Analysis of Attack Activities Using Spam to Spread Remote Control Trojans

Antiy CERT

First draft completed: February 10, 2023
First published: February 13, 2023

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

1 Overview

Recently, the Harbin Institute of Technology and Antiy Joint CERT Labs has monitored multiple attacks using spam to spread remote control Trojans. Attackers send emails with themes such as "order", "invoice", "receipt", etc., and combine the body of the email to induce users to click on phishing links, thereby downloading and executing malicious files. Phishing links are sharing links generated by attackers uploading bait compressed files named "order.rar" , "electronic invoice.rar" , etc. to file sharing platforms. This method can achieve the effect of reducing their own operating costs, avoiding tracing, and bypassing whitelists.

The decoy compressed package contains three files, of which the .data file and the .exe file have the same name, usually "order" and "electronic invoice", and the file named "cl32.dll" is the core malicious file. The attacker uses the running mechanism of white and black to induce the target to execute the exe file to load the dll file. After running, cl32.dll decrypts and executes the core malicious dll in the memory to connect to C2 and download the communication module. The communication module is named "client.dll". After correlation and source tracing analysis, it is confirmed that the dll file is a "communication transmission framework" shared on a forum, which can realize multi-protocol communication and data interaction. It is speculated that it provides support for C2 connection in multi-protocol communication.

From the sample analysis, the sample is written in Easy Language. **Based on the existing analysis results, it is confirmed that the sample has the process and network behavior characteristics of a remote control Trojan and has some malicious functions**. Based on the characteristics of the relevant malicious samples and the sharing content of the communication module source forum, **the researchers speculate that this attack activity is the**

attacker's malicious use of tools and technologies shared on a forum to construct a remote control Trojan and spread it through spam. Comprehensive sample analysis and tracing results, combined with the attacker's use of technology and malicious intentions, researchers believe that once the user executes **the remote control Trojan spread by spam in this attack activity, the user's terminal will face remote control risks and data leakage risks.**

2 ATT&CK Mapping of This Attack Activity

The distribution diagram of technical features corresponding to this attack activity:

