"SwimSnake (Silver Fox)" Cybercrime Group's Latest Variant Attack Campaign

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

1 Overview

Starting on August 13, 2025, SwimSnake (Silver Fox) cybercrime group launched a new wave of attacks. Antiy CERT responded and handled the situation. In this wave of attacks, the attackers used social engineering techniques to package and disguise PE executable files, then used WeChat, DingTalk, and other platforms to deliver a remote control Trojan, which they then used to defraud victims. The attack combined several previously used anti-virus evasion tactics employed by the SwimSnake cybercrime group, attempting to insert the remote control Trojan in a more covert manner. They **used the PoolParty technique to inject shellcode into the target process. This shellcode then connected to the C2 server to retrieve a payload file. This payload file then released the "White and Black" component in a specified path and created a scheduled task. Upon execution, the "White and Black" component decrypted the bin file and executed the final remote control Trojan**.

PoolParty is an open-source project that includes various methods for process injection using the Windows thread pool, enabling the covert execution of shellcode within target processes. Due to the open source nature of this project, numerous "SwimSnake"-related malware samples have been discovered this year using it as their primary injection method, injecting malicious code into target system processes to evade detection by security products.

"SwimSnake" attack group, also known as "Silver Fox" or "Gooda Bandit" by other security companies, mainly conducts attacks and fraud activities against domestic users. Antiy discovered and analyzed the early activities of the SwimSnake group in the second half of 2022 [1], including disguising common software download sites and search engine SEO and phishing emails to implement the campaign, using a combination of white and black methods to execute the campaign, and using instant messaging software (WeChat, WeCom, etc.) to further spread the campaign. Its main profit method is to conduct fraud by pulling groups through instant messaging software, and it also has the ability to steal secrets from infected hosts, and may engage in other activities such as data trafficking. The malicious files it spreads are extremely numerous, and the means of avoiding killing are changed very frequently, affecting a wide range of individuals and industries.

Antiy CERT believes that the main reason why SwimSnake group poses such a huge threat is that it is no

longer a simple black market group, but has formed a Fraud as a Service (FaaS) cybercrime operation model. It provides attack methods, tools, and infrastructure to organizations that carry out attack activities in the form of commercialization and on-demand sale or rental, thereby significantly lowering the threshold for committing cyber fraud.

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

Figure 1-1Long press to identify the QR code to view the detailed information of the "SwimSnake" group

2 Infection Signs and Activity Characteristics

After running the malicious code, the attacker gained remote control privileges, but they didn't immediately exercise remote control. Instead, they waited for an opportunity. For example, they would remotely control a user's computer after work and leave it on. Taking advantage of the user's computer being left on, or instant messaging apps like WeChat and DingTalk being open, they would create new groups and send malicious code to spread the malicious code further, infecting more victims.

Attackers will update the payload file from time to time to evade detection by anti-virus software.

This type of malicious program will drop files such as C3Exporer.exe, libcef_dll_wrapper.dll, libcef_dll_wrapper.bin, and temp.key in C:\Program Files\Internet Explorer.

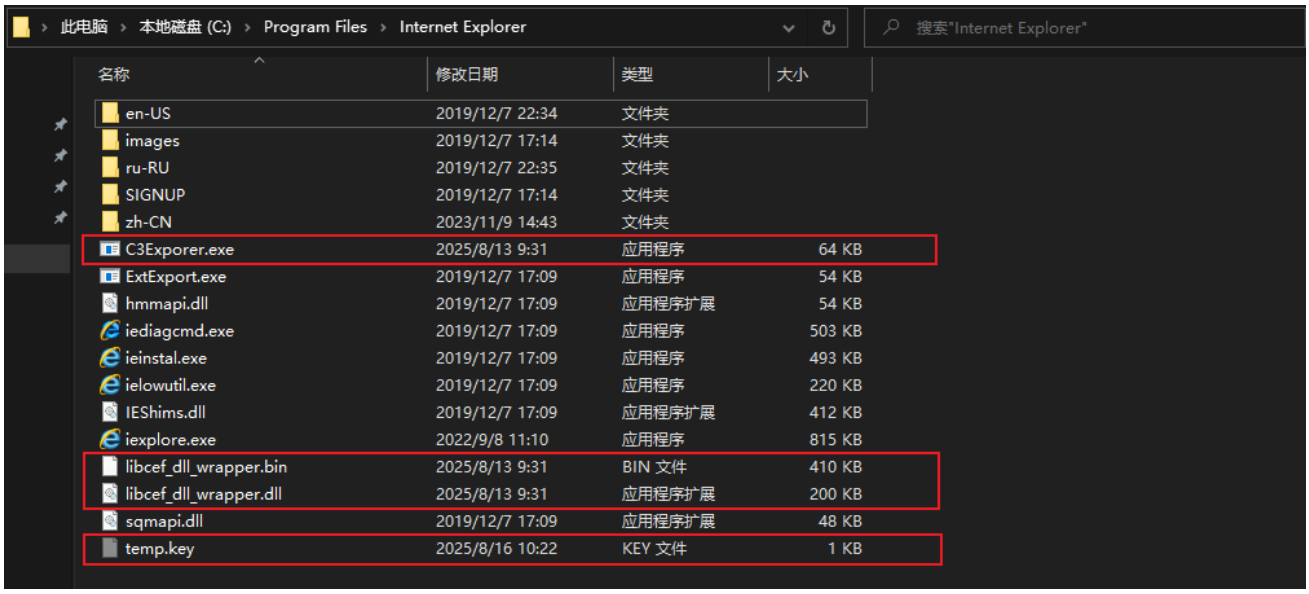

Figure 2-1Related malicious files

A malicious scheduled task exists in the Task Scheduler's \\Microsoft\\Windows\\AppID directory that launches the C3Explorer.exe program, enabling the malware to establish a persistence mechanism.

