Analysis of the Criminal Gang that Delivers Remote Trojans by Cloud Note-taking Platform

Time of first release: 30 March, 2023

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

1 Overview

In the "Analysis of Attack Activities for Delivering Remote Trojans by Cloud Note-taking Platform," [1], an attack activity was introduced by Antiy CERT on March 24, 2023. Based on the PDB paths of multiple samples and information such as folder names hosted in the cloud note-taking platform, we linked the attack to the "Valley Robber" [2] (aka "Silver Fox" [3]) gang discovered by friends.[1][2][3]

By analyzing the related attack activities, the Antiy CERT team discovered that this criminal gang initially used phishing websites and social software to disseminate deceptive files, conducting a wide-scale phishing operation. In order to obtain greater economic benefits, this gang began to focus on delivering malicious programs to industries such as finance and securities this year. After obtaining control of the hosts of relevant industry employees, they pretended to be the victims and remotely operated the WeChat on the victim's host, using WeChat groups to spread the malicious program more widely.

To counter terminal security products, after the bait files distributed by this gang were executed, they mainly adopted three methods to load the next stage of malicious payloads: loading malicious DLL files using the "white plus black" approach, obtaining malicious files from public service platforms, and obtaining encrypted malicious files from the attacker's server. The gang released various remote control Trojans, including variants of Gh0st remote control Trojans modified, the "Xidu" remote control Trojan [4] and its variants, and Fatal remote control Trojan, etc. They used these remote control Trojans to gain control of the victim's host and remain on the host to achieve long-term control over the target.

It is proved that the Antiy IEP can effectively kill the remote control Trojan.

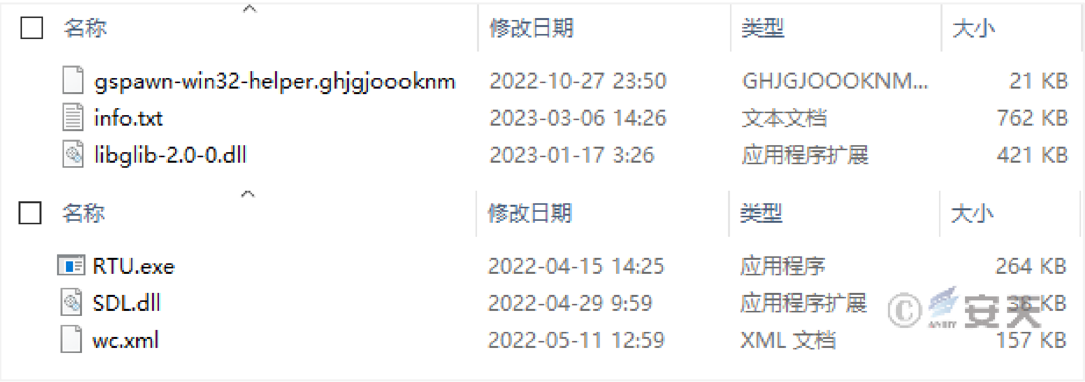
2 Correlation analysis

Based on the captured samples, we found that the gang hosted the malicious payload on multiple sharing links created, with the earliest date being January 21, 2022.

Table 2-1 Sharing links created by the gangs using cloud note-taking platform 1

User name	Folder name	Creation time	Sharing links
Quanshiyu 2022	Guduo	2022-1-21	Https [:] / note. * * .com / * * / index.html? Id = Cfae45c9e7cc8a7734b72abe98235dd1 & type = notebook & _ time = 1642761034339
Vip0418123000	Signed and genuine	2022-3-29	Https [:] / note. * * .com / * * / index.html? Id = F83f6c6da089d58ea8538c71344b8e64 & type = notebook & _ time = 1648556707433
Quanshiyu 2022	Xsd	2023-1-23	Https [:] / note. * * .com / * * / index.html? Id = 3865a47559efe2bcbe0fedf89106d323 & type = notebook & _ time = 1674487336507
Quanshiyu 2022	Xsd	2023-2-26	Https [:] / note. * * .com / * * / index.html? Id = 3865a47559efe2bcbe0fedf89106d323 & type = notebook & _ time = 1677420095103

The malicious payload hosted by the attacker is similar, the core of which is to load the DLL file of the first stage by the executable program in the malicious payload, to obtain and decrypt Shellcode and release the final remote control Trojan variant of Gh0st.

