Hidden Threats: Analysis of Active "Poisoning" Incidents Disguised as Open-source Projects

Antiy CERT

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

Time of first release:17 April, 2025

1 Overview

In recent years, the use of open source ecological trust in GitHub disguised open source projects for malicious code "poisoning" attacks continue to exist. Since the end of 2024, Antiquity CERT has continued to monitor attacks on remote Trojans delivered using Electron packages in this way. In that visual studio project compile configuration of the open source code, the attacker embed the malicious code into the visual studio project compilation configuration of the open source code, aiming at the user group who download the open source project to compile, develop and use the open source project, It makes the project execute the hidden command first, and make use of the load developed by multi-layer different languages and compile tool chain to realize the obfuscating load, avoid the security detection, and finally execute the remote control Trojan packaged by Electron. Related attack activity is still active, and infrastructure such as payload download URLs in the sample is still accessible.

At present, the detection rate of relevant samples is relatively low among all kinds of antivirus engines, and the antivirus engine of Antiy AVL SDK adopts full-format accurate identification and in-depth pre-processing. Support fine-grained disassembly of package files distributed by applications in the format of asar, such as Electron package, and accurate detection of embedded malicious scripts and other sub-files. The terminal defense system of Antiy IEP can effectively detect and kill the remote control Trojan.

Asar files are a proprietary format commonly used in Electron applications. Its full name is "Atom Shell Archive," which is an archive file format, similar to ZIP or TAR, and can package multiple files into one file. It packs many files, such as JavaScript files, HTML files, CSS files, pictures, fonts, and other resources into a single file according to a specific structure and algorithm.

Please refer to Antiy Virusview for the information of this format document.

Figure 1-1 Long press the identification QR code to view the detailed information of the ASAR file 1

2 Analysis of attack activities

The attacker creates open source projects with contents such as vulnerability exploitation tools and game plug-ins, embeds the malicious compilation configuration code in its Visual Studio project configuration, and uploads it to the GitHub open source platform. Use Open Source Users' Trust in Open Source Resources to Induce Downloads.