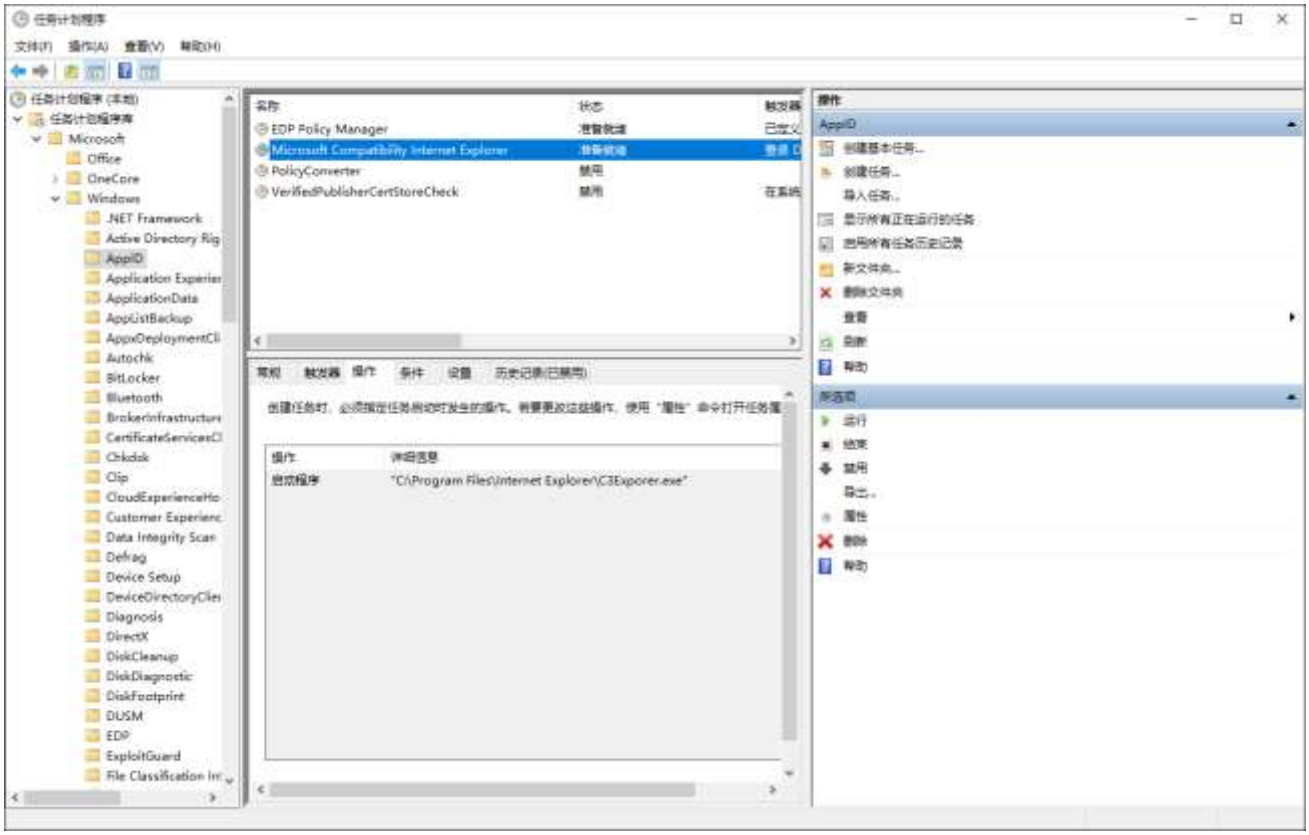

Figure 2-2Malicious scheduled tasks

If you find any of the above traces on your computer, delete the relevant malicious files and malicious scheduled tasks and restart the computer to clear the remote control Trojan running in the system process memory. To more

accurately and comprehensively eliminate threats on the victim host, users who discover such threats can contact the Antiy Emergency Response Team (cert@antiy.cn) for handling.

3 Sample Analysis

3.1 Analysis of Typical Initial Propagation Samples

In one instance of propagation, the attacker disseminated a payload to the victim's WeChat group via a compressed file named "2025-Q2 List of Internal Personnel Violations.zip". The package contained a 56.7K PE executable file, named "ds List of Internal Personnel Violations for the Second Quarter of 2025 nirotetmeoNFIWETQ (2).exe". This represents a classic filename obfuscation social engineering technique.

Table 3-1Sample tags

Virus name	**Trojan/Win32.SwimSnake**
Original file name	ds List of Internal Personnel Violations for the Second Quarter of 2025 nirotetmeoNFIWETQ (2).exe
MD5	1D833AC2A1AD219577143B095D33AF4E
Processor architecture	Intel 386 or later processors and compatible processors
File size	56.7 KB (58,064 bytes)
File format	BinExecute/Microsoft.EXE[:X 64]
Timestamp	2025-08-12 04:26:17
Digital signature	Chengdu GoldArmor Technology., Inc. (Invalid digital signature)
Packer type	none
Compiled language	Microsoft Visual C/C++

Attackers bypass host protection software with immature white-protection mechanisms by adding an invalid and expired digital signature. The object signed by the digital signature does not match the file and therefore cannot pass the signature verification.

Figure 3-1This sample has an invalid digital signature

After execution, the program checks the current user's permissions and ensures it is running as an administrator.

Figure 3-2Check permissions and make sure to run as administrator

After searching for the VSS service, it starts the service and executes the VSSVC.exe process.

Figure 3-3Start the VSS service and execute the VSSVC.exe process

The shellcode is injected into the memory space of the target process VSSVC.exe through PoolParty and then self-deleted.