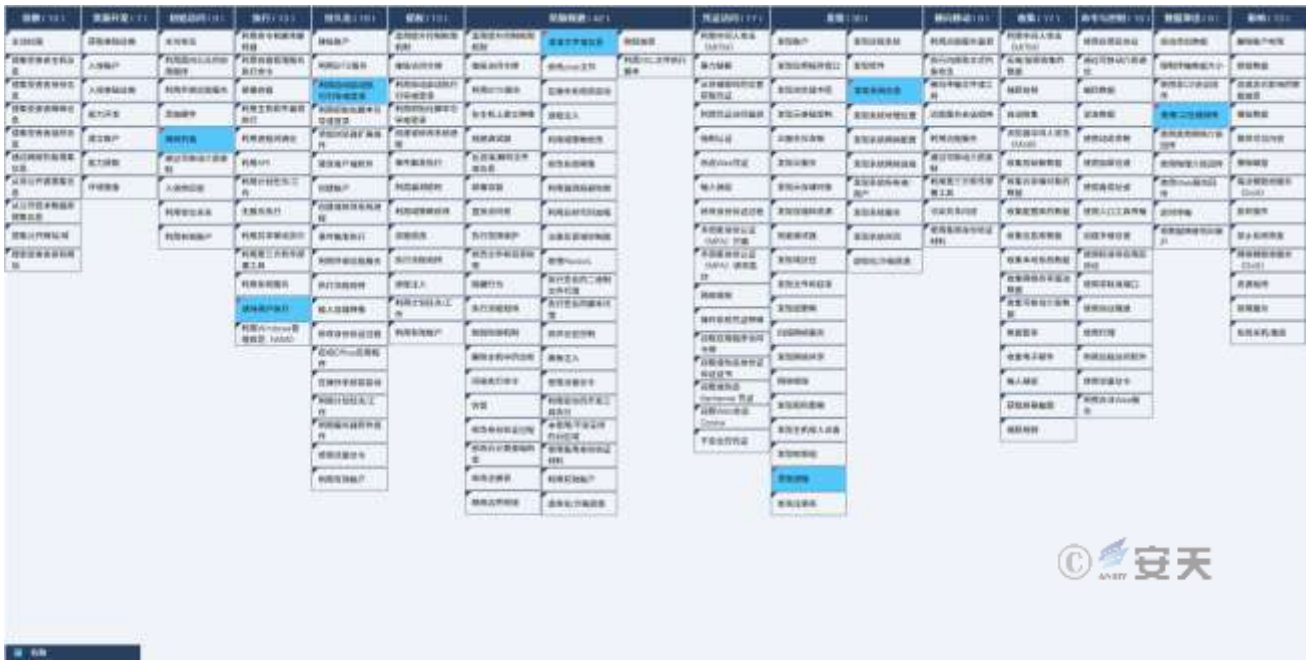

Figure 2-1 Mapping of technical features to ATT&CK

The specific ATT&CK technical behavior description is shown in Table 2-1.

Table 2-1 ATT&CK technical behavior description table corresponding to the event

ATT&CK Phase/Category	Specific Behavior	Notes
Initial Access	Phishing	Sending spam emails to spread remote control Trojans
Execute	Induce users to execute	Inducing users to execute in the name of "electronic invoice"
Persistence	Booting or logging in with autostart	Create a shortcut to the system startup directory
Defense Evasion	Obfuscating files or information	Encrypt dll files
Discover	Discovery Process	Detection of protection software processes
	Discover system information	Detect system version and other information

Data Exfiltration	Use C2 channel for backhaul	Connect C 2 and transmit data back

3 Protection Recommendations

In response to this remote control Trojan, Antiy recommends that government agencies and enterprises take the following protective measures:

3.1 Identify Phishing Emails

1. **View email senders:** Be wary of non-organized senders who send "business mail";
2. **View recipient address:** Be wary of mass emails and contact the sender to confirm;
3. **Check the delivery time:** Be wary of emails sent outside of working hours;
4. **View the email title:** Be wary of emails with titles containing keywords such as "order", "invoice", "wage subsidy", "purchase", etc.
5. **View the text wording:** Be wary of emails that begin with general greetings such as "Dear", "Dear User", "Dear Colleague", etc.
6. **View main text for purpose:** Be wary of emails that ask for email account passwords in the name of "system upgrade", "system maintenance", "security settings", etc.
7. **View the text content:** Be wary of web links included in them, especially short links;
8. **View the contents of attachments:** Before viewing, you must use anti-virus software to scan the attachments for viruses.

3.2 Daily Mailbox Security Protection

1. Install terminal protection software: Install terminal protection software, enable the scanning and detection function of email attachments in the protection software, perform security checks on the system regularly, and repair system vulnerabilities.
2. Email login password: When setting the email login password, ensure that it has a certain degree of complexity (including three character elements), ensure that the password is not recorded in a conspicuous place in the office area, and modify the login password regularly.

3. The email account must be bound to the mobile phone: After the email account is bound to the mobile phone, you can not only retrieve your password, but also receive SMS prompts of "abnormal login" and deal with it immediately.

4. Important files should be well protected:

   a) important emails that are no longer used in your inbox, outbox, and trash in a timely manner;

   b) loss after an attack;

   c) important emails or attachments should be sent encrypted, and the decryption password should not be included in the body of the email.

5. Protect sensitive information: Do not post sensitive information on the Internet. Information and data posted by users on the Internet can be collected by attackers. Attackers can analyze this information and data and send targeted phishing emails to users.

3.3 Protection for Government and Enterprise Organizations

1. Install terminal protection software: Install anti-virus software. It is recommended to install **Antiy Intelligent Endpoint Protection System**;

2. Improve password strength: Avoid using weak passwords. It is recommended to use a password of 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password on multiple servers.