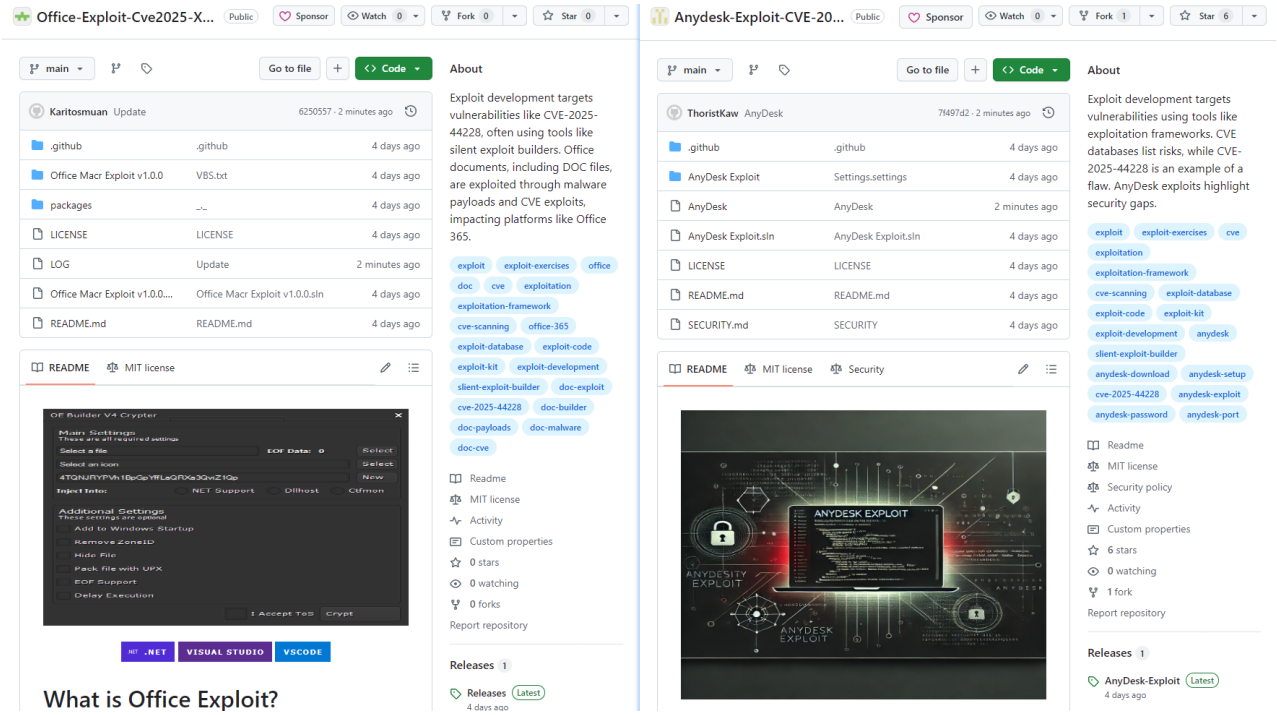

Figure 21 Part of a poison project on an open source platform 2-1

The disguised project uses the GitHub Action function to automatically and repeatedly submit the current date to the project repository, making the last update date of the project always new, increasing the chance of the victim downloading the compiled project. The submission code uses a hard-coded email address ischhfd83 @ rambler.ru.

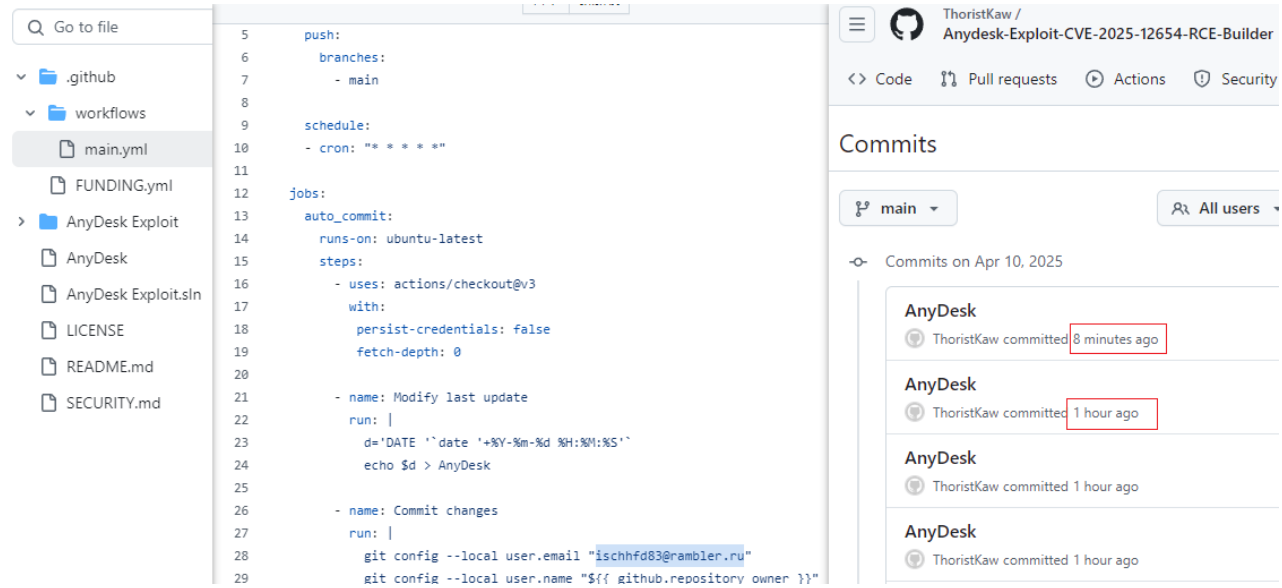

Figure 22 Automatic submission of project codes 2-2

The malicious code is triggered by the PreBuildEvent mechanism of the Visual Studio project, which is used to specify the command line code to be executed before the project is compiled and stored in the project file (. * proj file, such as .vcproj, .vbproj, etc.). Can be viewed through the Project Properties window and cannot be found by examining the project source code. The malicious code triggers execution when the project code is compiled.