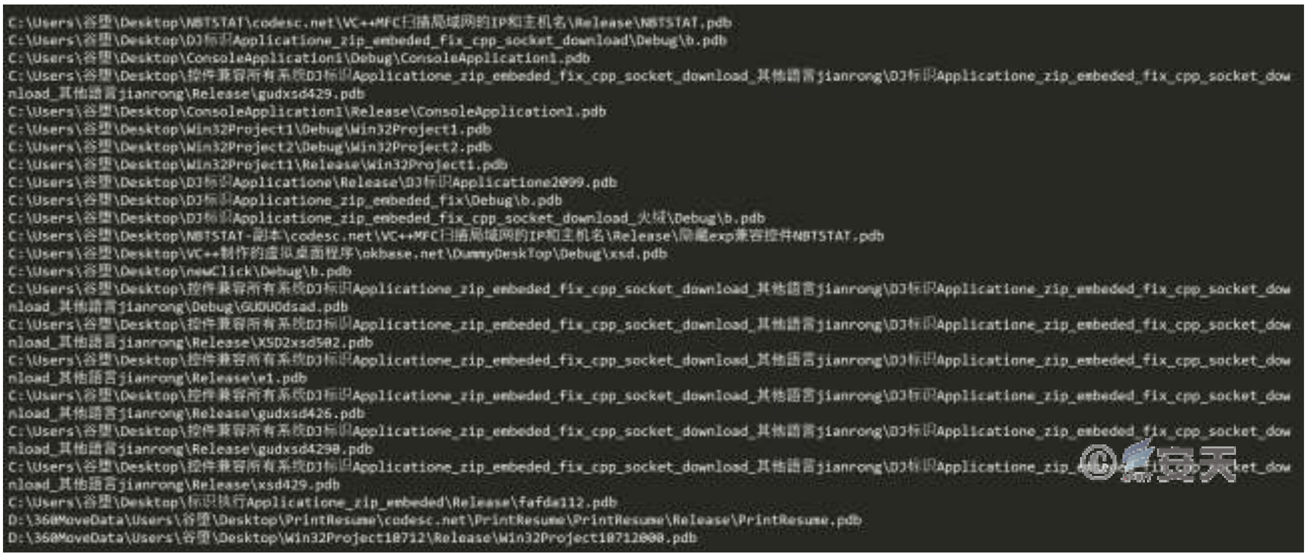


□ 名称	修改日期	类型	大小
gspawn-win32-helper.ghjgjoooknm	2022-10-27 23:50	GHJGJOOOKNM...	21 KB
info.txt	2023-03-06 14:26	文本文档	762 KB
libglib-2.0-0.dll	2023-01-17 3:26	应用程序扩展	421 KB

□ 名称	修改日期	类型	大小
RTU.exe	2022-04-15 14:25	应用程序	264 KB
SDL.dll	2022-04-29 9:59	应用程序扩展	38 KB
wc.xml	2022-05-11 12:59	XML 文档	157 KB