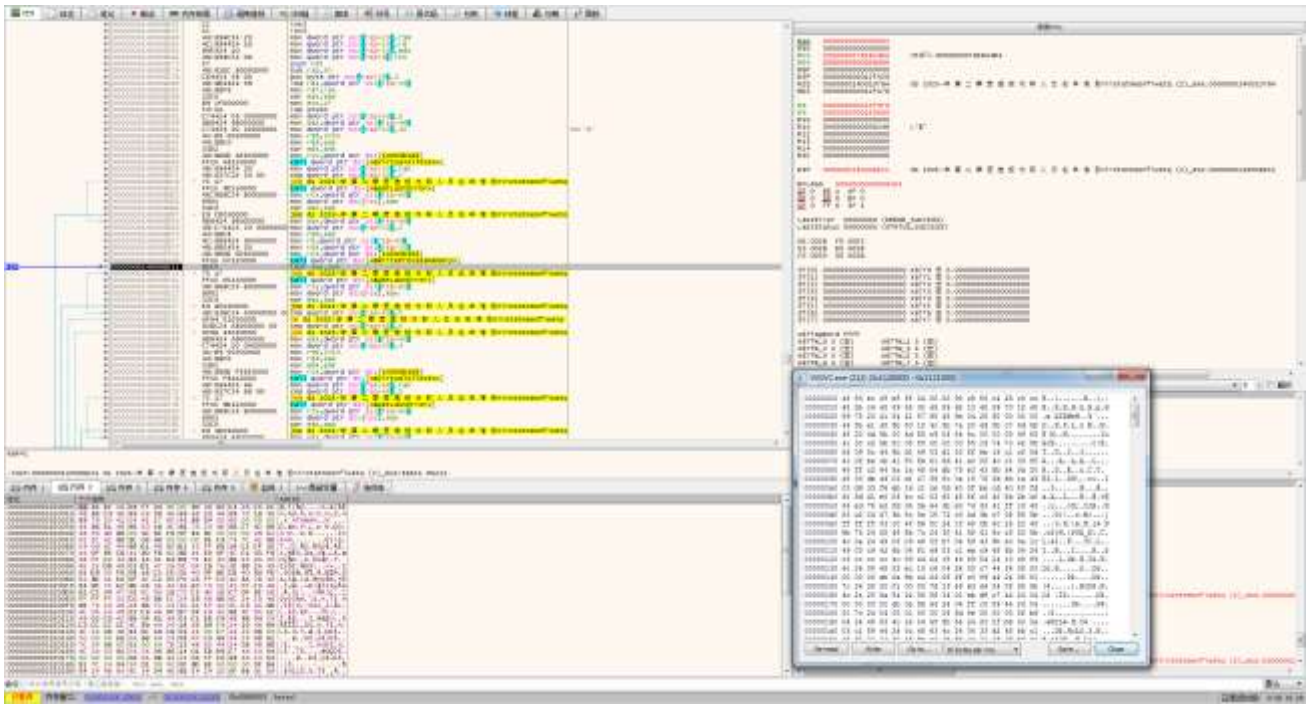

Figure 3-4 Inject shellcode into the VSSVC.exe process using PoolParty techniques

3.2 Download the Encrypted Trojan and Run the Process

The Shellcode decrypts and obtains the C2 server address.

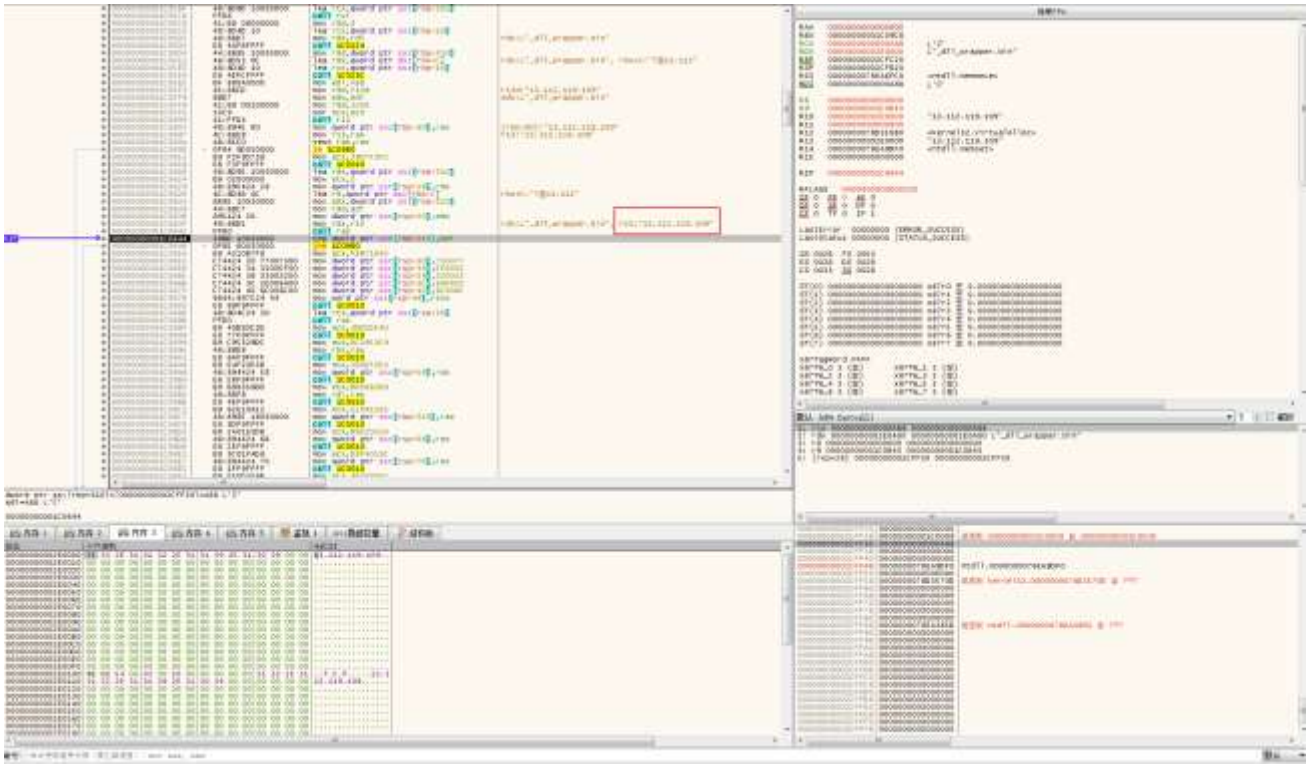

Figure 3-5Decrypted C2 server address

Apply for a memory space, connect to the C2 server address and receive data.