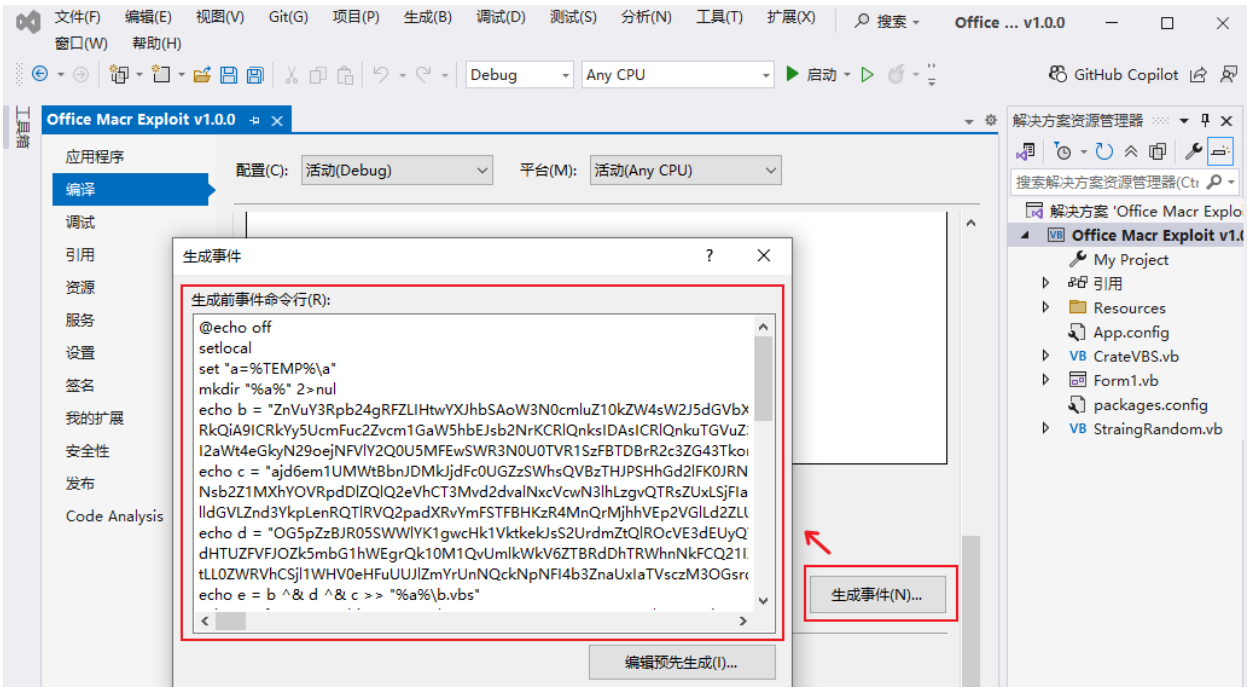

Figure 23 Viewing malicious code through project properties 2-3

Figure 24 Viewing malicious code through a project file 2-4

This code uses algorithms such as Bat, PowerShell script, Base64 and AES to nest and execute multi-layer follow-up payload, and attempts to obtain download addresses from many public websites such as pastebin, rlim, etc. Download an encrypted compression package containing multiple files from this address and decompress (the files in the package are a group of Node .JS programs packaged by Electron), and then execute the main program SearchFilter. exe extracted. Programs packaged with Electron actually execute JavaScript code, with a high degree of flat confusion in the code, Remote control functions such as return of system information through Telegram API, anti-virtual machine, closing of Windows Defender anti-virus software, screenshot, persistence of scheduled tasks, and downloading of subsequent loads are realized.

