ds:[13F3FD4]      013F3FD4:&"[redacted].console.com"
C74424 0C 00000000   mov dword ptr ss:[esp+C],0
C74424 18 01000000   mov dword ptr ss:[esp+18],1
C74424 1C 06000000   mov dword ptr ss:[esp+1C],6
73 05                jae e.13E5FA5
B8 D43F3F01          mov eax,e.13F3FD4                   13F3FD4:&"[redacted]console.com"
8D4C24 0C            lea ecx,dword ptr ss:[esp+C]
51                   push ecx
8D5424 14            lea edx,dword ptr ss:[esp+14]
52                   push edx
6A 00                push 0
50                   push eax
FF15 D4D23E01        call dword ptr ds:[<&getaddrinfo>]
85C0                 test eax,eax
75 3F                jne e.13E5FFB
8B7424 0C            mov esi,dword ptr ss:[esp+C]
85F6                 test esi,esi
74 30                je e.13E5FF4
8B3D E8D23E01        mov edi,dword ptr ds:[<&inet_ntoa>]
```

Figure 3-3Connections back to the C2 domain name

As of the time of sample analysis, the domain name has expired. If the connection is successfully established, the sample will create a thread to receive and execute relevant instructions from the server. The thread function is shown in Figures Figure 3-4.

```
FFD7                 call edi                            recv
83F8 FF              cmp eax,FFFFFFFF
74 26                je e.13E5EE3
03F0                 add esi,eax
83FE 04              cmp esi,4
7C DC                jl e.13E5EA0
8B4424 0C            mov eax,dword ptr ss:[esp+C]
50                   push eax
FFD3                 call ebx
8BF0                 mov esi,eax
897424 0C            mov dword ptr ss:[esp+C],esi
E8 6A2A0000          call <e.sub_13E8940>
56                   push esi
E8 94C0FFFF          call e.13E1F70
83C4 04              add esp,4
84C0                 test al,al
75 B3                jne e.13E5E96
8B0D E4343F01        mov ecx,dword ptr ds:[13F34E4]
8B35 F4D23E01        mov esi,dword ptr ds:[<&closesocket>]
51                   push ecx
C605 DC353F01 00     mov byte ptr ds:[13F35DC],0
FFD6                 call esi
83F8 FF              cmp eax,FFFFFFFF
75 0D                jne e.13E5F0B
FF15 08D33E01        call dword ptr ds:[<&WSAGetLastError>]
```

Figure 3-4 Main functions of remote control Trojan

Remote control Trojan commands include: screen capture, file upload and download, information collection, command execution, etc. The specific functions of remote control Trojan commands are shown in Table Table 3-4.

Table 3-4 Remote control Trojan command function table

Instruction	Function
5	Send screenshot data to the server
6	Receiving file data

8	Receive information from the server, find the specified file, process it, and send it to the server
10	Open the specified URL and get the file
11	Find the specified directory file and perform operations
13	Search for files in the specified directory and send the file information to the server
15	Get information upload, including computer name, user name, disk usage, etc.
16	Process creation and data transmission using pipes
20	Close the specified file stream
21	Write data to the specified file stream
23	Open the specified file stream and transfer data to the server
26	Send file data to the remote server and calculate the sending progress

3.2 wmRAT Remote Control Trojan: vncrms.exe

Table 3-5vncrms.exe sample tags

Virus name	Trojan/Win32.WmRAT[APT] [7]
Original file name	vncrms.exe
MD5	EFB54F507F2B7796DF5EDD923935C2C2
Processor architecture	Intel 386 or later processors
File size	92.00 KB (94, 208 bytes)
File format	BinExecute /Microsoft.PE[:X86]
Timestamp	2024 :08: 29 19:30:35 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

The sample is the same as the sample released by mvcnrs.msi, and is also connected to port 60099 of **** console.com. The functions of the two samples are exactly the same, so I will not go into details.

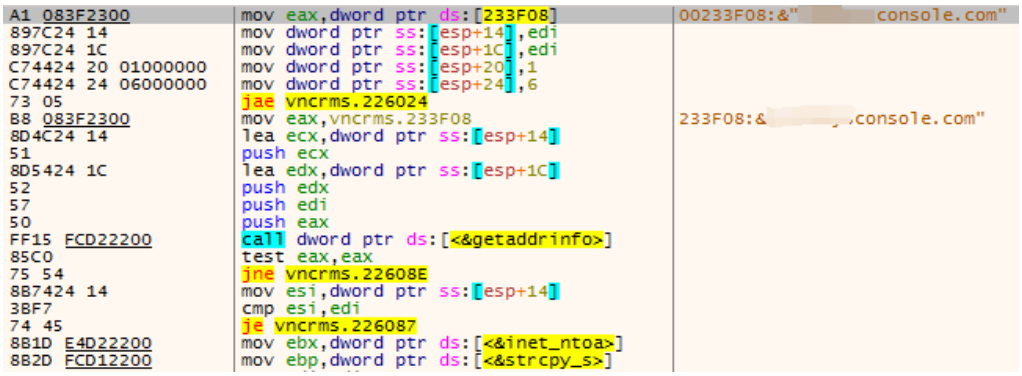


Figure 3-5Connections back to the C2 domain name

3.3 wmRAT Remote Control Trojan: urvcs.exe

Table 3-6 urvcs.exe sample tags

Virus name	Trojan/Win32.WmRAT[APT] [7]
Original file name	urvcs.exe
MD5	1AD144815A97407F2FFAB6A54BE11262
Processor architecture	Intel 386 or later processors
File size	92.00 KB (94, 208 bytes)
File format	BinExecute /Microsoft.PE[:X86]
Timestamp	202 3:11:0 2 20:56:08 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

The sample is the same as the sample released by mvcnrs.msi, and also attempts to connect to **** console.com. However, the target port of the connection is 80. Apart from this, the functions of the two samples are exactly the same, so I will not go into details.