3. Deploy intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracking of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large number of known malicious codes and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats;

4. Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

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

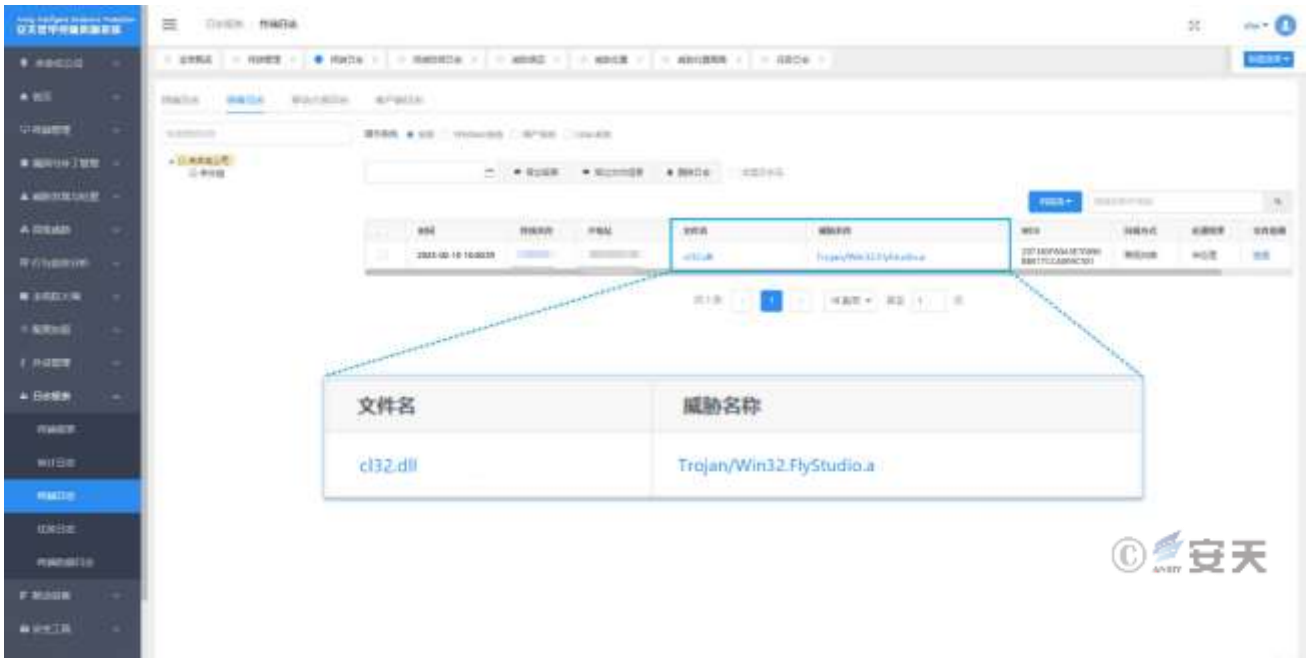

Figure 3-1Antiy IEP achieves effective protection for users

4 Email Analysis

Spam mainly uses subjects such as "order", "invoice", "receipt" and so on to construct the email body and embed phishing links in it, which exist in an implicit way (that is, the displayed link is inconsistent with the actual link), showing that after the link is accessed, it is indeed an invoice file.

Figure 4-1Spam email

Phishing links are mainly generated by document sharing platforms, such as "Kingsoft Documents", "NetEase Mailbox Master", "Lanzo Cloud Storage", etc. The bait compressed files are stored on multiple document sharing platforms, and corresponding links are generated. They are continuously sent to the target mailbox via spam emails, inducing the target to click and download the corresponding compressed files.

5 Sample Analysis

5.1 Analysis of the Decoy Compressed Package

The compressed package contains three files, namely "electronic invoice.exe", "electronic invoice.data", and " cl32.dll". Two of the executable programs have U PX shells. After analysis, it was verified that the files in the compressed package used the white-on-black technology to implement malicious code execution. The specific malicious file is cl32.dll.

Figure 5-1Decoy compressed file

5.2 Analysis of cl32.dll

5.2.1 Sample Tags

Table 5-1cl32.dll sample tags

Malicious code name	Trojan/Win32.FlyStudio.a
Original file name	cl32.dll
MD5	297180F60A3E70896BBE17CCA0E9C501
Processor architecture	Intel 386 or later processors and compatible processors
File size	640.50 KB (655,872 字节)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	2023-01-09 01:36:31

Digital signature	None
Packer type	UPX
Compiled language	Easy Language
VT first upload time	2023-02-06 03:52:36
VT test results	22 / 69

