

The "SwimSnake" Cybercriminal Group Distributes Remote Control Trojans by Leveraging Counterfeit WPS Office Download Sites

Antiy CERT

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

First published time: May 15, 2025

1 Overview

Antiy CERT discovered that the "SwimSnake" cybercriminal group used a counterfeit WPS Office download site to spread remote control Trojans. If users download WPS Office from this website, they actually download a fake installer hosted in OSS. After the program is executed, a normal WPS installer is released in the temporary folder %temp% to confuse users, and three files are released in the C:\ProgramData folder. After executing the Shine.exe program, the malicious libcef.dll file is loaded. The DLL reads the 1.txt file, thereby executing the file originally named "Install.dll" in the memory, calling its Shellex export function, and finally executing the Gh0st remote control Trojan and creating a registry startup item to achieve persistence.

The "SwimSnake" cybercriminal group (also known as "Silver Fox", "Valley Thief", "UTG-Q-1000", etc.) has been active since the second half of 2022, launching 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 detection are frequently changed, and the industries involved in the attack targets are wide. Users can download and use the "SwimSnake" special investigation tool and the Antiy System Security Kernel Analysis Tool (ATool) on the Antiy Vertical Response Platform (<https://vs2.antiy.cn>) to investigate and remove the "Gh0st" Trojan.

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

2 Sample Analysis

2.1 Phishing Websites

The website impersonating the WPS Office download site `hxxps://wpsice[.]com` :

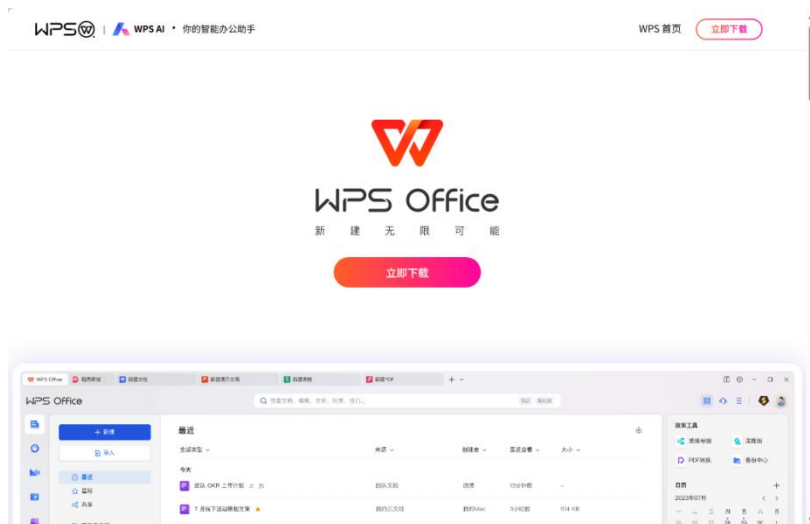


Figure 2-1 Counterfeit website page

If you click the "Download Now" button, you will download a fake installer hosted in OSS.