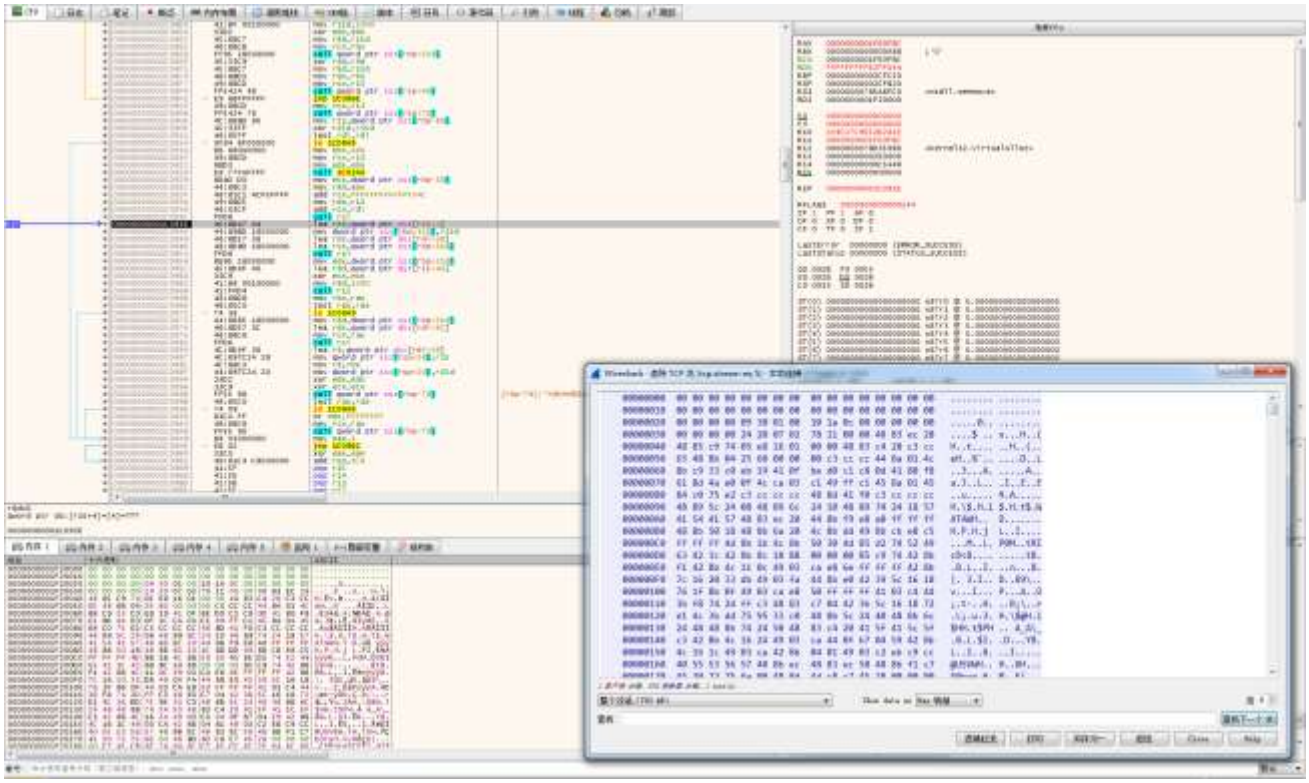

Figure 3-6Connecting to the C2 server address and receiving data

It is decrypted in memory to obtain a file originally named "InstallEx.dll", and its "run" export function is executed to achieve memory operation.

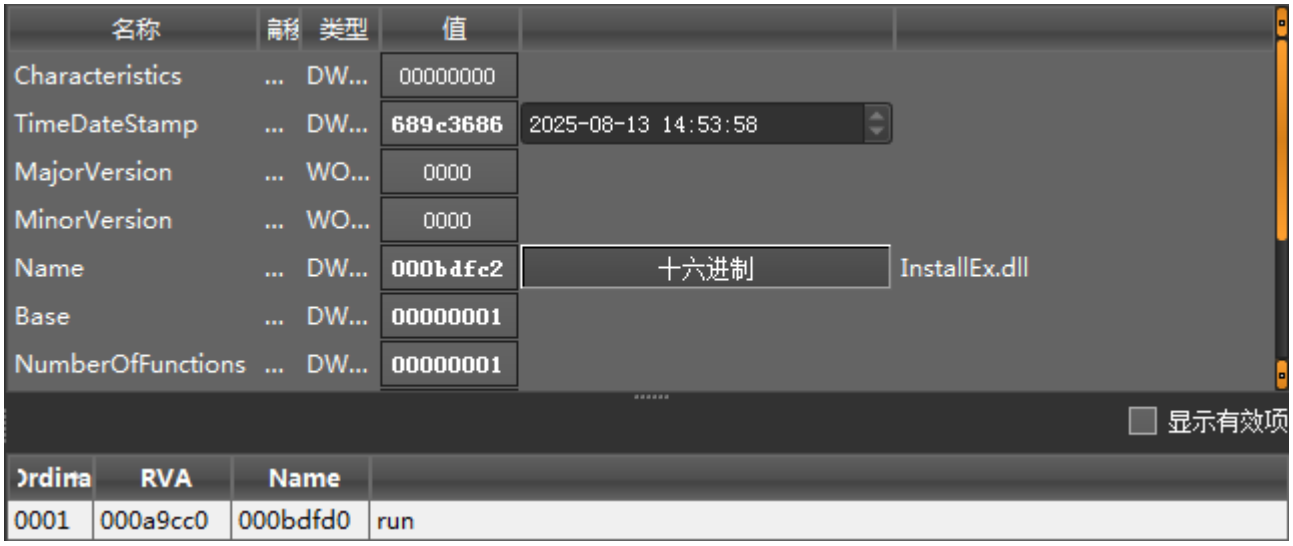

Figure 3-7Decrypted InstallEx.dll

3.3 Download the running executor InstallEx.dll

The DLL file first ensures that the currently loaded running process is "svchost.exe", "Winlogon.exe",

"dllhost.exe", "vssvc.exe", or "explorer.exe". If not, it injects the code into the memory of the target process and then executes the subsequent process.