5.2.2 Dynamically Decrypt and Load Dll

c l32.dll is loaded, it decrypts and loads another dll file in memory, which is named "DLL.dll" below.

```
_____DLL.dll:02EB87F0 ; ---------------------------------------------------------------------
_____DLL.dll:02EB87F0 cmp     byte ptr [esp+8], 1
_____DLL.dll:02EB87F5 jnz     loc_2EB93DF
_____DLL.dll:02EB87FB pusha
_____DLL.dll:02EB87FC mov     esi, offset unk_2E70000
_____DLL.dll:02EB8801 lea     edi, [esi-9F000h]
_____DLL.dll:02EB8807 push    edi
_____DLL.dll:02EB8808 mov     ebp, esp
_____DLL.dll:02EB880A lea     ebx, [esp-3E80h]
_____DLL.dll:02EB8811 xor     eax, eax
_____DLL.dll:02EB8813
_____DLL.dll:02EB8813 loc_2EB8813:                           ; CODE XREF: _____DLL.dll:
_____DLL.dll:02EB8813 push    eax
_____DLL.dll:02EB8814 cmp     esp, ebx
_____DLL.dll:02EB8816 jnz     short loc_2EB8813
_____DLL.dll:02EB8818 inc     esi
_____DLL.dll:02EB8819 inc     esi
_____DLL.dll:02EB881A push    ebx
_____DLL.dll:02EB881B push    offset unk_E6B4A
_____DLL.dll:02EB8820 push    edi
_____DLL.dll:02EB8821 add     ebx, 4
_____DLL.dll:02EB8824 push    ebx
_____DLL.dll:02EB8825 push    offset unk_487E2
_____DLL.dll:02EB882A push    esi
_____DLL.dll:02EB882B add     ebx, 4
_____DLL.dll:02EB882E push    ebx
_____DLL.dll:02EB882F push    eax
_____DLL.dll:02EB8830 mov     dword ptr [ebx], 3
     DLL.dll:02EB8836 push    ebp
```


Figure 5-2Decrypting and loading the dll

5.2.3 Download Communication Module

Decrypting and loading the DLL.dll , it reads the .data file in the current directory and decrypts it in memory. The decrypted content is the C2 connection address and the communication module download address.

```
debug056:00B36C56 db    0
debug056:00B36C57 db    0
debug056:00B36C58 aOnline14313626 db '[online]',0Dh,0Ah   ; DATA XREF: Stack[00001248]:0019FCA8to
debug056:00B36C58 db '1=43.136 .  =6:12345|http://43.136 .  .6:8080/7X/client.dll',0Dh
debug056:00B36C58 db 0Ah
debug056:00B36C58 db 0Dh,0Ah
debug056:00B36C58 db '[config]',0Dh,0Ah
debug056:00B36C58 db 'time=2023'
debug056:00B36CB6 db 0C4h
debug056:00B36CB7 db 0EAh
debug056:00B36CB8 db  32h ; 2
```

Figure 5-3Decryption of C2 and communication module download address configuration information

Connect the U RL download communication module.

```
push    80000004h
push    0
push    offset aWinhttpWinhttp ; "WinHttp.WinHttpRequest.5.1"
push    10030h
push    0
mov     ebx, [ebp+var_4]
push    dword ptr [ebx]
push    3
```

Figure 5-4Download communication module

5.2.4 Process Behavior

After the communication module is downloaded, a child process is created with the newly copied exe file as the carrier, and the own process is terminated.

SGTool.exe	3104	3104	Sogou.com Inc.	搜狗输入法 工具
电子发票.exe	1844	1844		
K7497O839QD4LF3F65J877.e...	3208	1844		
GoogleUpdate.exe	472	472	Google LLC	Google 安装程序
GoogleCrashHandler.exe	1576	472	Google LLC	Google Crash Hand

Figure 5-5Process behavior

5.2.5 Persistence

After the program is run, a shortcut will be created and copied to the startup directory to achieve persistent operation.