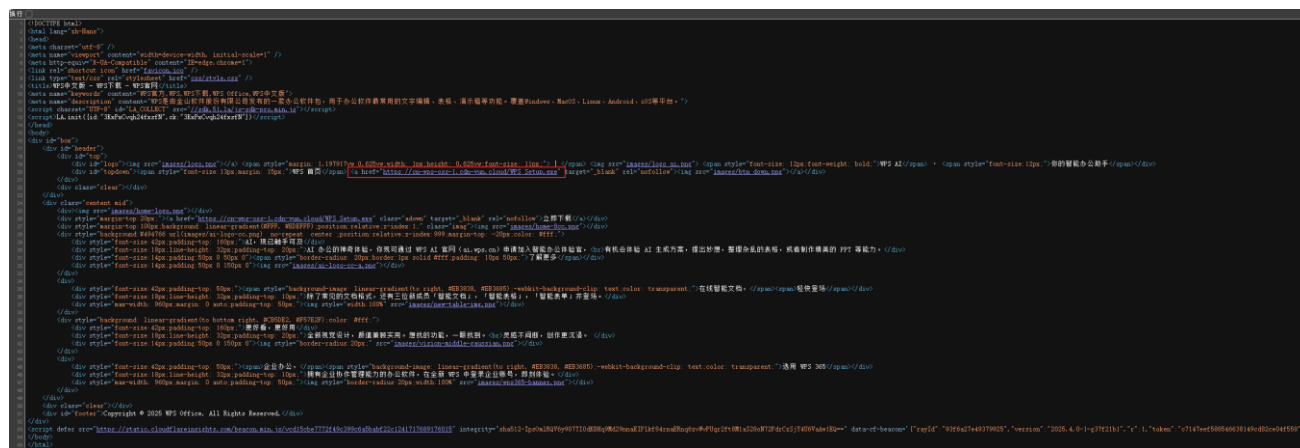


Figure 2-2 The source code of the counterfeit website

2.2 Fake Installer

Table 2-1 Header row table description

| Virus Name | Trojan/Win32.SwimSnake |
|--------------------|------------------------|
| Original File Name | WPS_Setup.exe |

| | |
|------------------------|---|
| MD5 | 9232FBCCF8B566B0C0A6D986B65BBC98 |
| Processor Architecture | Intel 386 or later processors and compatible processors |
| File Size | 253 MB (265,306,009 bytes) |
| File Format | BinExecute/Microsoft.EXE[:X86] |
| Timestamp | 2023-05-31 21 :15:01 |
| Digital Signature | none |
| Packer Type | none |
| Compiled Language | Microsoft Visual C/C++ |

After the program is executed, a normal WPS installation program will be released and executed in the temporary folder %temp% to confuse the user.

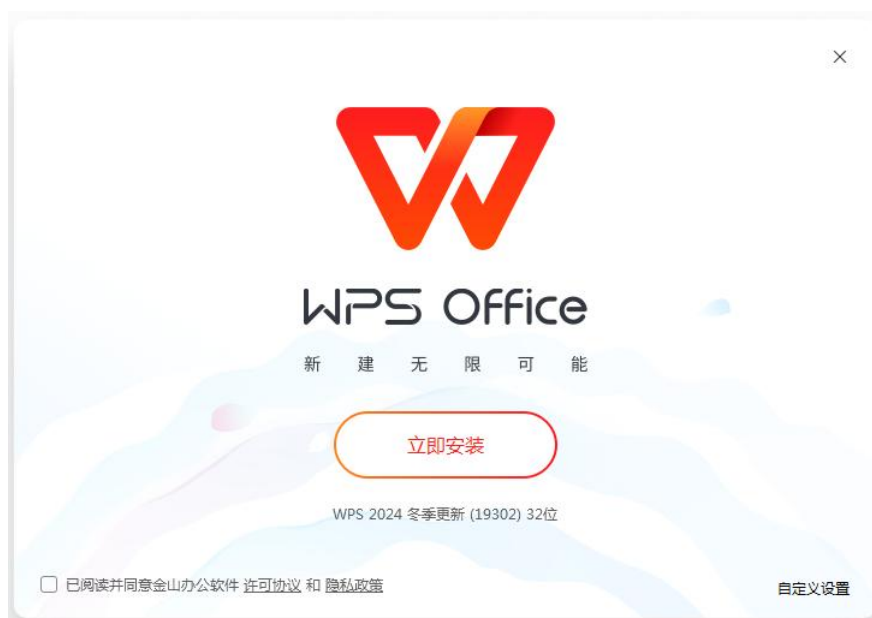


Figure 2-3Release and execute the normal WPS installation program

Then, three files are released in C:\ProgramData: Shine.exe contains a normal digital signature, libcef.dll is a malicious DLL file, and 1.txt is a Shellcode containing the Gh0st remote control Trojan.




| | | | |
|--|----------------|--------|----------|
|  1.txt | 2025/5/6 18:23 | 文本文档 | 1,208 KB |
|  libcef.dll | 2025/5/6 18:23 | 应用程序扩展 | 1,569 KB |
|  Shine.exe | 2025/5/6 18:23 | 应用程序 | 460 KB |

Figure 2-4Dropping attack components in C:\ProgramData

After the Shine.exe program runs, it loads libcef.dll and reads the 1.txt file, thereby loading and executing a file originally named "Install.dll" in the memory and calling its Shellex export function, and finally executing the Gh0st remote control Trojan.