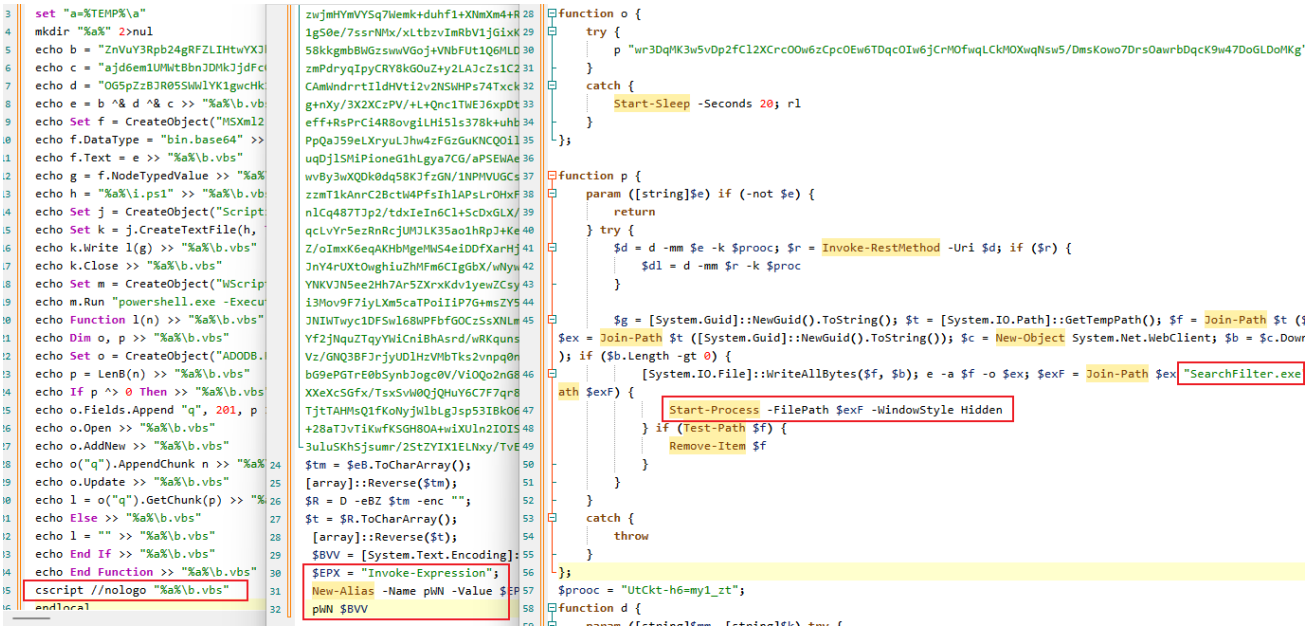

Figure 25 Multi-layer loading 2-5

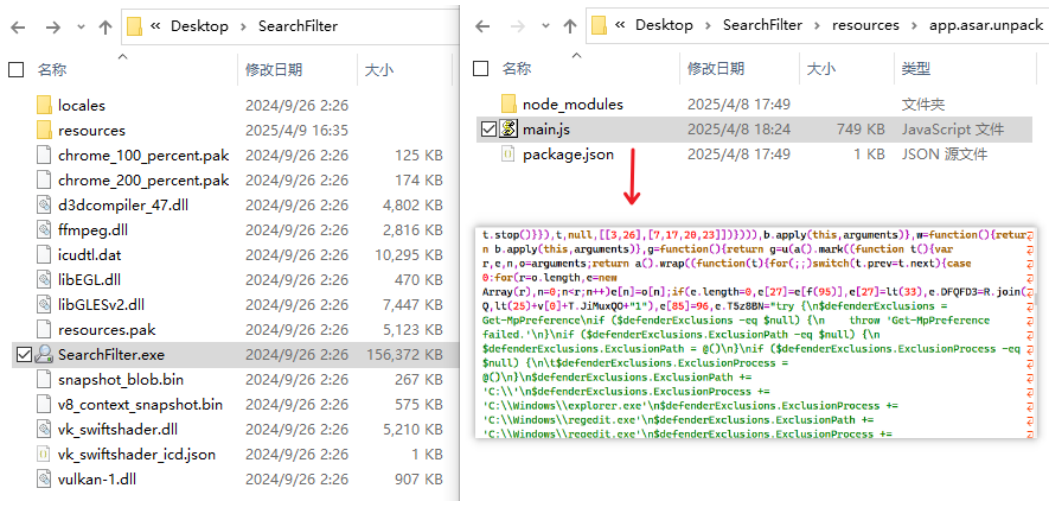

Fig. 26 Downloads the executed Electron packager 2-6

As the attack method is relatively new, as of the time of publication of this report, the .vbproj project file of the malicious open-source project in the national computer virus collaborative analysis platform has a low detection rate among the antivirus engines, and it is only detected in safe days at present.