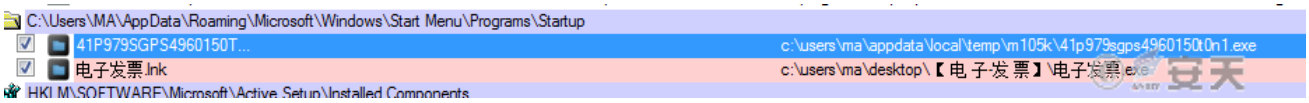

Figure 5-6Creating a shortcut in the startup directory

5.2.6 Connect C2 Address

After the communication module is downloaded successfully, it will connect to C2 and send an online packet.

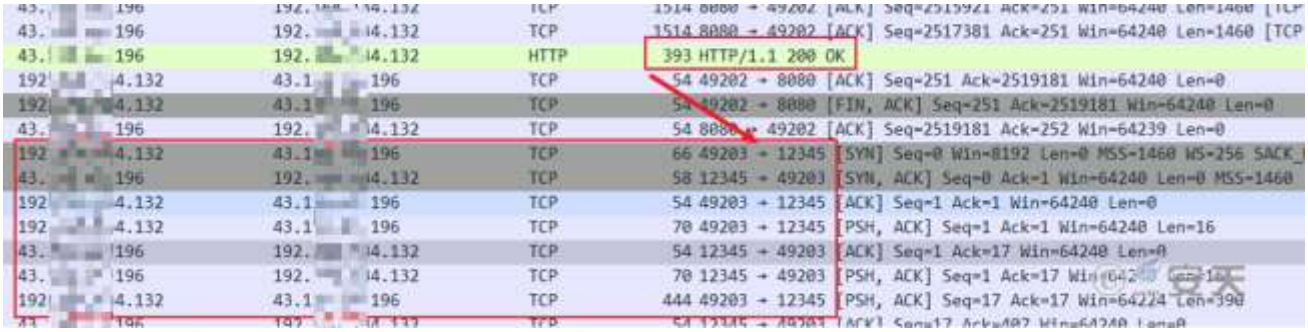

Figure 5-7Connect C2

The encrypted information is then continuously sent.

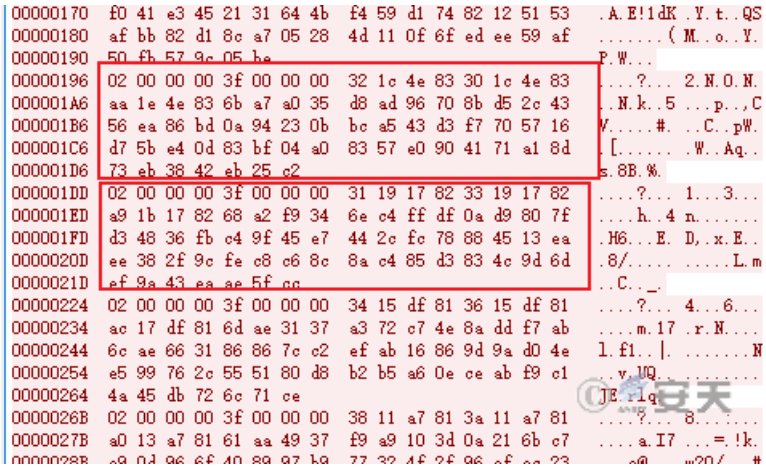

Figure 5-8Sending encrypted information

5.3 Analysis of client.dll

5.3.1 Sample Tags

Table 5-2client .dll sample tags

Malicious code name	Trojan/Win32.FlyStudio.a
Original file name	client.dll
MD5	77679E51504F2B94565B6E974D29FFFF
Processor architecture	Intel 386 or later processors and compatible processors
File size	2.40 MB (2,519,040 bytes)
File format	BinExecute /Microsoft.DLL[:X86]

Timestamp	2023-01-10 10:52:55
Digital signature	None
Packer type	None
Compiled language	Easy Language
VT first upload time	2023-01-16 15:36:15
VT test results	41 / 68

5.3.2 Communication Function

After analyzing the client.dll file, it was confirmed that the file was a communication transmission framework shared in a forum.