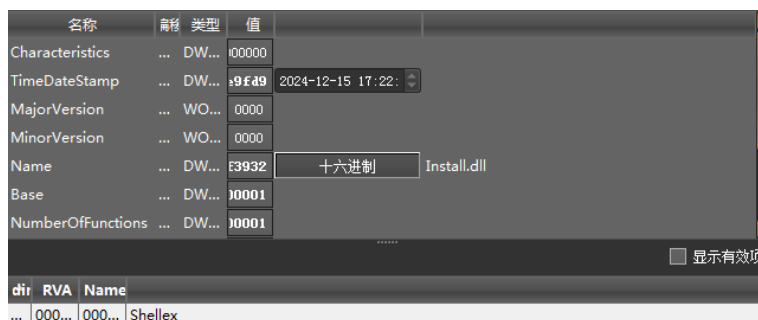


Figure 2-5Install.dll file information

The path of the program is added to the registry startup item "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run " to achieve persistence.

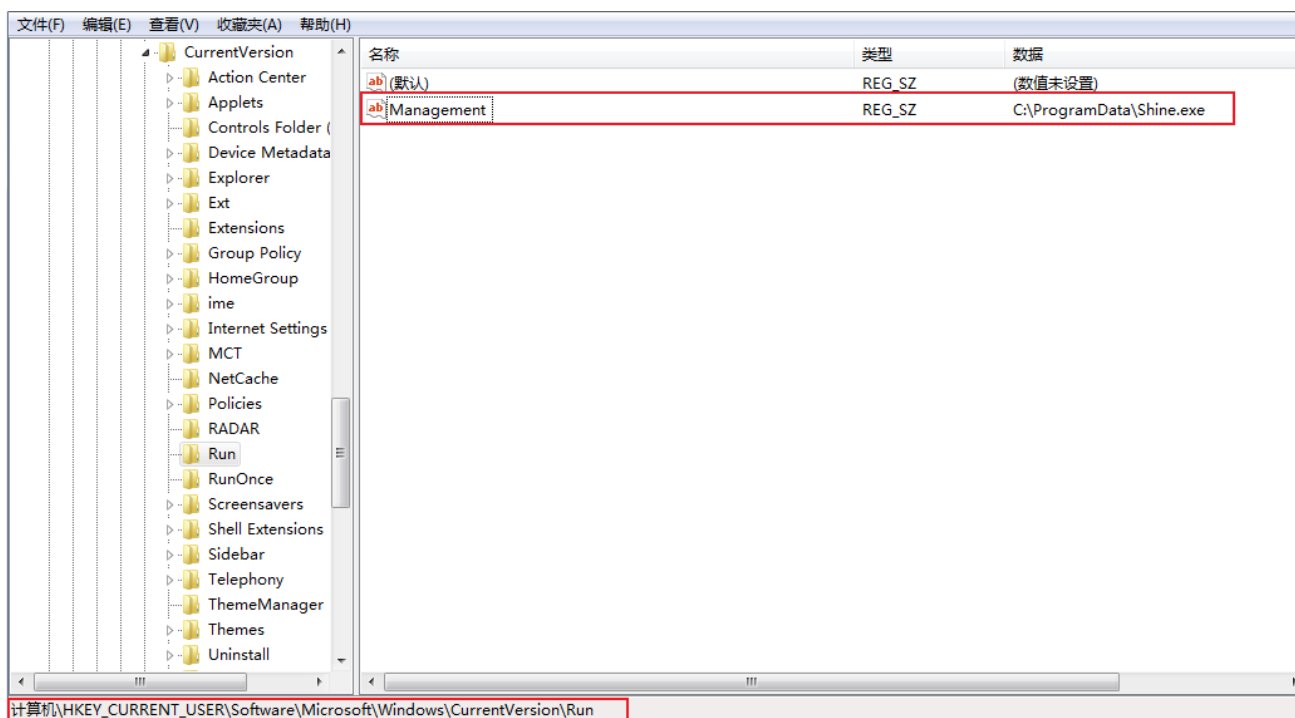


Figure 2-6Creating a registry startup item to achieve persistence

3 Use Tools for Investigation and Handling

Based on the fact that the attackers used variants of the Gh0st remote control Trojan family in this attack, users can download and use the "Visco" special investigation tool and the Antiy System Security Kernel Analysis Tool on the Antiy Vertical Response Platform (<https://vs2.antiy.cn>) to investigate and remove the Gh0st remote control Trojan.