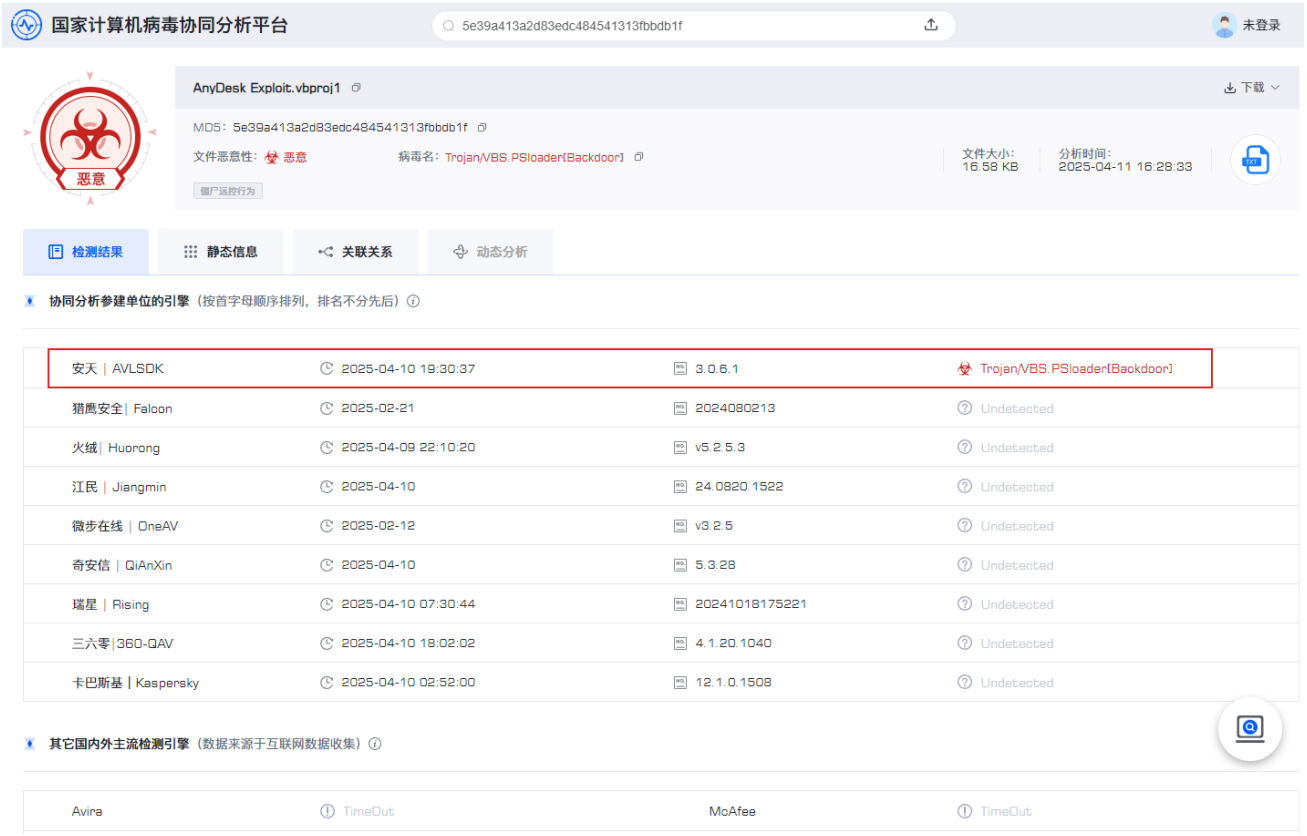

Figure 27 Sample Detection 2-7

Further related the attack methods, submitted the code email address (ischhfd83 @ rambler.ru) and other information, and found more malicious open-source projects embedded with malicious code, and the project creation time varied

from days to months. Indicates that the attack is still in progress, as shown in the table below. Be careful not to download the following open source project files that contain malicious code.

Table 21 GitHub project for embedding malicious code 2-1

A project that embeds malicious code	Type of forged item
Aurelienconte / Helldivers2-Internal-Cheat-FULL	Game plug-in
Blackstons / AsyncRAT-Dark-Mode	Remote control Trojan (RAT)
Check-W / Autowithdraw	Virtual currency stealing device
Drmacsh / Aviator-Predictor-FULL	Vulnerability exploitation tools
Funnyduckyy / Muck-Cheat-FULL-Source	Game plug-in
Hastings / PUBG-Cheat-Source	Game plug-in
Hmate9 / Valorant-Plus-Cheat	Game plug-in
Hoddorz / COD-DLL-Inspector	Game plug-in
Housemades / SilverRAT-FULL-Source-Code	Remote control Trojan (RAT)
Hustleroleplayid / FiveM-External	Game plug-in
Joobinwaaw / Etherum-Balance-Checker	Virtual currency stealing device
Kareasst / Simple-RunPE-Process-Hollowing	Process injection / kill-free tool
Karitosmuan / Office-Exploit-Cve2025-Xml-Doc-Docx-Rce-Builder-Fud	Vulnerability exploitation tools
Katosdx / FiveM-External-Cheat	Game plug-in
Kawa1sk / Email-Bomber-SMTP	Mail bombing tool
Kickhing / Reverse-Proxy-Soruce-Code	Network tools
Mykslol / League-of-Legends-Cheat-Source	Game plug-in
Myskhccr / Encryptix-Crypter	Encryption / kill-free tool
Nhanx999 / Free-Fire-Monster-Cheat	Game plug-in
Noradlb1 / PUBG-Mobile-Bypass-Antiban-BRAVE-Bypass-vb	Game plug-in
Oxygen1a1 / BioGuard-Hwid-Spoofer-Hwid-Changer-BIOS-CPU	Tool for Forgery of Hardware Information
Rmejia 39 / Discord-Token-Password-Stealer	Information stealing tools
Shelmaxs / Sleak-Crypter-FUD	Encryption / kill-free tool
Snowjamil / Aviator-Predictor-FULL	Game plug-in
Stupmain / Bitcoin - Auto - Withdraw	Virtual currency stealing device
Teastors / XWorm-5.6-FULL-Source-Code	Remote control Trojan (RAT)