Figure 2-1 Partial malicious load 1

Based on the PDB paths of multiple samples and the names of folders hosted in the cloud note-taking platform, we linked the attack to the "Valley Robber" (aka the "Silver Fox") gang discovered by friends.



```
C:\Users\谷堕\Desktop\NBTSTAT\codesc.net\VC++MFC扫描局域网的IP和主机名\Release\NBTSTAT.pdb
C:\Users\谷堕\Desktop\DJ标识Applicatione_zip_embeded_fix_cpp_socket_download\Debug\b.pdb
C:\Users\谷堕\Desktop\ConsoleApplication1\Debug\ConsoleApplication1.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\gudxsd429.pdb
C:\Users\谷堕\Desktop\ConsoleApplication1\Release\ConsoleApplication1.pdb
C:\Users\谷堕\Desktop\Win32Project1\Debug\Win32Project1.pdb
C:\Users\谷堕\Desktop\Win32Project2\Debug\Win32Project2.pdb
C:\Users\谷堕\Desktop\Win32Project1\Release\Win32Project1.pdb
C:\Users\谷堕\Desktop\DJ标识Applicatione\Release\DJ标识Applicatione2009.pdb
C:\Users\谷堕\Desktop\DJ标识Applicatione_zip_embeded_fix\Debug\b.pdb
C:\Users\谷堕\Desktop\DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_火绒\Debug\b.pdb
C:\Users\谷堕\Desktop\NBTSTAT-副本\codesc.net\VC++MFC扫描局域网的IP和主机名\Release\隐藏exp兼容控件NBTSTAT.pdb
C:\Users\谷堕\Desktop\VC++制作的虚拟桌面程序\okbase.net\DummyDeskTop\Debug\xsd.pdb
C:\Users\谷堕\Desktop\newClick\Debug\b.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Debug\GUDUOdsad.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\XSD2xsd502.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\e1.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\gudxsd426.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\gudxsd4290.pdb
C:\Users\谷堕\Desktop\控件兼容所有系统DJ标识Applicatione_zip_embeded_fix_cpp_socket_download_其他語言jianrong\DJ标识Applicatione_zip_embeded_fix_cpp_socket_dow
nload_其他語言jianrong\Release\xsd429.pdb
C:\Users\谷堕\Desktop\标识执行Applicatione_zip_embeded\Release\fafda112.pdb
D:\360MoveData\Users\谷堕\Desktop\PrintResume\codesc.net\PrintResume\PrintResume\Release\PrintResume.pdb
D:\360MoveData\Users\谷堕\Desktop\Win32Project10712\Release\Win32Project10712000.pdb
```

Figure 2-2 Sample PDB Path Information2

3 The characteristics of the attack by the gang of "Valley Robber"

After combing the recent related attacks, we summarize the characteristics of the attacks currently used by the gang.

3.1 Mode of transmission

The gang used two main methods to disseminate the initial decoy documents:

1. The purchase of search engine keywords promotes phishing websites forged as download sites, thereby inducing users to download the execution bait files;
2. Using social software such as WeChat to send decoy files disguised as apps or documents.

After obtaining the control right of the lost host, the gang collects relevant information of the victim, and remotely operates the WeChat of the victim by pretending to be the identity of the victim, so as to further spread the malicious program.

3.2 How to load a malicious payload

In order to counter terminal security products, after the bait files distributed by this gang were executed, they mainly adopted three methods to load the next stage of malicious payloads: loading malicious DLL files using the "white plus black" approach, obtaining malicious files hosted on public service platforms, and obtaining encrypted malicious files from the attacker's server.

3.2.1 Loading malicious DLL files with "white plus black" method

After the decoy file runs, release a batch of files in the designated path, execute the normal executable program, load the malicious DLL file in the way of "white and black," decrypt Shellcode and load the final remote control Trojan.

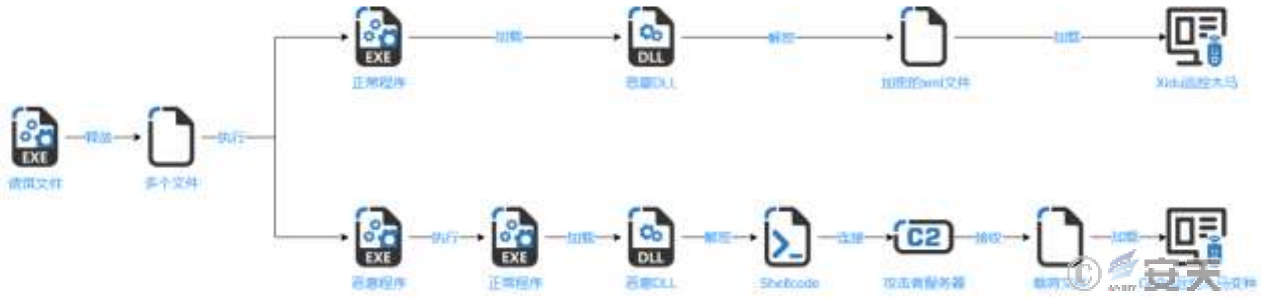


Figure 3-1 Loads a malicious payload in the manner of white plus black 31

3.2.2 Obtaining hosted malicious files from public service platforms

After the decoy file is run, the malicious file is obtained from the public service platform, thus loading the final remote control Trojan.