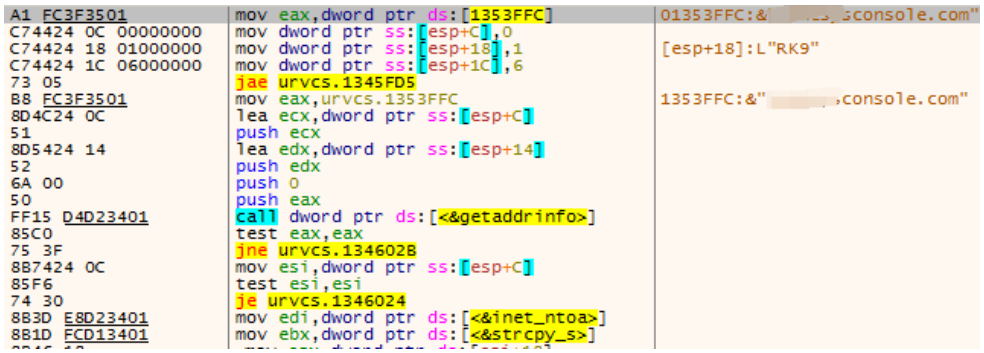


Figure 3-6Connections back to the C2's target port 80

3.4 MiyaRAT Remote Control Trojan: nsrzx.exe

The MiyaRAT remote control Trojan is a new type of remote access Trojan that the "BITTER" organization began to use in 2024. It is mainly used for cyber espionage against high-value targets such as government, defense, and energy. 3.4, 3.5, and 3.6the MiyaRAT family.

Table 3-1 nsrzx.exe sample tags

Virus name	Trojan/Win32.MiyaRAT[APT] [9]
Original file name	nsrzx.exe
MD5	B11D50D48CB10C40DCAD8B316253885D
Processor architecture	Intel 386 or later processors
File size	446 KB (456 , 704 bytes)
File format	BinExecute /Microsoft.PE[:X86]
Timestamp	202 4:09:13 18:56:19 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

The PDB of this sample is: "C:\DRIVE_Y\EDRIVE\repos\Leov3_client\Release\Leov3_client.pdb ". "Leo" is a common Western male name, derived from the Latin word for lion, and may also be an abbreviation. However, it can be inferred that it is the name of an internal project, group or person of the organization, and "V3" is the version number of the corresponding file.

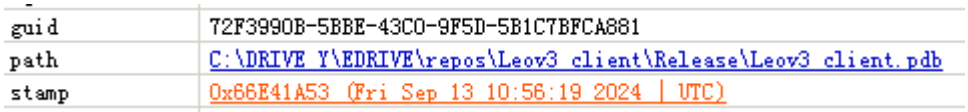


Figure 3-7 8

The sample first obtains the C2 address and connects to the C2 server ****psvc.com through WSAConnectByNameW.

```
B9 74DE0B00      mov ecx,nsrzx.BDE74                  BDE74:&L"\.    )svc.com"
A1 84DE0B00      mov eax,dword ptr ds:[BDE84]
0F470D 74DE0B00  cmova ecx,dword ptr ds:[BDE74]       000BDE74:&L"\    psvc.com"
40               inc eax
51               push ecx
50               push eax
56               push esi
E8 BA050300      call nsrzx.89776
83C4 0C          add esp,C
8D85 A0DFFFFF    lea eax,dword ptr ss:[ebp-2060]
50               push eax
8D85 5CDFFFFF    lea eax,dword ptr ss:[ebp-20A4]
50               push eax
6A 00            push 0
6A 00            push 0
6A 00            push 0
6A 01            push 1
6A 00            push 0
6A 00            push 0
56               push esi
6A 00            push 0
FF15 80800A00    call dword ptr ds:[<&CreateProcessW>]
85C0             test eax,eax
0F85 5BFDFFFF    jne nsrzx.58F45
FF15 54800A00    call dword ptr ds:[<&GetLastError>]
FF75 08          push dword ptr ss:[ebp+8]
FF15 3C820A00    call dword ptr ds:[<&closesocket>]
```

Figure 3-9Connections back to the C2 domain name

The sample then obtains system information, including user name, computer name, disk information, etc.

```
FF15 0480BE00          call dword ptr ds:[<&GetUserNameW>]
8D85 30DBFFFF          lea eax,dword ptr ss:[ebp-24D0]