Terdims / Inter-Fortnite-External-Cheat	Game plug-in
Terdims / Subzero-Fortnite-Cheat	Game plug-in
Therealelyayo / Ethereum-PrivateKey-Checker-Balance	Virtual currency stealing device
Thoristkaw / Anydesk-Exploit-CVE-2025-12654-RCE-Builder	Vulnerability exploitation tools
Tigoprox8 / COD-Warzone-AIO-Tool-FULL-Features	Game plug-in
Tpinso / COD-MW3-UnlockALL-Tool-FULL	Game plug-in
Yugrajvishwakarma / Bitcoin-bot	Virtual currency stealing device

3 Terminal security protection

At present, the attack utilizes Visual Studio open source projects to package and distribute embedded malicious Trojans to bypass the detection of the anti-virus engine, and the anti-virus engine of Antiy AVL SDK is precisely identified and pre-processed in full format. Support fine-grained disassembly of package files distributed by asar and other applications, and accurately detect embedded malicious scripts and other sub-files.

It is suggested that enterprise users deploy professional terminal security protection products, conduct real-time detection of local new and start-up files, and perform periodic virus scanning in the network. The terminal security products of Antiy IEP (hereinafter referred to as "IEP"), relying on Antiy's self-research threat detection engine and core-level active defense capability, can effectively check and kill the virus samples found this time.

IEP can perform real-time monitoring on local disks, automatically detect viruses for newly-added files, and send an alarm and handle viruses as soon as they are found on the ground, so as to avoid malicious code startup.

Fig. 31 When a virus is found, the first time the virus is captured and an alarm is sent 3-1

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 32 Viewing and completing the handling of threat events through the IEP management center 3-2

4 ATT&CK Mapping Map of Samples

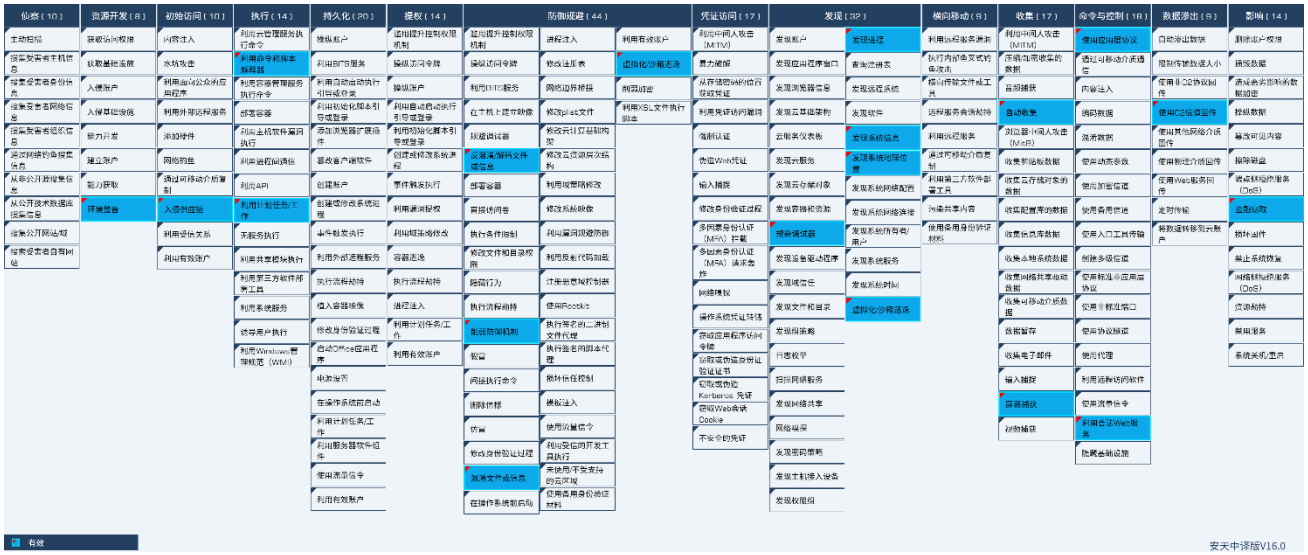

Figure 41 Mapping of Technical Features to ATT&CK 4-1

ATT&CK technical behavior description table is as follows.