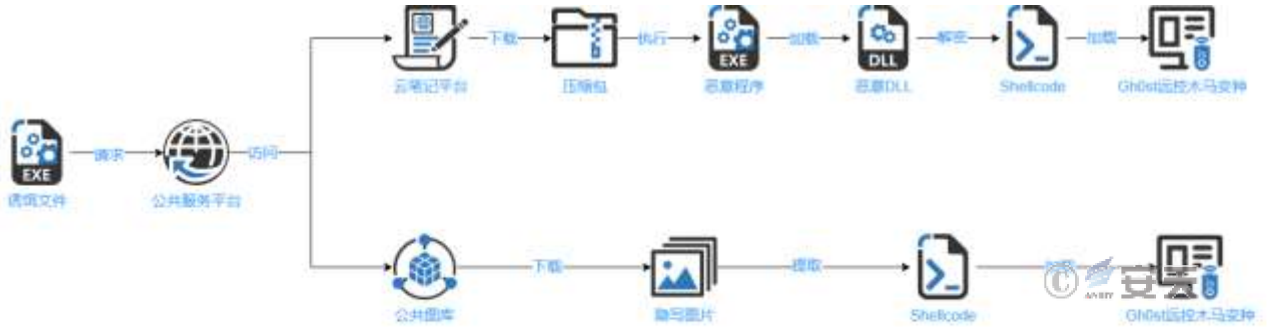
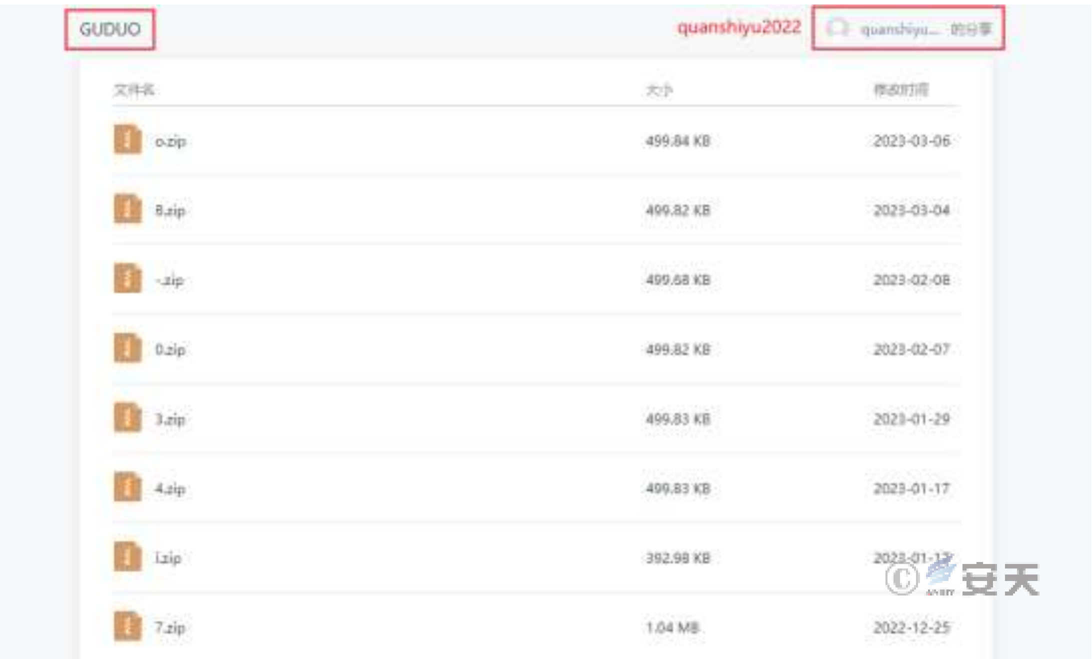


Figure 3-2 Acquisition of a malicious payload from a public service platform2

3.2.2.1 Hosting a malicious payload using a cloud note-taking platform

The gang hosted the malicious load in the form of compressed package files in the cloud note platform, and used the malicious program to load the malicious DLL files to decrypt Shellcode, and finally released the variant changed by the remote control Trojan based on Gh0st.