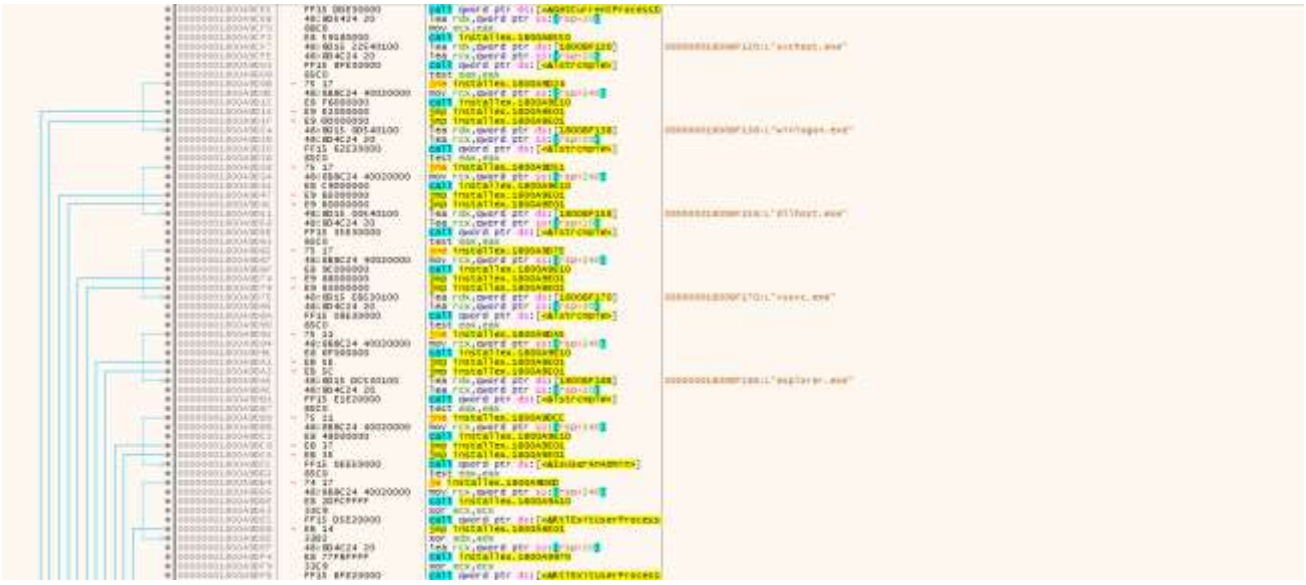

Figure 3-8Check whether the current process is the specified process

Create a mutex "Global\\Admin!!!" to avoid duplicate loading.

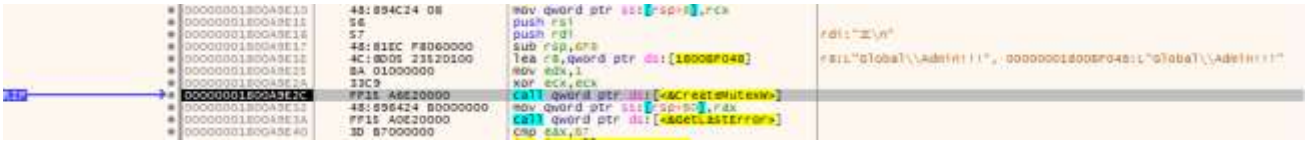

Figure 3-9Creating a mutex

Traverse the processes to detect whether there is a 360tray.exe process and bypass 360 in a targeted manner.

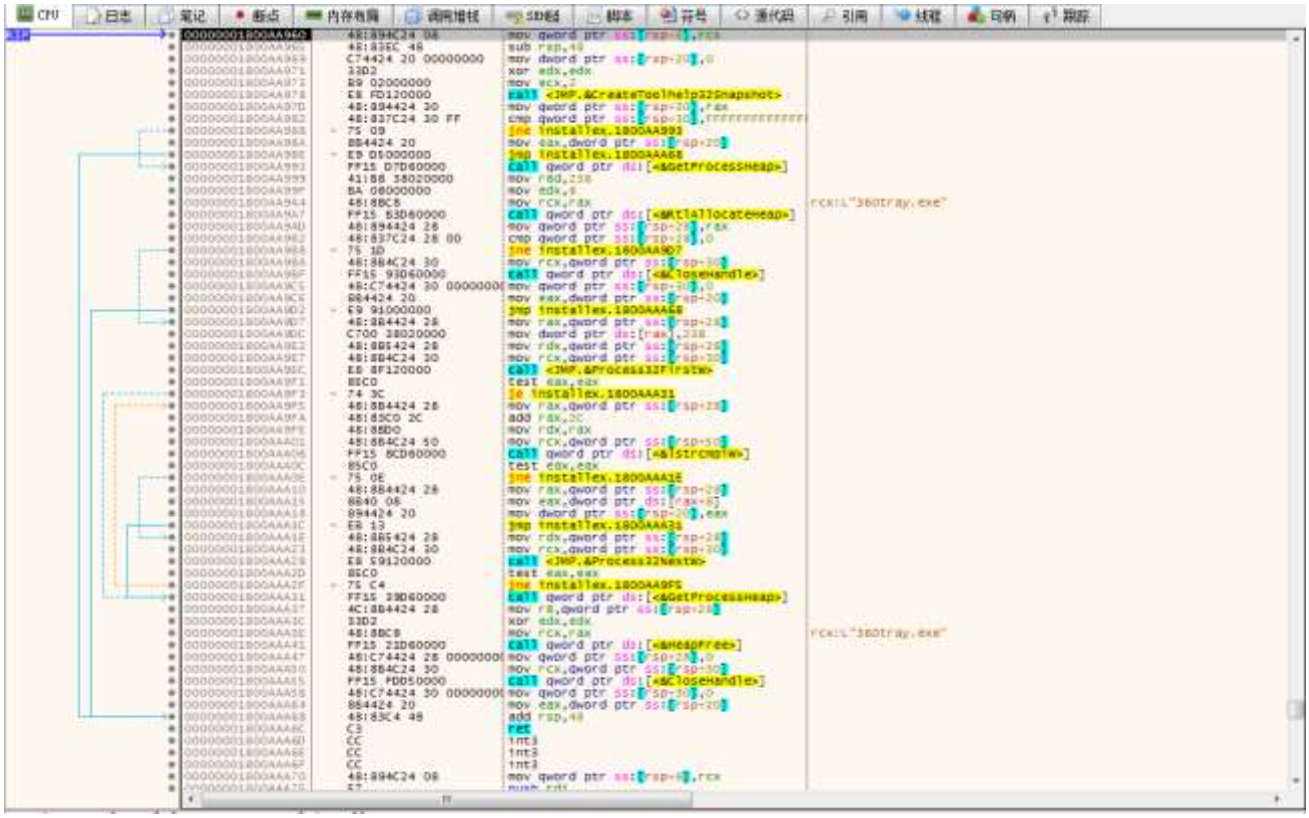

Figure 3-10Traversing the process and detecting whether 360tray.exe exists

This DLL file contains C3Exporer.exe, libcef_dll_wrapper.dll, and libcef_dll_wrapper.bin. It writes these three files (white and black) to C:\Program Files\Internet Explorer and creates a scheduled task for C3Exporer.exe at \\Microsoft\\Windows\\AppId to achieve persistence.

Figure 3-11Release three files and create a scheduled task

3.4 White and Black Payload Loading Process

libcef_dll_wrapper.dll is loaded and executed, it reads the bin file with the same name in the same path and decrypts it to obtain the final payload. The original name of the file is Server64.dll.