The "SwimSnake" special inspection tool can be used to inspect the loaders dropped by the "SwimSnake" cybercriminal group in its attack activities and the remote control Trojans loaded into the memory (including the Gh0st remote control Trojan family).

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 3-1 Antiy vertical response platform

3.1 Use the "SwimSnake" Special Troubleshooting Tool to Detect the Gh0st Remote Control Trojan

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

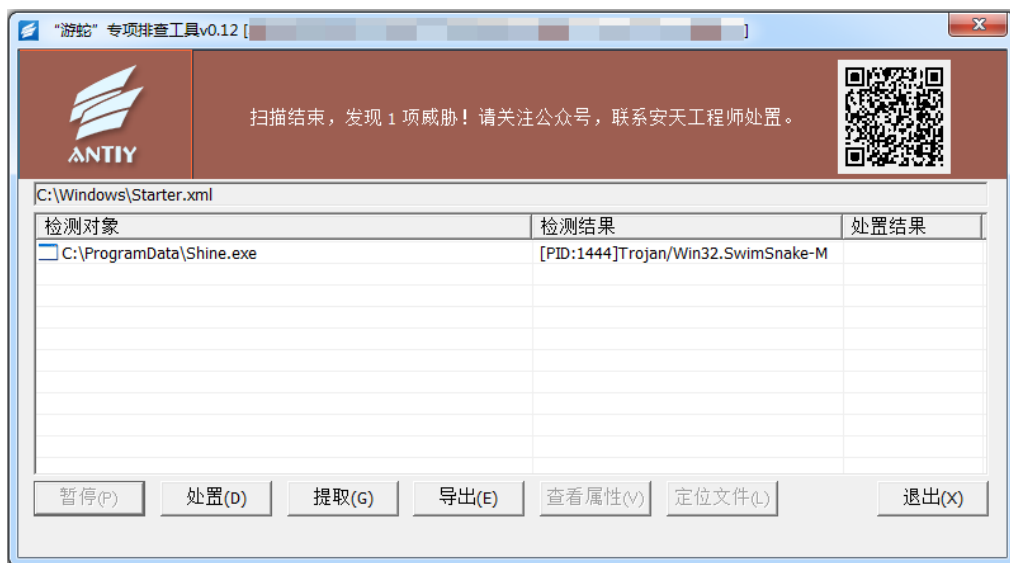


Figure 3-2Using the "SwimSnake" special troubleshooting tool to discover malicious processes

3.2 Use Antiy System Security Kernel Analysis Tool to Remove Gh0st Remote Control Trojan

After discovering the Gh0st remote control Trojan, users can download and use ATool on the Antiy Vertical Response Platform to remove the Trojan. For example, in the "Process Management" page of ATool, right-click the malicious process "Shine.exe" : first click "Locate in Windows File Manager" to locate the path where "Shine.exe" is located, then click "Terminate" to end the "Shine.exe" process, and finally delete the malicious files in the path where the "Shine.exe" program is located .



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

In the "Startup Items" page of ATool, use the "Find" function to search for malicious process names, find and delete malicious startup items.