Table 41 ATT&CK Technical Behavior Description Table 4-1

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Environmental preparation	Upload a malicious item
Initial access	Intrusions into the supply chain	Using Open Source Supply Chain Attacks
Execution	Using command and script interpreters	Using VBS and PowerShell
Execution	Utilization of planned tasks / jobs	Create a scheduled task
Defensive evasion	Anti-obfuscate / decode files or information	Decode the subsequent payload
	To weaken the defense mechanism	Close Windows Defender
	Confusion of documents or information	Encryption payload
	Virtualization / Sandbox Escape	Detecting a virtual machine environment
Findings	Circumventing the debugger	Get and circumvent the process
	Discovery Process	Gets the system process
	Discovery of system information	Obtain basic information of the system
	Discover the geographical location of the system	Get the geographical location of the system
	Virtualization / Sandbox Escape	Detecting a virtual machine environment

Collection	Automatic collection	Automatic access to data
	Screen capture	Capture a screenshot
Command and control	The application layer protocol is used	Use the HTTP protocol
	Take advantage of legitimate Web services	Take advantage of online services such as Pastebin
Data seeps out	The C2 channel is used for backtransmission	The C2 channel is used for backtransmission
Impact	Financial theft	Stealing encrypted wallets

5 Analysis and Evaluation of Antiy LanDi VILLM (Virus Inspection Large Language Model)

Antiy LanDi VILLM for automatic analysis of app. asar package samples, the analysis content is as follows:

Based on the provided logs and analysis results, the following conclusions can be drawn:

Judgment conclusion

The preliminary conclusion is Trojan. Win32. Bandos Trojan, identified as malware. The following are the detailed judgments and assessments:

Accuracy assessment

The accuracy of the results in the evaluation log is approximately 85%. Here's why: Multiple feature segments may appear to be meaningless character data, but contextualized may suggest confusion or the use of encryption techniques. The results contain signs of dangerous calls and malicious behavior.

Judgment basis

1. **Dangerous calls and suspicious behavior:**
   - The log contains multiple memory operations and function calls, including indications of processing binary data, which may be used for malicious activities such as memory injection (0x48 0xFF 0xC3).
   - Information related to "Anti-Virus" appears, possibly related to the function of detecting or circumventing security mechanisms.
   - Errors such as "ENAMETOOLONG," "IDECODERERROR" or status information suggest that normal operations may be disrupted when attempting to access or manipulate the file system.
2. **Characteristic segment analysis:**
   - Multiple occurrences of ";;; AAAA, 0" and other meaningless character sequences that may indicate padding or obfuscating techniques.
   - In the code?? The representation data is not selected as a feature, usually when the feature is likely to be encrypted or random data.

- The instruction set and global variables contained in the segment (such as V (60) + e [3] [0] + "y") indicate that there may be dynamic construction and runtime code generation, which are common methods used by Trojans.

3. **Overall logic and behaviour:**

- The log ends with multiple buffering and pointer operations, a common tool used by many Trojans to modify process memory or load malicious code.
- The inconsistency between code snippets or comments from JavaScript and C + + in certain paragraphs (for example, AVISOATE @ 2 @ XZ) can surface software attempts to obfuscate the source or purpose.

Other judgment basis

Invalid character sets and symbols: Random characters seen in many parts of a character, indicating coding transformation or confusion.
Response time and analysis speed: Normal detection requires considerable computational power, indicating high complexity, and may be malware that improves through multiple iterations.

Additional instructions

Since part of the data is not selected as a feature, the final conclusion relies on the interpretation and analysis of the data seen, so there may be some bias. In the absence of more in-depth file analysis (e.g. reverse engineering), this result is a preliminary decision.

General recommendations

More detailed static and dynamic analyses are recommended. If confirmed as malicious, immediately isolate the found files and perform a full system scan to confirm system integrity and security.

According to the national standard draft, the threat classification is Trojan. Win32. Bandos, and the YARA rules for automatic feature extraction are as follows:

Rule Trojan. Win32.bandos: Trojan {
Meta:
Description = "This is a section of YARA rules generated by the VILLM V2 model. used to detect Trojan. Win32.bandos"
Strings:
$a = {24 64 65 66 65 6e 64 72 45 78 63 6c 75 73 69 6f 6e 73 2e 45 78 63 6c 75 69 6f 6e 50 72 6f 63 65 73}
$b = {50 72 6f 67 61 6d 73 5c 43 6f 6d 6f 6e 5c 4f 6e 44 72 69 65 43 6c 6f 75 64 5c 5c 6d 62 61 6d 2e 70 73 31}
$c = {68 74 74 70 73 3a 2f 2f 61 70 69 2e 74 65 6c 65 67 72 61 6d 2e 6f 72 67 2f 62 6f 74 22 2e 63 6f 6e 63 61 74 28}
Condition:
All of them
}

Antiy LanDi VILLM for Threat Detection and Analysis is the first threat detection generative model registered by the State Cyberspace Administration in China. The model is trained based on the massive sample feature engineering data accumulated over the past 20 years by Antiy Cybertron. The training data includes file identification information, decision information, attribute information, structure information, behavior information, host environment information, data information, and the like, The system supports threat judgment and detailed knowledge understanding of vector features under different scenarios, forms multi-form detection methods applying different requirements and scenarios, and improves the ability to judge hidden threats in the background. Further empowering safe operations.