GUDUO

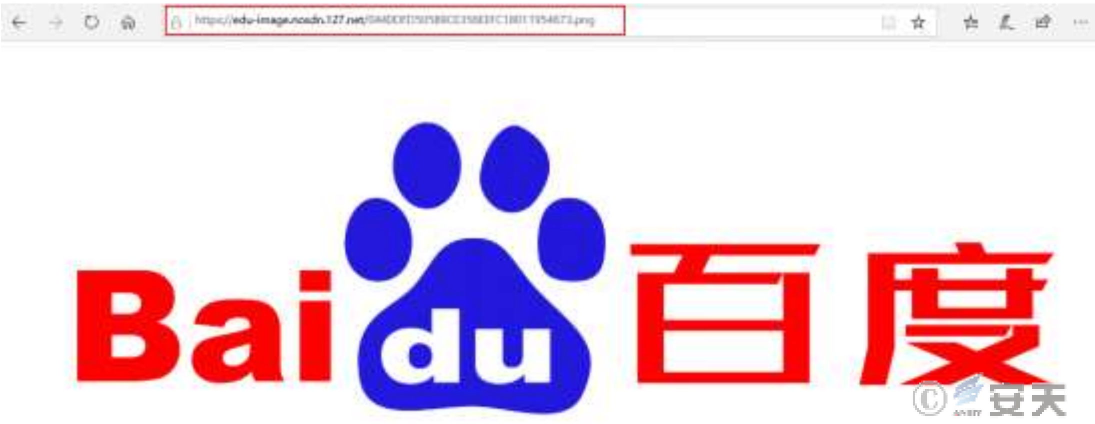
quanshiyu2022 quanshiyu... 的分享

文件名	大小	修改时间
o.zip	499.84 KB	2023-03-06
8.zip	499.82 KB	2023-03-04
-.zip	499.68 KB	2023-02-08
0.zip	499.82 KB	2023-02-07
3.zip	499.83 KB	2023-01-29
4.zip	499.83 KB	2023-01-17
l.zip	392.98 KB	2023-01-12
7.zip	1.04 MB	2022-12-25

Figure 3-3 Hosting a malicious payload using a cloud note-taking platform 3

3.2.2.2 Using a public file hosting service to host steganographic images

This criminal gang embedded the Shellcode into the image and uploaded it to the public image hosting platform where the images were stored. The bait file downloaded the image and decrypted it in memory, ultimately releasing the modified variant of the Gh0st remote control Trojan.



https://edu-image.nosdn.127.net/[illegible].png

Figure 3-4 Steganography using public service hosting4

3.2.3 Getting encrypted malicious files from an attacker's server

After the decoy file is run, an encrypted compression package or an encrypted file is obtained from the server controlled by the gang, and the encrypted file is decrypted by using a specified decompression password or a customized decryption method, thereby loading the final remote control trojan.

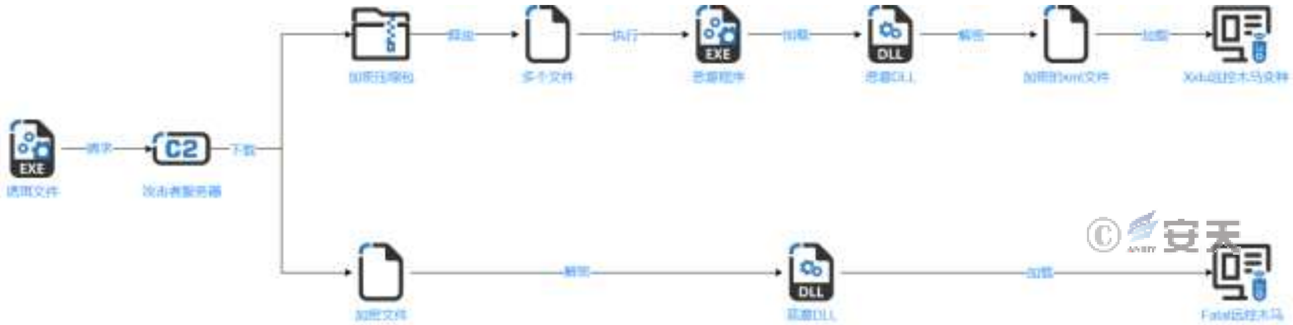


Figure 3-5 Retrieves the encrypted malicious payload from the attacker's server 5