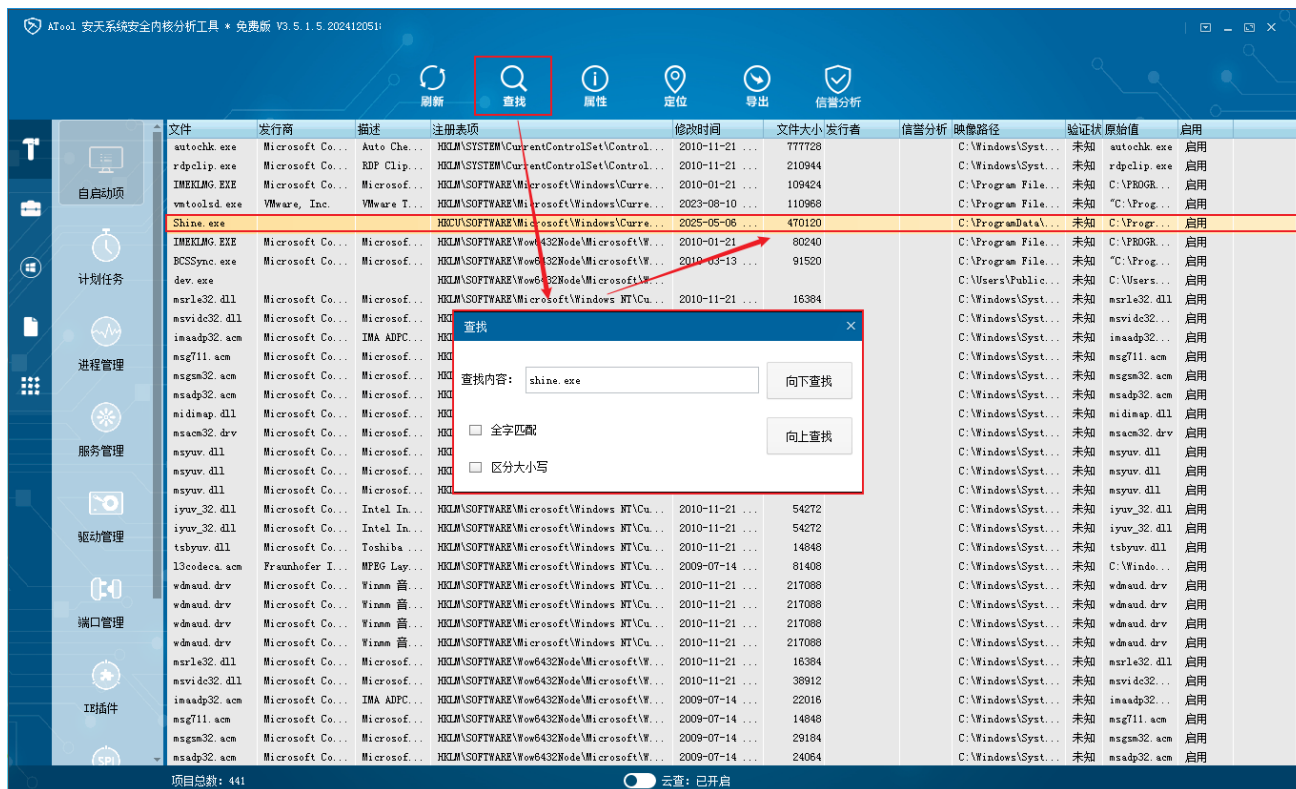


Figure 3-4 Searching for malicious auto-start items by malicious process name

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.