C785 30DBFFFF 100000(  mov dword ptr ss:[ebp-24D0],10
50                     push eax
8D45 CC                lea eax,dword ptr ss:[ebp-34]
50                     push eax
FF15 7480BE00          call dword ptr ds:[<&GetComputerNameW>]
6A 00                  push 0
FF15 8880BE00          call dword ptr ds:[<&GetModuleHandleW>]
85C0                   test eax,eax
74 13                  je nsrzx.B99560
68 04010000            push 104
8D8D 9CFBFFFF          lea ecx,dword ptr ss:[ebp-464]
51                     push ecx
50                     push eax
FF15 B080BE00          call dword ptr ds:[<&GetModuleFileNameW
68 04010000            push 104
8D85 A4FDFFFF          lea eax,dword ptr ss:[ebp-25C]
50                     push eax
68 480FBF00            push nsrzx.BF0F48                    BF0F48:L"USERPROFILE"
FF15 3480BE00          call dword ptr ds:[<&GetEnvironmentVari
```

Figure 3-10Obtain system information data

The sample constructs the obtained system information into Figure 3-11

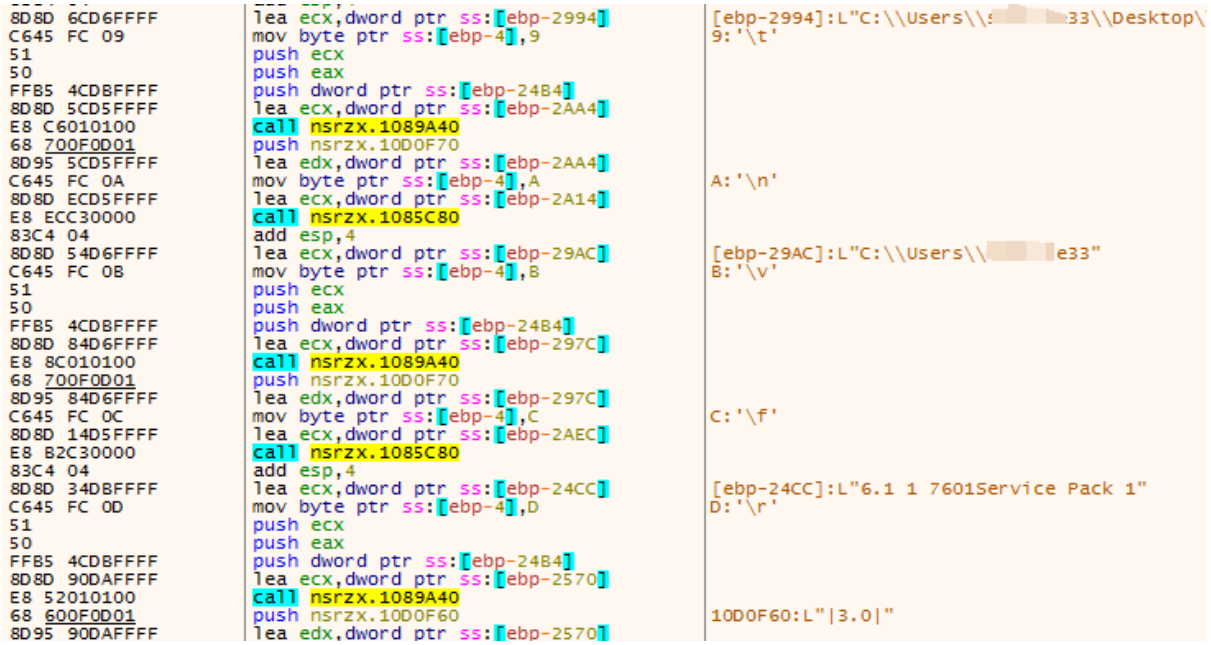


Figure 3-11All system information obtained

The sample encrypts the system information and sends it to C2, then loops to receive and execute the attacker's instructions. The remote control Trojan instructions supported by the sample are summarized in Table 3-7.

Table 3-7 Remote control Trojan command function table

Instruction code	Function
GDIR	Directory enumeration
DEL	File deletion
GFS	Directory enumeration (recursive)
SH1start_cmd , SH1start_ps	Process creation (cmd , powershell)
SH1 , SH2	Command passing
SFS	File transfer, secondary instruction UPL1 file upload, DWNL file download
GSS	Screenshots
SH1exit_client	Process exit

The attacker's command plaintext is encrypted with 0x43 XOR, and the command will be decrypted after receiving it. The following is a detailed analysis of each remote control Trojan command.

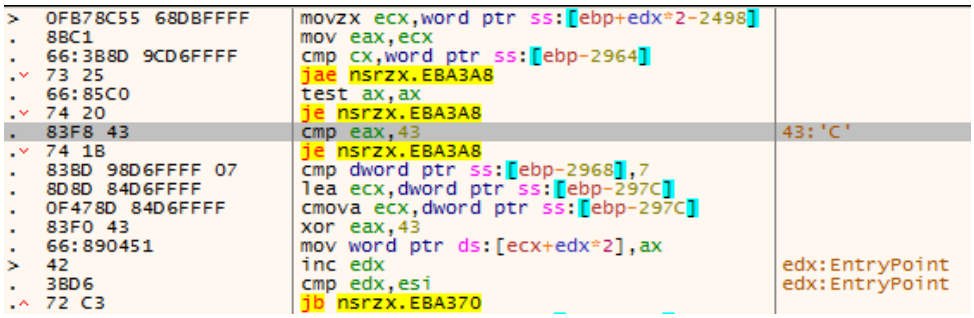


Figure 3-12XOR encryption with 0x43 instruction code

The GDIR command, similar to the Windows dir command, is used to list file and subdirectory information.

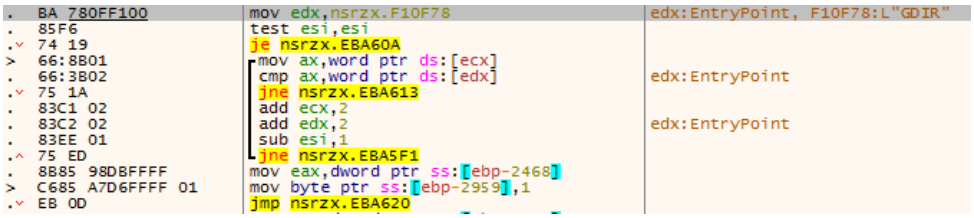


Figure 3-13GDIR command - get system information

DELz command is used to delete the specified file.

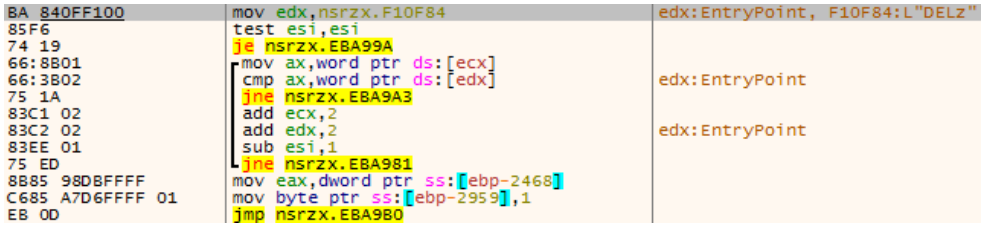


Figure 3-14 DELz command - delete files

GFS command calculates the size of all files and subdirectories in the specified directory. The calculation results are sent to C2 three times, starting with "@@GSF=total file size" and ending with " =@@GFS ".