3.3 Final malicious payload

By analyzing multiple batches of samples, we found that this criminal gang ultimately deployed various remote control Trojans, including modified variants of the Gh0st remote control Trojan, the "Xidu" remote control Trojan and its variants, the Fatal remote control Trojan, etc. These remote control Trojans all have malicious functions such as information data collection, keyboard recording, downloading and executing files, and remote control. The gang used multiple remote control Trojans to gain control of the victim's host and remained on the victim's host, thereby achieving lo

4 The effective defense of Antiy IEP

After discovering the attack behavior of this criminal gang, Antiy immediately initiated the response and conducted a verification of the defense capabilities of Antiy's terminal security product "IEP". After the test, it was found that IEP could effectively defend against the attack payloads utilized by the criminal gang in this incident. However, considering that the criminal gang might later develop variant viruses for a new round of attacks, it is recommended that IEP users upgrade their systems to the latest version.

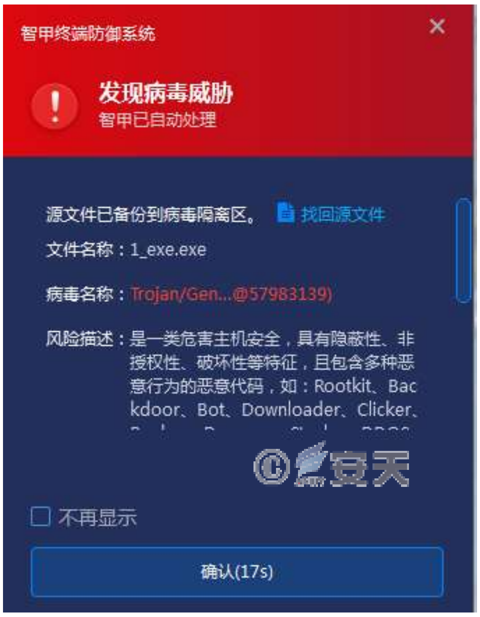
In this incident, IEP relied on the threat detection engine independently developed by Antiy, combined with three capabilities, to achieve the defense against the attack payloads:

1. Dual control mechanism for black and white, ensuring no blind spots in security protection.

Some terminal anti-virus products will allow programs that invoke signatures or white files by default. However, this mechanism can be exploited by attackers to achieve "kill-avoidance", such as in this incident, the attacker used the "white plus black" execution method to load malicious DLL files. Antiy IEP adopts a "black and white dual control" mechanism. It not only protects against black files but also regulates the sensitive behaviors of white files. In this incident, when IEP monitored the behavior of virus files that were started using system files, since the white file's startup object was an untrusted file, IEP still monitored and protected this behavior. Through the black and white dual control mechanism, IEP can effectively respond to the current "white plus black" attack method that attackers often use to evade detection and elimination.

2. Real-time protection, immediately curbing threats

IEP has core-level defense capabilities, which can immediately perceive and detect any actions of viruses such as execution, tampering, and destruction. It can intercept the attack before it takes effect, ensuring that the system and user data are not damaged. However, some security products, although having certain virus detection capabilities, do not possess core-level protection capabilities. Even if they can detect the virus, they cannot perform timely interception, and it is too late for users to notice when they do.



发现病毒威胁

智甲已自动处理

源文件已备份到病毒隔离区。 找回源文件

文件名称：1_exe.exe

病毒名称：Trojan/Gen...@57983139)

风险描述：是一类危害主机安全，具有隐蔽性、非授权性、破坏性等特征，且包含多种恶意行为的恶意代码，如：Rootkit、Backdoor、Bot、Downloader、Clicker、

Figure 4-1 Automatic interception of virus detected by Antiy IEP1

3. Memory anomaly detection, accurately detect and kill memory Trojan

Through virtualization technology, IEP can detect the rewriting behavior in the memory environment. For abnormal rewriting behaviors, it extracts the memory data features and uses the Antiy AVL-SDK threat detection engine for detection. Thus, through memory analysis, it can confirm the existence of malicious shellcode. In this incident, IEP effectively discovered the attacker's behavior of releasing remote control Trojan in the memory by using malicious images.