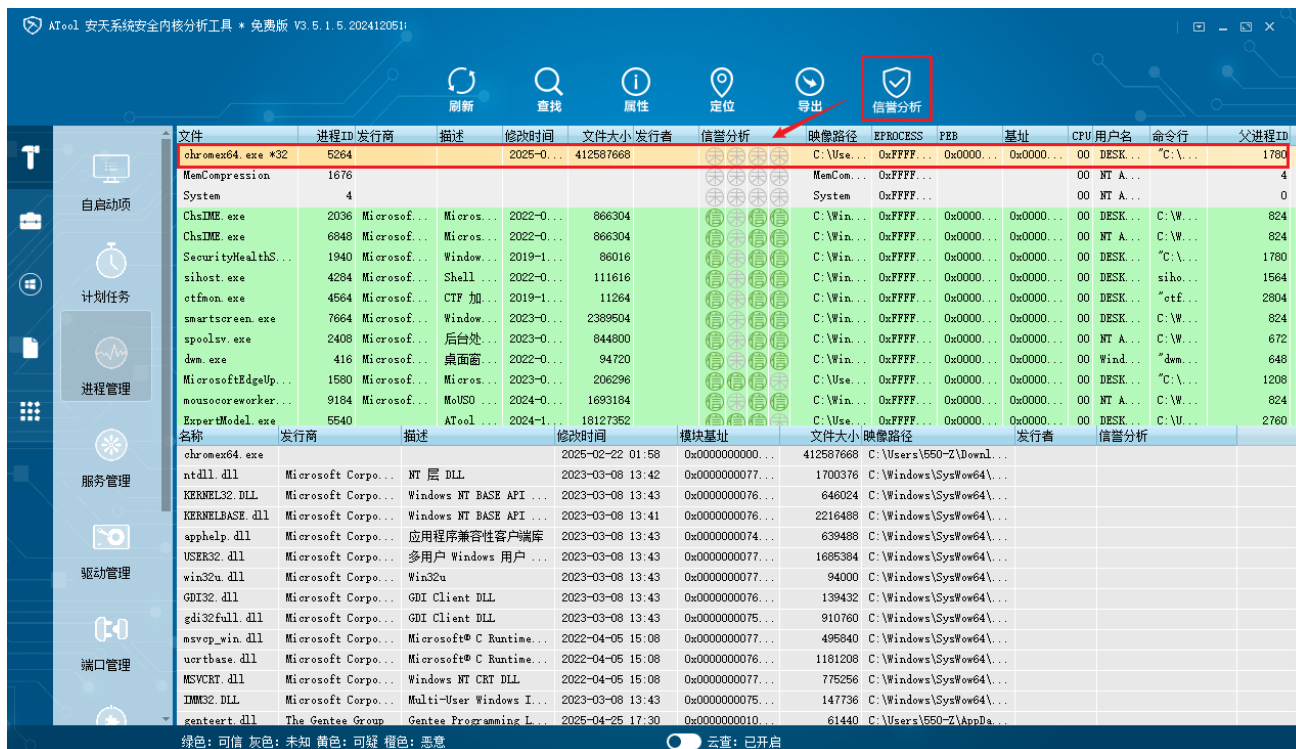


Figure 3-5 Using ATool's "Reputation Analysis" feature to discover malicious processes

4 Terminal Security Protection

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

IEP can monitor local disks in real time and automatically detect viruses on newly added files. In response to this threat, when the virus file libcef.dll is found locally, IEP will immediately detect and kill the virus file and send an alert to the user, effectively preventing the virus from starting.

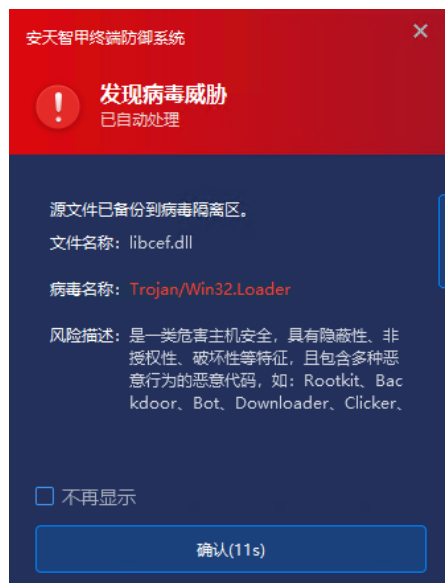


Figure 4-1 When a virus file is dropped, IEP will capture it and send an alert immediately

In addition, IEP has a driver-level active defense module that can monitor process behavior in real time. When a process is found to have risky behavior, it can be immediately intercepted to effectively prevent the execution of attack behavior. In this incident, when the attacker used Shine.exe to load the malicious file libcef.dll, IEP would capture the loading behavior of the malicious program through the memory protection module and immediately intercept it.



Figure 4-2 Direct 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.