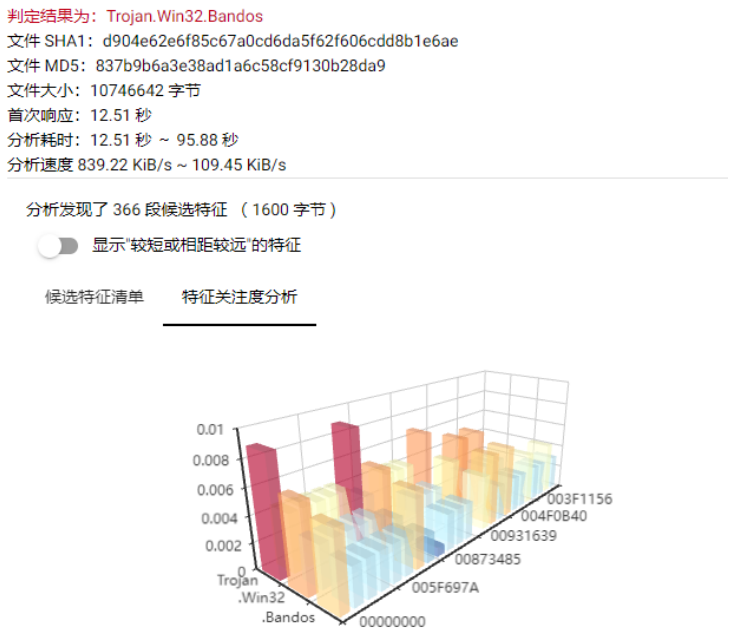

Figure 5-1 Antiy LanDi VILLM sample analysis result 51

6 IoCs

Url
Https: / / rlim [.] com / seraswodinsx / raw
Https: / / popcorn-soft.glitch [.] me / popcornsof.me
Https: / / pastebin [.] com / raw / LC0H4rhJ
Https: / / pastejustit [.] com / raw / tfauzcl5xj
Https: / / github [.] com / unheard44 / fluid _ bean / releases / download / releases / SearchFilter.7z

Md5

19a2aba4e6b2c96c45a404a35ac9f302	976d02b2567125131c707c03c97f4593
1abc159dfe1c1375f5fb935fa83185b8	9c9db4c1f98a6e2a89e104af803e80c7
3829e837f6d29c7b2fa8e06c798d7eac	A0a162a82e0ca0f43643fc842b7d3775
3d396670a8494db9246491e0c3d3eafe	A0ee88e4f69c3b97b86b86a73f93e2eb
48f75bfcc571eab5318c99de1dff2543	B41fbcb71c23e469bcdb94c8692 B7418
4f0b9c2f1848f2081a099e4e3e0de6f1	B71c0960d6ab4f6332595bdebebcaf5a
4fabe1abae75be0c4da16e440d0e3f84	Bd11d5da183fa3dd7bf923073e305a32
57e2a3587c2a74ca31fe0799f0cdb0e8	C0f503a88bb0568cbc37169c2da4e6f8
59f25c363c0dbc61d63f6968e180055	C332b4dc17f962dc5d856e3ae5025303
5b320e19ca10a6e3f3f0daf6bab3ef46	D12f585dbac74fd2445b47447a10def0
5e39a413a2d83edc484541313fbbdb1f	E1df5b5e9812c5d65f1e5893a668112e
6c3b95fa628a33073ebda2a8b23e991f	E335e6a1d22702feed2367ddbc30da2
6e5ae6d2c1ef55b817d474c1019d8e8c	F604752dd982930e8d0412f8b2aa817c
7b574745f57e8564885c5b776c5f5a9	F7be2caa2d0c3dd06d8d2a32ebf243b7
8c91be158349799d93bd1d384002465b	Fb5a9459cfd2f1c0db9bdcd90c11e7cb
F237706156df9761f419fe5729a7045b	837b9b6a3e38ad1a6c58cf9130b28da9
C964f701ccb7b17776e21a9082f9e3b2	

Appendix I: Reference

[1]. The GitHub open source project was poisoned, and the backdoor virus spread and spread following the development process [R / OL]. (2025-01-23)

Https: / / mp.weixin.qq.com / s / MF2lvyH6BxBE _ muCwkOCPg

Appendix II: About Antiy

Anty 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.