The Antiy IEP terminal defense system provides a unified management platform for security managers. Users can view the details of various security events that occur within the network on the management platform and can complete the handling of threat events in batches with one click.

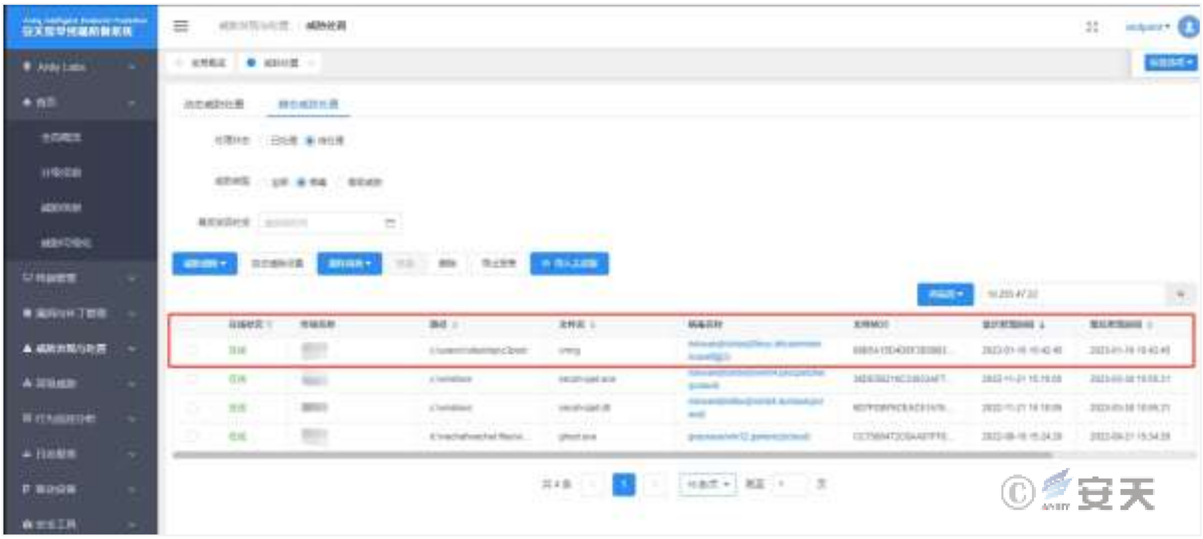


Figure 4-2 Management platform of IEP2

5 Summary

The "Valley Robber" (also known as "Silver Fox") criminal gang is currently updating the malicious functions of the bait files and remote control Trojans, purchasing phishing websites that masquerade as download sites by purchasing search engine keywords, and using social software groups to send malicious programs disguised as applications or documents.

We hereby suggest that users verify the official websites when downloading application software, and do not easily trust the advertising links promoted by search engines; do not easily open files in chat groups, forums, or emails that have not been security-checked. Currently, this criminal gang remains highly active, and Antiy will continue to monitor its subsequent activities.

Appendix I: Reference

[1]. Analysis of Attacking Activity of Remote Control Trojan with Cloud Note-writing Platform

Https: / / www.antiy.cn / research / notice & report / research _ report / 20230324.html

[2]. An Analysis of the Latest Sample of "The Valley Robber.

Https: / / mp.weixin.qq.com / s / sFKNKZy9HoArZLAuSNBIIQ

[3]. Watch out for the new black products "silver fox" large-scale social workers attack finance, government, enterprise, education and other industries

Https: / / mp.weixin.qq.com / s / DSA58emW0ZtGoyoEgufBJw

[4]. The backdoor virus uses "white plus black" to evade detection and kill users can control computers at will

Https: / / mp.weixin.qq.com / s / y0jLawhtJQBMoZNqUbXZCw

Appendix II: 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.