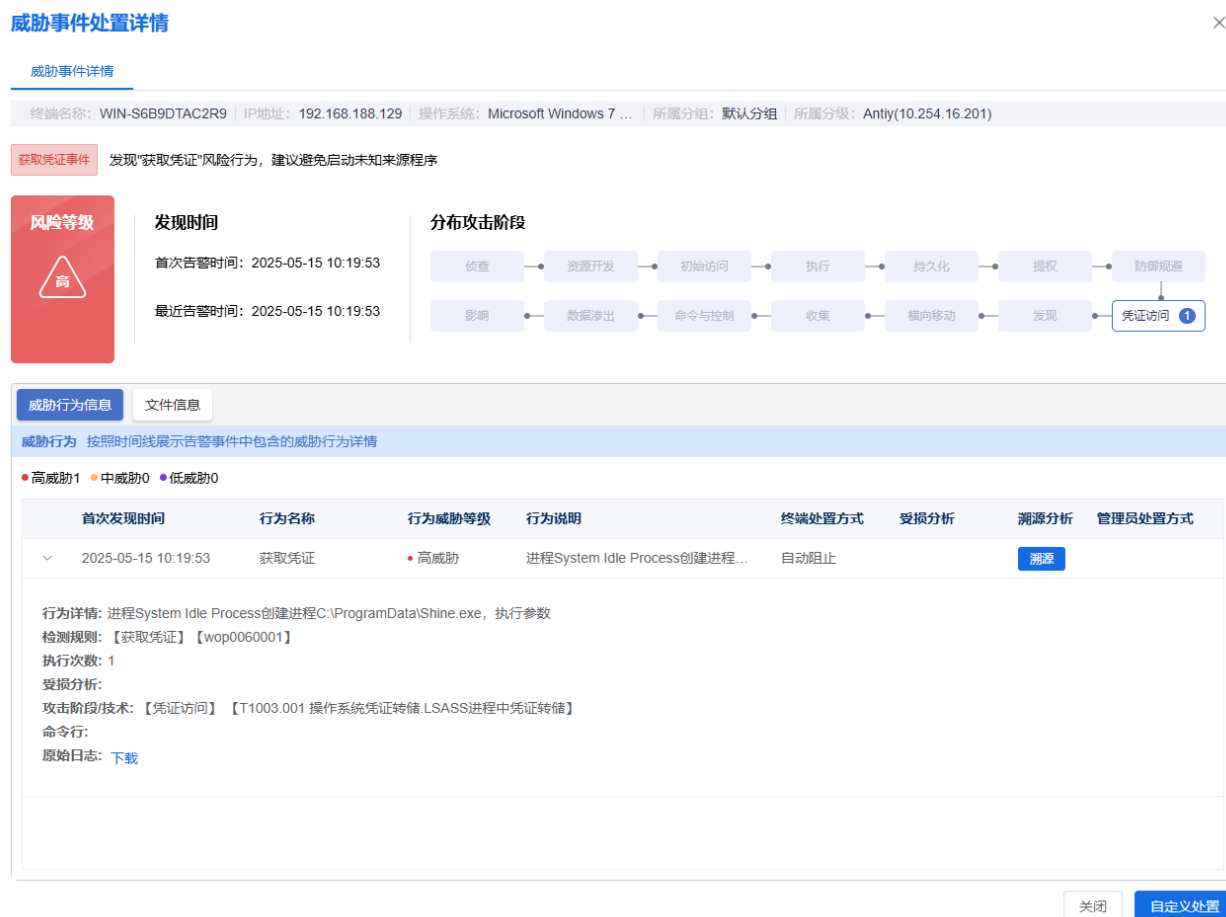


Figure 4-3 IEP Management Center helps administrators achieve efficient terminal security management

5 Attack Payload Executor Life Cycle and Security Product Key

Capabilities Mapping Matrix

Through threat event analysis, we can obtain the attack process of running objects and running actions in the entire life cycle of the attack payload execution body, and further evaluate the key capability mapping matrix of anti-virus engine and active defense that the security protection software deployed on the terminal side should have. The key capabilities of detection and defense of this series of attack activities are described in the following table:

| Attack Executor Lifecycle | Object | Action | Threat Detection Engine Key Capabilities | Active Defense Capability Key Capabilities |
|---------------------------|--------|--------|--|--|
|---------------------------|--------|--------|--|--|