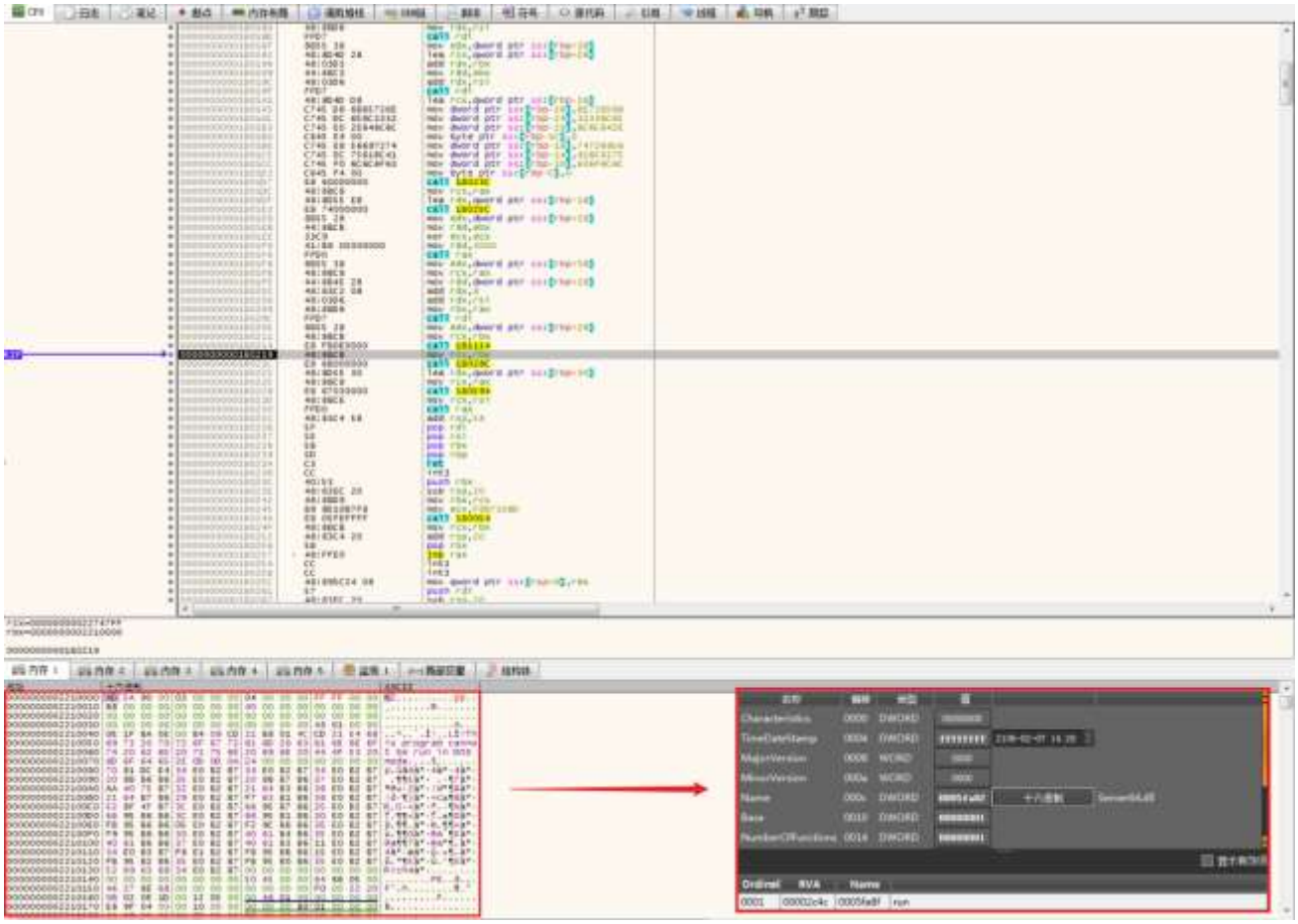

Figure 3-12Decrypting the bin file in the same path to obtain the final payload

3.5 Remote Control Trojan Server64.dll

Server64.dll is a remote control Trojan. This remote control Trojan belongs to the same category (Gh0st) as the remote control Trojan ultimately released by the first-category sample in the report titled "Malware Attack Rampant, Launch Immediate Specialized Inspection and Disposal". It possesses multiple functionalities, including network communication, file downloading, remote control, file management, and keylogging.