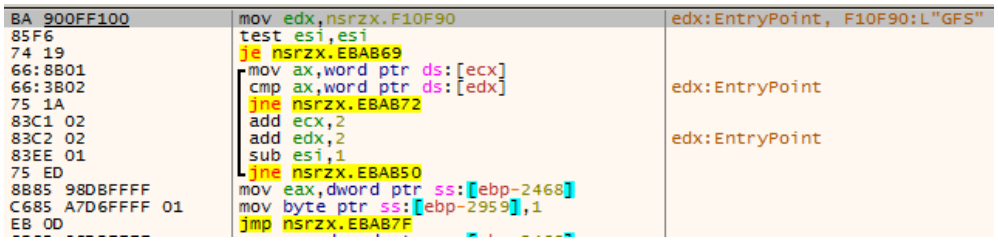


Figure 3-15GFS command - directory enumeration to obtain file and subdirectory sizes

SH1start_cmd and SH1start_ps instructions are used to start cmd and powershell, execute the commands in the pipeline, and return the execution results to C2.

Figure 3-16 SH1start_cmd , SH1start_ps ——execute cmd , ps commands

SH1 and SH2 instructions are used to execute shell instructions that write to the pipeline. SH2 will perform a short sleep before and after writing, depending on the situation.

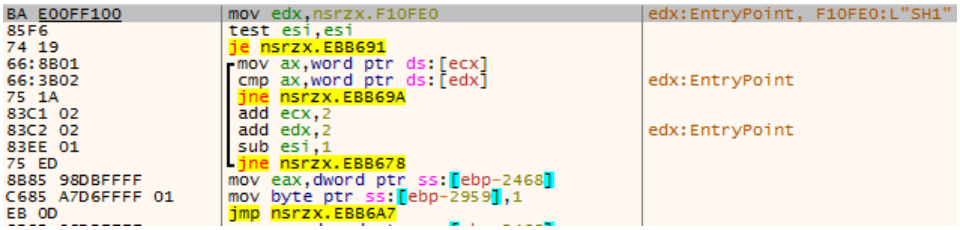


Figure 3-17 SH1, SH2 instructions - write pipeline shell instructions

SFS instructions are used to upload and download files.

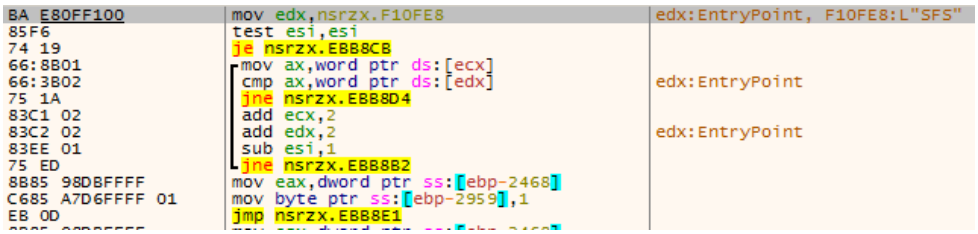


Figure 3-18SFS instructions - file upload and download

The GSS instruction is used to take a screenshot of the target machine. The corresponding functional logic is to obtain the screen device context (Device Context) and create a compatible memory DC for off-screen drawing. By default, a bitmap object with a resolution of 1920 (0x780) x1080 (0x438) is created to store the screenshot data, and the screen content is copied to the memory bitmap to implement the screenshot function. At the same time, the width and height of the screenshot image are reduced by 1/3 and 1/5 of the original image, respectively, which may be intended to reduce the image size and reduce the subsequent transmission bandwidth. It may also indicate that the

main purpose of obtaining the screenshot action is to quickly determine the current host's operating status and attack value.

Figure 3-19GSS instructions - Screen capture

SH1exit_client command to exit the current Trojan program.

Figure 3-20 SH1exit_client command - exit

3.5 MiyaRAT Remote Control Trojan: winzxlz.msi

Table 3-8winzxlz.msi sample tags

Virus name	Trojan/Win32.MiyaRAT[APT] [9]
Original file name	winzxlz.msi
MD5	F3943F24B7BD752B19DAB25A5409F20C
Processor architecture	Intel 386 or later processors
File size	519.00 KB (531,968 bytes)
File format	Archive/Microsoft.MSI
Timestamp	202 4:10:25 19:02:01 UTC

Compiled language	Microsoft Visual C /C++
Packer type	None

After the sample is run, it will release files in the C:\Windows\Installer directory and run. The information of the released files is shown 错误!未找到引用源。Table 3-8.

Table 3-9Release file tags

Virus name	Trojan/Win32.MiyaRAT[APT] [9]
Original file name	Binary._ CCA3E30A6A966CBDD6526C4D6229BFFA
MD5	B6631F979E854C4C313F48AC85009A61
Processor architecture	Intel 386 or later processors
File size	463.00 KB (474,112 bytes)
File format	PE32 executable (GUI) Intel 80386, for MS Windows
Timestamp	202 4:10:25 19:02:01 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

The PDB path of the sample is: "C:\Users\DOMS\KugelBlitz\VSRepos\DEV\Leo_v4Client\Release\Leov4_client.pdb", which can be verified with the "Leov3" analysis in Section 3.4. "LEO" is the corresponding group, person and project number, and "V4" is the version number.

guid	E36D9BFD-8A33-4E2B-BBA-242F3834EB1A
path	C:\Users\DOMS\KugelBlitz\VSRepos\DEV\Leo_v4Client\Release\Leov4_client.pdb
stamp	0x671B7AA9 (Fri Oct 25 11:02:01 2024 | UTC)

Figure 3-21PDB information

The core function of the released sample is located in the function sub_F49DE0. After running, it will try to connect to port 46346 of ****psvc.com.