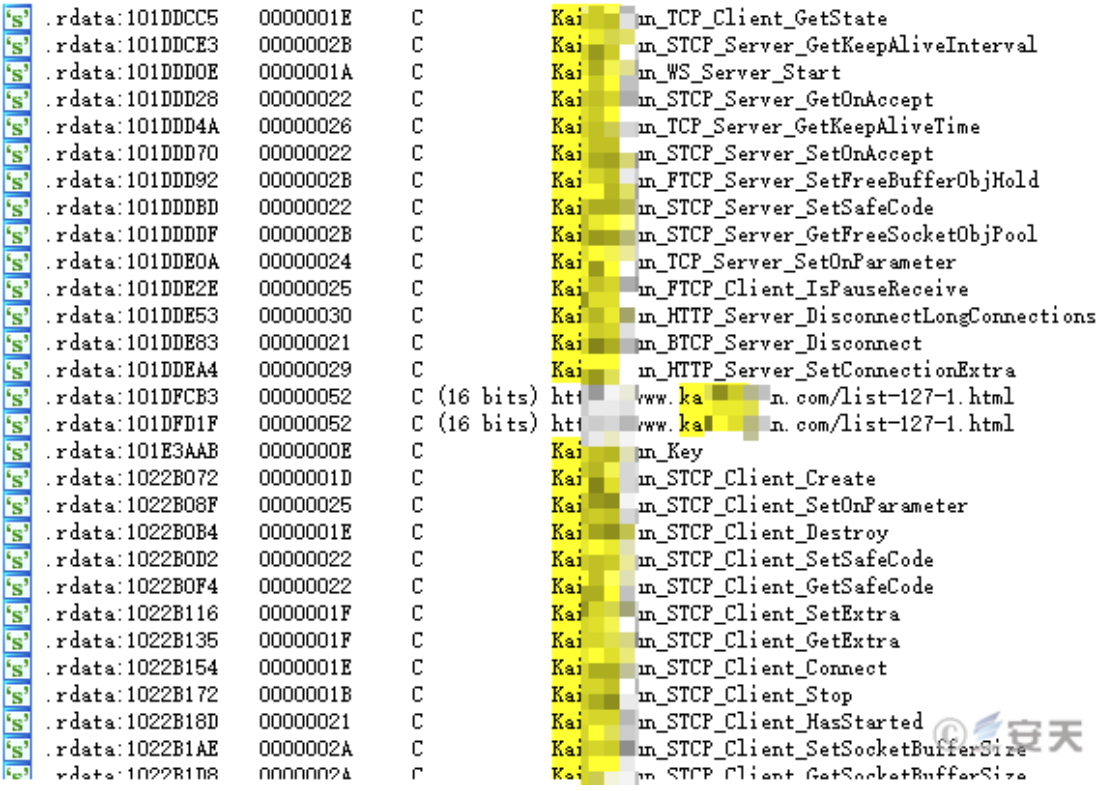

Figure 5-9Communication module

5.3.3 Terminal Protection Process Detection

The communication module also comes with a detection function for the core process of the target host terminal protection software.

Figure 5-10Terminal protection process detection

6 IoCs

5d561153af1589bd1d64556bddd257e0
297180f60a3e70896bbe17cca0e9c501
77679e51504f2b94565b6e974d29ffff
2f49e81d731dc4ed960e546a57b06f4a
6e47449010e84f52736fa9033820fdb6
43.**.**.196:12345
175.**.**.96:12345
150.**.**.22:12345
http[:]//27.**.**.194:8080/7X/client.dll
http[:]//43.**.**.80:8080/7X/client.dll
http[:]//192.**.**.60:8080/7X/client.dll
http[:]//134.**.**.215:8080/7X/client.dll
http[:]//43.**.**.85:8080/7X/client.dll
http[:]//47.**.**.161:8080/7X/client.dll
http[:]//43.**.**.194:8080/7X/client.dll

http[:]//43.**.**.8:8080/7X/client.dll
http[:]//150.**.**.22:8080/7X/client.dll
http[:]//43.**.**.196:8080/7X/client.dll
http[:]//175.**.**.96:8080/7X/client.dll
https://www.kdocs.cn/view/l/crE7FLdvYnGN
https://dashi.163.com/html/cloud-attachment-download/?key=djAycC8yc05PUU82cjV5ZUVPUG9QNzBWQT09
https://wwpb.lanzoue.com/ihvhc0mu6mvc

Appendix: 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.