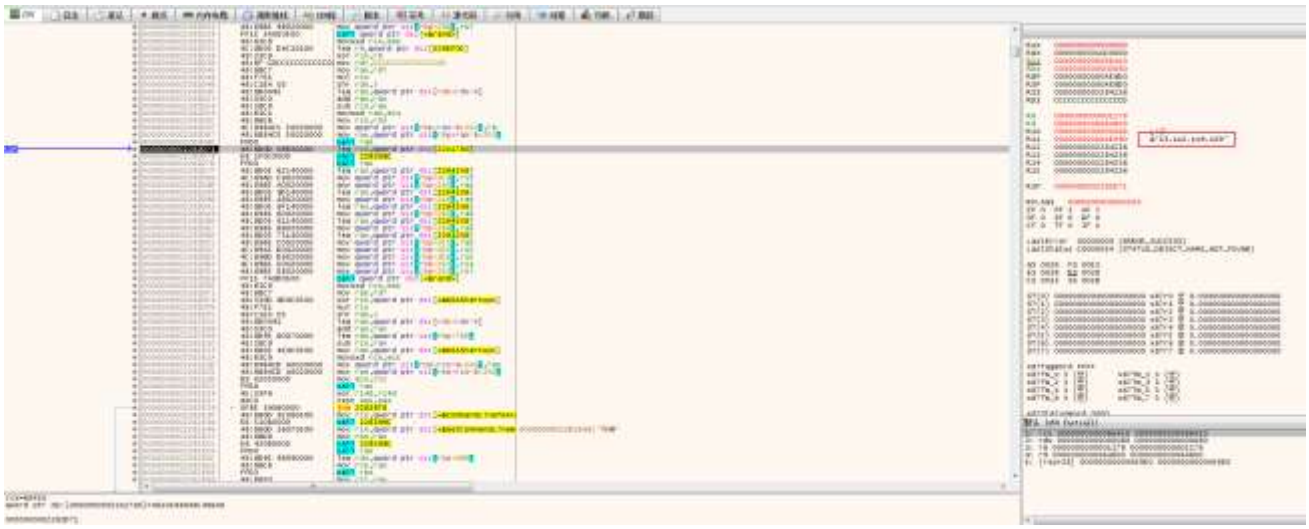

Figure 3-13The C2 address connected by the remote control Trojan

4 Tactical Analysis and Beacons of Attack Activities

4.1 Attack Tactics Annotation

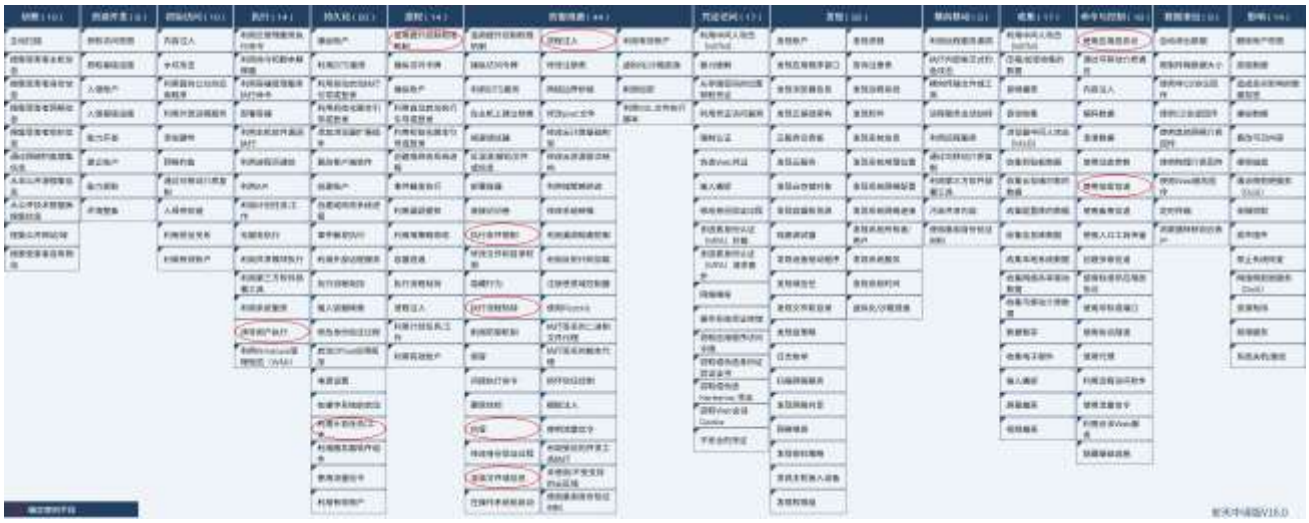

Figure 4-1 Mapping of technical features to ATT&CK

Tactical behavior description table:

Table 4-1 ATT&CK technical behavior description table

ATT&CK stages/categories	Specific behavior	Notes
Execute	Induce users to execute	Disguised as an internal file to trick victims into executing
Persistence	Utilize scheduled tasks/jobs	Achieve persistence by creating a scheduled task
Privilege escalation	Abuse of the control privilege escalation mechanism	Induce users to run with administrator privileges
Defense evasion	Execution condition restrictions	Detect the 360tray.exe process
	Execution process hijacking	Load DLL using white and black method
	Counterfeit	Use an invalid digital signature
	Obfuscate files or information	Encrypt shellcode
	Process injection	Inject Shellcode into the target process through PoolParty
Command and Control	Use application layer protocols	Use HTTP protocol for communication
	Use encrypted channels	Communication data is encrypted

4.2 Some IoCs Beacons

The following are some of the executable payload hashes and C2 addresses from related attack activities. It's important to note that due to the rapid evolution of the SwimSnake attack and the subsequent execution chain consisting of memory-based Trojans, hash intelligence is essentially worthless, and the C2 itself has very low timeliness. Fighting SwimSnake attacks tests the host security software's primary defense and antivirus engine capabilities, as well as the responsiveness of security product manufacturers and engine providers.

IoCs
1D833AC2A1AD219577143B095D33AF4E
95B4D47D7183F9BFC172AE3848B4A01E
1D668425CD90659D08F27BB0B689786F
0F70BBBF2FA68818315EFBEBB1CD9EF2
FF426DF9872124672C73FFED67D8BC8D
13.112.119[.]109

5 Fraud as a Service: Effectively Addressing New Trends

A key reason why "SwimSnake" poses such a significant threat is that it is no longer simply a black market group. Instead, it has developed a Fraud as a Service (FaaS) cybercrime operation model. This model provides attack methods, tools, and infrastructure to organizations carrying out offensive activities in a commercialized, on-demand sales or rental format, significantly lowering the barrier to entry for cyber fraud. This means that attack organizations operating under this model are no longer limited to a single, early-stage group, but have expanded into a diverse network. Furthermore, these organizations have both upstream and downstream relationships, as well as no direct connection, simply reusing and mimicking tactics.

"Fraud" and "Scam" are used interchangeably to describe fraudulent activities. To describe the fraud-as-a-service model potentially employed by the SwimSnake group, Antiy CERT searched historical documentation and discovered the terms FaaS (Fraud-as-a-Service) and SaaS (Scam-as-a-Service). Antiy CERT conducted internal discussions based on legal definitions, technical characteristics, and industry consensus, and also consulted AI platforms. While "scam-as-a-service" is a more commonly used term in the industry (DeepSeek also recommends its use), its abbreviation is identical to the more commonly used "software-as-a-service" abbreviation, a significant flaw. Generally speaking, FaaS typically encompasses a complete criminal ecosystem, such as full identity theft services offered on dark web markets, while "scam-as-a-service" more often refers to ready-to-use attack toolkits, such as phishing website templates purchased by cybercriminals. Based on the continuous tracking and analysis of the attack activities of the SwimSnake group over the past few years, Antiy CERT believes that SwimSnake's "Fraud as a Service" model is no longer limited to the level of attack toolkits, and it is more accurate to use FaaS to express it.

SwimSnake's FaaS model represents that the "convergence" of cyberattacks and fraud crimes has entered a "mature" stage. Defending against them cannot simply rely on the self-protection of government and enterprise organizations and personal security awareness. Cracking down on them is not simply the responsibility of judicial organs, but has become a complex social governance.

6 Antiy IEP EDR Helps Users Defend Against SwimSnake Threats

After testing, Antiy Intelligent Endpoint Protection System product series (hereinafter referred to as "IEP"), relying on Antiy's self-developed threat detection engine and kernel-level active defense capabilities, can effectively detect and defend against the virus samples discovered this time.

IEP monitors local disks in real time and automatically detects viruses on newly added files. In response to this threat, when the virus file libcef_dll_wrapper.dll is found locally, IEP immediately detects and kills the virus and sends an alert to the user, effectively preventing the virus from launching.