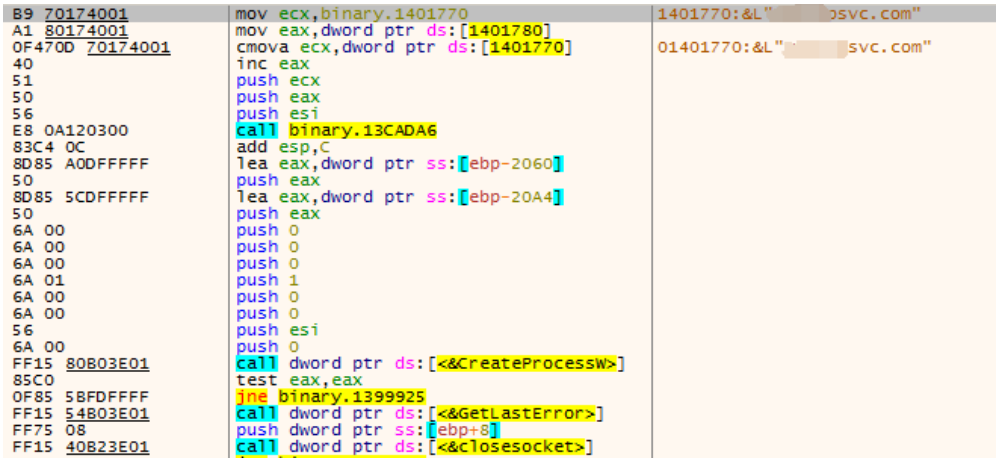


Figure 3The target domain name and port that the sample wants to connect to

The sample then collects data such as the target machine's user name, machine name, Trojan file path, %userprofile% environment variable, disk information, system version, etc., and then encrypts the collected information and sends it to the target server.

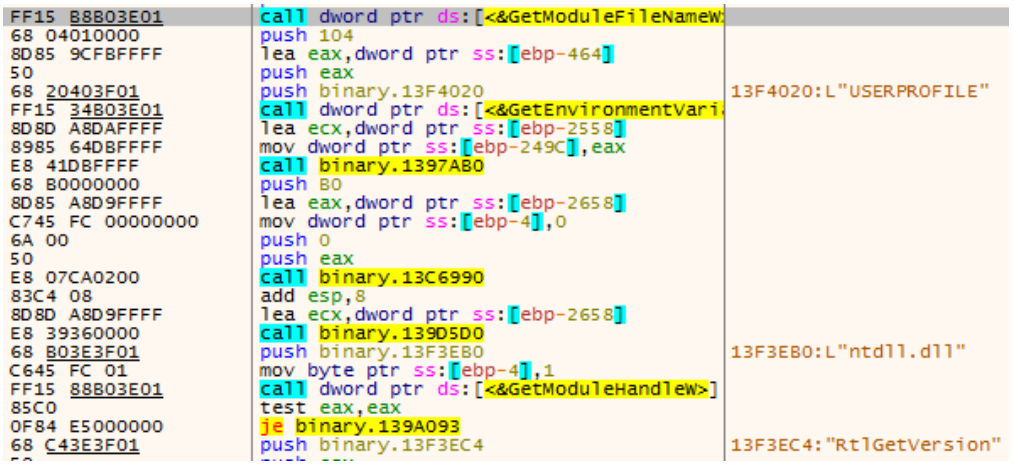


Figure 3-22Obtain host system information

Wait for the instructions sent by the server in a loop and execute the corresponding functions.

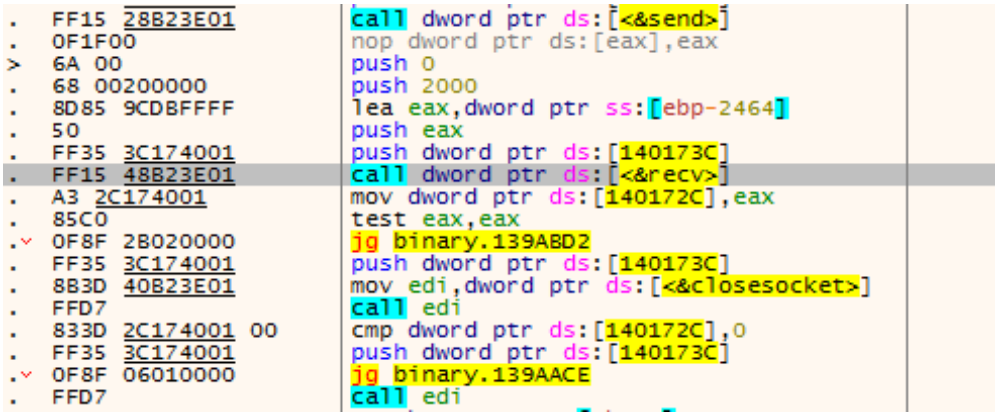


Figure 3-23Loop receiving instruction execution

The command functions of the Trojan are the same as those of the nsrzx.exe sample, so they will not be described here.

3.6 MiyaRAT Remote Control Trojan: wsrvx.exe

Table 3-10wsrvx.exe sample tags

Virus name	Trojan/Win 64.MiyaRAT[APT] [9]
Original file name	wsrvx.exe
MD5	EAE58B38AA86E0FEEC37A529807F3FA0
Processor architecture	Intel 386 or later processors
File size	145 KB (148 , 992 bytes)
File format	BinExecute /Microsoft.PE[:X64]
Timestamp	202 4:10:25 18:59:18 UTC
Compiled language	Microsoft Visual C /C++
Packer type	None

The C2 address and port that this sample connects back to are the same as those of the nsrzx.exe sample, both of which are port 46346 of ****psvc.com.

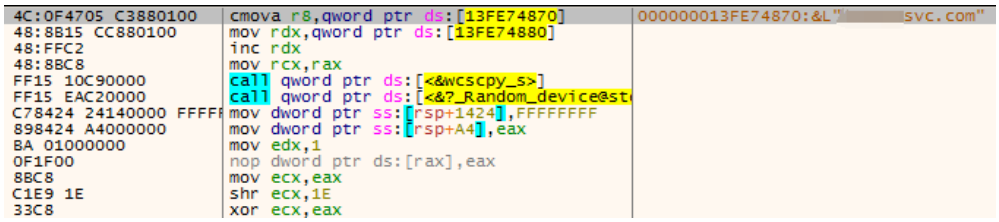


Figure 3-24Connect to C2 domain name and port

The wsrvx.exe sample is a 64-bit program. Except for the different software architecture, the behavior of the wsrvx.exe sample is basically the same as that of nsrzx.exe, which will not be described here.