| | | | | | |
|-----------------------|-----------------------|---|---|---|---|
| Pre-set and drop | Drop | Phishing Websites | Impersonating the WPS Office download site, tricking users into downloading a backdoored installer. The program is larger than 200M . | Phishing Domain Detection | <ol style="list-style-type: none"> 1. (Host firewall) monitors application access to C2 server request packets, obtains accessed IP, domain name and URL, and detects the delivery engine to intercept threat C2 server access request packets 2. (Host firewall) Set record/alert/block rules for application request IP, Domain and URL for untrusted addresses |
| Load Execution | Execute | Installer bundled with backdoor | Release the file: %temp%\WPS_Setup.exe (white file) C:\Program Data \Shine.exe (white file) C:\Program Data \libcef.dll C:\Program Data \ 1.txt | <ol style="list-style-type: none"> 1. Installation package type identification 2. Installer derivative files disassemble and recursively detect 3. Identification of redundant and false data anomalies in large files | <ol style="list-style-type: none"> 1. (File defense) Monitor disk file creation/modification, delivery engine detection, and delete threat files 2. (File defense) Set up full file monitoring |
| | | Load and decrypt; 1. White plus black loading : Shine.exe (white file) 2. Decryption: libcef.dll | Shine.exe (white file) load: libcef.dll libcef.dll decryption: 1.txt Solved: Install.dll (executable file) | <ol style="list-style-type: none"> 1. Offline digital signature verification 2. PE format and compiler type identification 3. PE real entry point malicious instruction detection | (Process defense) Monitors process module loading, disassembles the full path of the process and the full path of the loaded module, and then detects the delivery engine, intercepts the loading of threat modules, and deletes the threat modules. |
| | | Memory Loading: Install.dll | Gh0st Remote Control Trojan | Gh0st remote control trojan embedded malicious command detection | <ol style="list-style-type: none"> 1. (Memory Defense) Monitor memory loading behavior 2. (Memory Defense) Set to prohibit loading memory containing certain shellcode content |
| | Persistence | Add a registry startup item: libcef.dll | Add a registry startup item: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Value: String: "Management" : "C:\Program Data\Shine.exe" | Registry key detection | (Registry defense) Monitors the creation/modification of registry startup items, disassembles the file path, startup item name and content of the registry modification process, and then delivers engine detection and deletes threat startup items |
| Effective Application | Process effectiveness | Remote control Trojan (Gh0st): Install.dll | <ol style="list-style-type: none"> 1. Collect system information and send online packets back to C2 2. Wait for receiving and execute remote control commands | Remote control C2 domain name detection | <ol style="list-style-type: none"> 1. (Host firewall) monitors application access to C2 server request packets, obtains accessed IP, domain name and URL, and detects the delivery engine to intercept threat C2 server access request packets 2. (Host firewall) Set record/alert/block rules for |

| | | | | | |
|--|--|--|--|--|--|
| | | | | | application request IP, Domain and URL for untrusted addresses |
|--|--|--|--|--|--|

6 IoCs

| IoCs |
|--|
| 9232FBCCF8B566B0C0A6D986B65BBC98 |
| A9710294489B6893F59120C5DF76A60C |
| 444F87D1D78B9C1162963D6F775FB60E |
| h xx ps://wpsice [.] com |
| h xx ps://cn-wps-oss-1.cdn-yun [.] cloud/WPS_Setup.exe |
| 45.207.12 [.] 71:1803 |

7 List of Historical Reports on the Threat of "SwimSnake" By Antiy

- [1]. Analysis of the Attack Activity of Launching Remote Control Trojans Through Forged 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 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 the 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 Attack Activities of 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 Carry out Phishing Attacks
[R/OL].(2024-06-21)

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

- [11]. Phishing Download Website Spreads "Swimsnake" Threat, Malicious Installer Hides Remote Control Trojan
[R/OL].(2024-12-20)

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

- [12]. "Swimsnake" Cybercriminal 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

Appendix 1: References

[1]. [Identified] Fake WPS website [R/OL]. (2025-05-08)

<https://bbs.kafan.cn/thread-2281325-1-1.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 cyberspace 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.