Figure 6-1When a virus file is dropped, IEP immediately captures it and sends an alert

In addition, IEP features a driver-level active defense module that monitors process behavior in real time. When risky processes are detected, they are immediately intercepted, effectively preventing the attack from executing. In this incident, when the attacker used C3Exporer.exe to load the malicious file libcef_dll_wrapper.dll, IEP's memory protection module detected the malicious program loading behavior and immediately blocked it.

Figure 6-2Direct active defense module intercepts malicious program loading behavior

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.

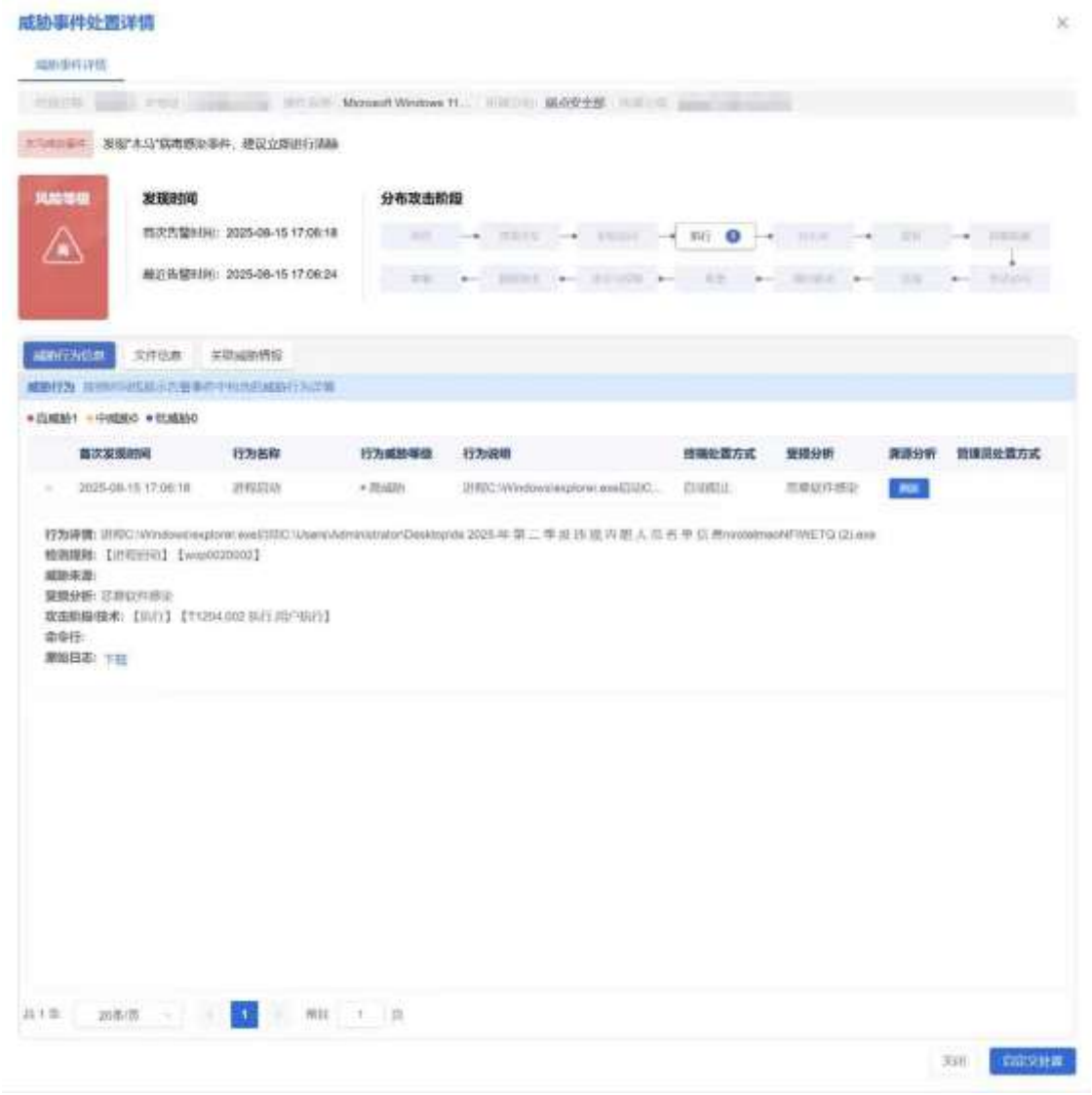

Figure 6-3 IEP Management Center empowers administrators to achieve efficient endpoint security management

The anti-Virus Trojan tool has been updated and users can download it from the vertical response platform vs2.antiy.cn.

List of Historical Analysis Reports on SwimSnake by Antiy

Since 2022, Antiy CERT has published 12 analysis reports on SwimSnake.

[1] Analysis of the attack activity of delivering remote control Trojans through the fake Chinese version of Telegram website [R/OL]. (2022-10-24)
https://www.antiy.cn/research/notice&report/research_report/20221024.html

[2] Analysis of attack activities using cloud note platforms to deliver remote control Trojans [R/OL]. (2023-03-24)
https://www.antiy.cn/research/notice&report/research_report/20230324.html

[3] Analysis of a Black Market Group Using Cloud Notes 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" black market 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" black market group [R/OL]. (2023-07-11)
https://www.antiy.cn/research/notice&report/research_report/TrojanControl_Analysis.html

[6] Analysis of the "SwimSnake" black market group's activities in spreading malicious code via WeChat [R/OL]. (2023-08-22)
https://www.antiy.cn/research/notice&report/research_report/SwimSnakeTrojans_Analysis.html

[7] Special Analysis Report on the "SwimSnake" Black Market group [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 by the "SwimSnake" black market 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" black market[R/OL].(2024-04-07)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html

[10] Analysis of the "SwimSnake" black market group's phishing attack activities using malicious documents [R/OL]. (2024-06-21)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html

[11] Phishing download website spreads the threat of "SwimSnake", malicious installer contains remote control Trojan [R/OL]. (2024-12-20)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202412.html

[12] "SwimSnake" black market attacks are rampant, and special investigation and disposal should be launched immediately [R/OL]. (2025-04-23)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202504.html

[13] The entry for "SwimSnake" in the Computer Virus Classification Encyclopedia was updated on 2025-08-16.
https://virusview.net/malware/Trojan/Win32/SwimSnake