3.7 C# Remote Control Trojan: winapricin.exe

A remote control Trojan developed in C# language by the "BITTER" organization in recent years. It uses.NET Framework as the runtime framework to ensure high compatibility in Windows systems, supports cross-version operation, and reduces development costs through compatibility advantages. Its technical evolution direction is consistent with the typical characteristics of South Asian APT organizations.

Table 3-11winapricin.exe sample tags

Virus name	Trojan / Win32.APosT [10]
Original file name	winapricin.exe
MD5	A3DD7F773CD3B374071CC9C98A0DAE4F
Processor architecture	Intel 386 or later processors
File size	40.50 KB (4 1,472 bytes)
File format	BinExecute /Microsoft.PE[:X86]
Timestamp	2078-11-13 15:18:10 UTC
Compiled language	Microsoft Visual C #
Packer type	None

The sample file name starts with "win", which is a social engineering technique to make users mistakenly think it is a Windows file. The timestamp is 2078, and it is obvious that the sample has been constructed with a timestamp to avoid time zone comparison and increase the difficulty of tracing the source, but it also brings a very obvious anomaly.

The sample first creates an ordered list, which registers and stores different MessageTypes to define different functions.

Figure 3-25Registered storage of MessageType containing remote control Trojan function

Each MessageType type contains name, opcode and Message members, and each Message member points to a specific class. The different classes and their functions are shown in Table 错误!未找到引用源。Figure 5-1.

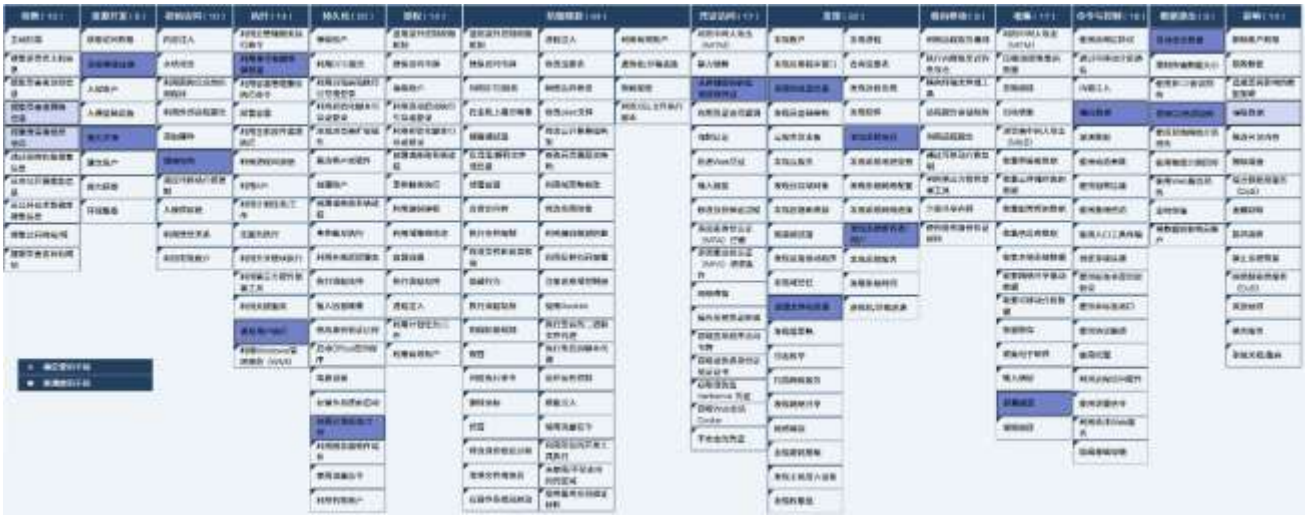


Figure 3-26 Attack actions and attack executor behaviors and tactical capabilities mapping

4 Assessment of Security Capabilities Required to Detect and Defend Against Relevant Attack Activities

Through a detailed analysis of threat events, we can obtain the attack process of running objects and running actions in the entire life cycle of the attack payload execution body, and further evaluate the key capability mapping matrix of anti-virus engine and active defense that the security protection software deployed on the terminal side should have. The key capability points of detection and defense of this series of attack activities are described in Table 41of Antiy AVL SDK anti-virus engine and IEP terminal protection system have all the capabilities listed in the list.

Table 41capabilities required to counter attack actions and attack execution entities

Attack Execution Lifecycle		Object	Action	Key capabilities of anti-virus engines	Active defense capability key capabilities
Pre-set and drop	Drop	Spear Phishing Emails	Attackers sent spear phishing emails with the subject line of Ministry of Foreign Affairs documents	1. Email metadata extraction 2. Email sender detection 3. Email content detection (social engineering rhetoric , QR codes, etc.) 4. Attachment detection (double extension, etc.)	1. (Phishing email protection) Email protocol parsing and extracting email source data, disassembling email object metadata such as body content, attachment file name, attachment file and sender 2. (Phishing email protection) Set social engineering keyword alert reminder rules in email subject

		Email attachment 1: RAR compressed file	Receive email attachment 1 and attachment 2	1. RAR compression format recognition 2. Recursive detection of RAR archive derivative files	1. (File Defense) Set up file defense for full disk monitoring 2. (File Defense) Set file defense to detect compressed files,.chm,.pdf,.cdt and other file extensions 3. (File Defense) Set the file defense decompression layer number and other detection configurations 4. (File Defense) Get email attachment file delivery engine detection 5. (File Defense) CHM format file embedded script to set alarm/interception rules 6. (File Defense) Set alert/interception rules by embedding scripts in PDF files
		Email attachment 2: PDF document		1. PDF data stream Stream object parsing 2. Embedded malicious script detection 3. Built-in malicious URL detection	
Load Execution	Implement	Email attachment 1: CHM file with malicious script embedded in the compressed file	Email attachment 1: Tricking users into opening CHM files	1. CHM format recognition 2. Disassembly of CHM embedded script 3. Derived malicious script sub-file recursive detection	WScript , Powershell and CMD through hh.exe
		Email attachment 2: PDF document	Email attachment 2: Open the PDF document to jump to the phishing website built by the attacker	Malicious URL Detection	(Host firewall) monitors application access to C2 server request packets, obtains accessed IP, domain name and URL, and performs delivery engine detection to intercept threat C2 server access request packets
	Persistence	System scheduled tasks created by CHM files	Email attachment 1: Create a scheduled task after opening CHM	/	1. (Process Defense) Monitor the creation/modification of scheduled tasks, disassemble the file path and command parameters of the execution object in the scheduled task, and then send the engine to detect and delete the threat scheduled task 2. (Process Defense) hh.exe creates a scheduled task to set alarm/interception rules

Effective Application	Process effectiveness	After the CHM file is opened, a PE format payload file is created to execute the scheduled task	Request the C2 server with host information	Malicious URL Detection	1. (Host firewall) monitors application access to C2 server request packets, obtains accessed IP, domain name and URL, and detects the delivery engine to intercept threat C2 server access request packets 2. (Host firewall) Set up logging/alarm/blocking rules when the application request IP, Domain, and URL are untrusted overseas addresses
			1. Accept instructions from the C2 service and issue them 2. The issued command is stored in the Public user document and named fc.cdt Download subsequent attack payloads in the ProgramData directory through cmd execution instructions	/	1. (File defense) Monitor disk file creation/modification, delivery engine detection, and delete threat files 2. (File Defense) PE file objects downloaded by third-party applications are marked as application downloads 3. (File Defense) Set reminder rules for files downloaded by apps
		Remote control Trojan wmRAT : mvcnrs.msivncrms.exeurvcs.exe	1. Execute the downloaded payload file 2. Payload file release file 3. Payload file sent to C2 backlink 4. Payload file executes remote control instructions	1. MSI format recognition, structure analysis, signature verification, and recursive detection of derived files 2. PE format identification and object disassembly 3. Detection of extracted proprietary embedded malicious instructions	1. (Process Defense) Monitor process startup behavior 2. (Process Defense) Monitor cmd / Powershell processes for dangerous command execution 3. (File defense) Monitor disk file creation/modification, delivery engine detection, and delete threat files 4. (File Defense) Set alarm/blocking rules when the attributes of files downloaded by the application have abnormal timestamps

		Remote control Trojan MiyaRAT: nsrzx.exewinzxlz.msiwsrvx.exe		1. PE format identification 2. Detect specific rich/ pdb path /registry/mutex and other compilation, linking, packaging and other environmental information 3. Detection of specific encryption algorithms 4. MSI format recognition, structure analysis, signature verification, and recursive detection of derived files	5. (Host firewall) monitors application access to C2 server request packets, obtains accessed IP, domain name and URL, and detects the delivery engine to intercept threat C2 server access request packets
		C# Remote Control Trojan : winapricin.exe		1. PE format identification 2. Compiler Identification (C#) 3. Parsing.NET's TypeRef table 4. Detection of extracted proprietary API call sequences	
		Python stealer: updater.exe		1. Identification of compiler/packager (py to exe) 2. Extract the embedded python intermediate bytecode file pyc 3. Parse the pyc object structure and extract function names, variables, constants, etc. for threat detection	
	Purpose-driven	Python stealer: updater.exe	After the payload file is executed, it steals browser credential data	/	1. (Active defense) Monitor the behavior of the program reading browser credentials 2. (Active defense) Untrusted programs read browsers and set records/alarms/interception

					rules based on sensitive certificates
		Remote control Trojan MiyaRAT: nsrzx.exe	Payload file executes remote control command - screenshot	/	1. (Active defense) Monitor the application's behavior of calling API to take screenshots 2. (Active defense) Screen capture of untrusted programs to set collection/alarm/interception rules

5 Defensive Thinking

Attack organizations such as "White Elephant" and "BITTER" represent a style of operation, that is, they completely ignore the risk of exposure or even being exposed, and carry out large-scale pre-attacks that seem to be of low level. They maximize the initiative of the attacker to launch the attack, relying on a wide net to capture probabilistic events. This behavior is also a manifestation of the "persistence" in APT attacks. In the technical report "A^{2}PT and Attack Weapons in "Quasi-APT" Incidents" [12] at the 2015 Internet Conference, researchers from Antiy pointed out that APT [12]simple technical concept, but must be related to its political and economic background. A (advanced) is relative, and its essence is the potential difference between attack capability and defense capability, while P (persistence) depends on the persistence of the attacker's operating will and the cost support capability. It may be the ability to connect, the ability to persist, or the ability to repeatedly enter. Therefore, P is the essential attribute of APT. Today we need to make a supplementary point of view. P itself not only includes the ability to maintain connection, persistence and repeated entry, but also includes continuous attempts.

From the attack payloads analyzed in this report, it can be seen that the attack characteristics of this activity are consistent with the attack style of threat actors in this direction. Its overall skills still use email as the main attack entry point, and adopt a wide-net mode to capture opportunities with low probability. Based on a certain understanding of our relevant institutions, it has certain social engineering skills and packaging for the email content, and constructs corresponding work emails and documents to implement social engineering attacks. It does not use vulnerabilities to construct execution opportunities, but directly adopts the form of embedding malicious scripts or links in attachments. This reflects that the vulnerability reserves of the attack organization are not rich, and it also shows that in the "casting a wide net and trying your luck" stage, it tries to avoid using valuable vulnerability resources as much as possible, and tries to achieve relevant attack effects at a lower cost through social engineering deception, format nesting, etc.

Since Antiy captured the attack activities of this organization in 2013, this organization has been operating in a relatively barbaric and crude manner, but this method is still continuing, which also indirectly shows that this attack is likely to achieve effective results. It exposes that some government, enterprises and individual users in China have blind spots in defense capabilities and security awareness. In these attacks, emails are used as the entrance to directly reach the terminal devices of the attacked personnel. Since encryption protocols are widely used in email sending and receiving, related attacks are highly invisible at the gateway exit and bypass traffic side of government and enterprise institutions. The large number of mobile offices and government and enterprise institutions using free Internet mailboxes may also cause the attack link to be outside the security defense boundary of government and enterprise institutions. Although the success rate of this attack is not high, once it succeeds, the control of the controlled host terminal is obtained by the attacker, and its host information and accessible resources can be obtained by the attacker. The relevant hosts and the obtained credentials will further become the attack entrances for attackers to move horizontally and spread the trust chain.

However, because the focus of domestic security investment has been on border and traffic security box equipment for a long time, the investment in terminal security protection has always accounted for a low proportion, and the low-price bidding model has been adopted in procurement. Effective security protection and virus detection capabilities have not been used as assessment indicators for security software procurement. Even a few information security managers have already believed that anti-virus is a functional switch, and as long as it is turned on, it has the corresponding capabilities, while ignoring that detection and protection capabilities can only be achieved by relying on the continuous operation and iteration of advanced anti-virus engines and kernel main defense. Defense resources and costs have not been deployed more at the key points of attack landing, so that a certain proportion of domestic government and enterprise terminals are under low-level protection and are easily penetrated by similar attacks.

On the host security environment side, there are many key application defense points that need to be strengthened, such as effective convergence of open ports and open service exposure surfaces, reasonable configuration reinforcement of the host system, effective protection of browsers and emails (WEB and client), especially security checks and execution action management and interception of executables. These protections require long-term accumulation and continuous operation of host strategies, and the construction of driver -level main defense capabilities to capture deep security events. If only relying on general application layer event collection, on the one hand, many attacks cannot be identified, obtained, and left traces, and on the other hand, when the threat is discovered,

it has already spread. If most threats are not intercepted in the first delivery, it will also bring a huge burden on network management.

Therefore, from the perspective of basic protection, the fulcrum of security returns to the host system side. Only by covering effective terminal security protection capabilities to every working host, every cloud workload, and every mobile office terminal, and continuously strengthening the security defense cornerstone on the system side, and building an end-to-end security operation closed loop on this basis, forming a closed loop of detection and response between the network security operation management system and each endpoint, forming a closed loop of coordinated linkage between each endpoint asset, and forming a closed loop of security vendors and user-side security intelligence consumption, can we better protect against threats and increase the opponent's attack cost. At the same time, since the personal mailboxes, home hosts, smart terminals and other devices of key personnel are also related attack points, in this case, they have actually constituted the necessary security extension required by the security protection on the government and enterprise side. Therefore, it is necessary to strengthen the corresponding security management and perception capabilities of mobile office and portable machines, rather than "running naked" or relying on Internet security software, so that effective threat intelligence and perception capabilities escape the scope of government and enterprise linkage.

Threats are an effective touchstone. Although the threat actors in this geopolitical direction have not seen any substantial improvement in their capabilities over the years, due to the extensive nature of their attacks, they are actually a measure for our relevant agencies and key personnel to test their basic defense capabilities. Only by being able to defend against attacks at this level can we defend against higher-level A^2PT attacks.

Appendix 1: References

[1] Antiy. Dance of the White Elephant: Cyberattacks from the South Asian Subcontinent [R/OL]. (2016-07-10)
https://www.antiy.com/response/WhiteElephant/WhiteElephant.html

[2] Antiy. Hidden Elephants: A Series of Cyber Attacks from the South Asian Subcontinent [R/OL]. (2017-07-09)
https://www.antiy.com/response/The_Latest_Elephant_Group.html

[3] Antiy. Computer Virus Encyclopedia: Document/Microsoft.CHM[:Microsoft Compiled HTML Help]
https://www.virusview.net/format/Document/Microsoft/CHM/Microsoft%20Compiled%20HTML%20Help

[4] Qianxin. The Shadow Remains: Analysis of the Recent Attacks of the BITTER Organization [R/OL]. (2023 - 08 - 03)
https://ti.qianxin.com/blog/articles/Persistence-in-Shadows-Recent-Analysis-of-Magnolia-Attacks-CN/

[5] Qianxin. The BITTER Organization Launches a New Special Horse Miyarat, And Domestic Users Become the Primary Target [R/OL]. (2024 - 10 - 12)
https://mp.weixin.qq.com/s/eseliIVHqiWI-Q1CoCA81g

[6] 360 Threat Intelligence Center. APT-C-08 (BITTER) Organization: Multiple Attack Vectors Revealed [R/OL]. (2024 - 11 - 05)
https://mp.weixin.qq.com/s/pvm0QUAMS0U5dIge1ImcCQ?color_scheme=light

[7] Antiy. Computer Virus Encyclopedia: Trojan/Win32.WmRAT[APT]
https://www.virusview.net/malware/Trojan/Win32/WmRAT/APT

[8] Antiy. Computer Virus Encyclopedia: Archive/Microsoft.MSI
https://www.virusview.net/format/Archive/Microsoft/MSI

[9] Antiy. Computer Virus Encyclopedia: Trojan/Win32.MiyaRAT[APT]
https://www.virusview.net/malware/Trojan/Win32/MiyaRAT/APT

[10] Antiy. Computer Virus Encyclopedia: Trojan/Win32. APosT
https://www.virusview.net/malware/Trojan/Win32/APosT

[11] Antiy. Computer virus encyclopedia: Trojan/Win64. Agentb
https://www.virusview.net/malware/Trojan/Win64/Agentb

[12] Antiy. Attack Weapons in A^2PT and "Quasi-Apt" Incidents. China Anti-Virus Conference. 2015
http://www.antiy.com/presentation/Attack_Weapons_in_A2PT_and_APT-To-Be_Incidents.pdf

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.