Analysis of the Large-scale Attack Activities Launched by the "Swimming Snake" Cybercrime Gang against Domestic Users

Antiy CERT

Time of first release:18 May, 2023

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

1 Overview of the gang

The "Swimming Snake" criminal gang has been active since the second half of 2022 and launched a large number of attacks against domestic users. The gang spread malicious programs through various means such as phishing emails, fake electronic bill download sites, fake application download sites, and social networking software, etc. After the malicious programs are deployed, they obtain multiple payload files from the attacker's server and use the "white plus black" method to load malicious payloads by leveraging NetSarang series tools, Tencent game-related programs, etc. They create scheduled tasks using COM components and release and execute the Gh0st remote control Trojan variant after multiple layers of decoding. This criminal gang spreads malicious programs through various channels, launching a large number of attacks against domestic users within a short period of time, and frequently changing server addresses. The downloaded payload files have all been obfuscated to evade the detection of security products. Therefore, Antiy CERT named it "Swimming Snake".

Table 1-1 Overview of the criminal gang1

Overview of the gang	Description
Name of the gang	Swimming Snakes
Main modes of transmission	Phishing mail, fake electronic bill download site, fake application download site, social software
Time of occurrence and active time	Active since the second half of 2022
The targeting system	Windows

Main Technical Features	Using malicious downloader to obtain a payload file; The malicious load is loaded by means of "white plus black." Obtaining the C2 address by using the downloaded configuration file; Remote control by using the variant of Gh0st remote control Trojan.
Infrastructure	Malicious payload files are often hosted in directories such as "picuress / 2022," "picuress / 2023," "images" in their servers, and the frequency of changing server addresses is high.

Based on experience, the email protection module of Antiy Endpoint Detection and Response System (Antiyi EDR) can accurately identify phishing emails in this event; Antiy IEP can effectively detect and eliminate malicious software such as malicious downloaders and remote control Trojans.

2 Technical sorting of the gang

2.1 Mode of transmission

This criminal gang has recently been frequently spreading malicious programs through phishing emails. The subject lines of these emails are usually related to electronic invoices. The content of the phishing emails is as follows:

> 您于 xxxx 年 x 月 x 日开具的充值电子发票，票据信息如下：
>
> 开票日期：[日期]
>
> 发票金额：[金额]
>
> 发票代码：[代码]
>
> 发票号码：[号码]
>
> 发票明细 DUI

"The invoice details" is a hyperlink that leads to a fake electronic invoice download site created by the attacker. The compressed file provided for download on this website contains malicious programs.

Figure 2-1 A counterfeit bill download site1

In addition, this criminal gang also spreads malicious programs through various means such as fake application download sites and social software. After obtaining control of the victim's host, they further conduct remote control over the host, impersonate the victim and use social software to send the malicious program, thereby enabling the malicious program to spread more widely.

Table 2-1 Names of some phishing files 21

File name
这几笔错误的账单我圈出来了 你看看.zip
交易对接总额详细报表.rar
USDT 回款清单.exe
2023 年国务院税务总局最新政策计划.zip
下发明细.exe
出入款对接报表.rar
Telegram-zh_CN 官方中文语言包.exe
Letsvpn-latest 最新 vpn 客户端电脑版.zip
点击安装简体中文语言包.exe
Telegram_zh_CN.rar1.exe

The gang typically hosted malicious payload files under directories such as "picuress/2022," "picuress/2023," "images" in its servers, and changed server addresses more frequently.

Table 2-2: URLs for hosting malicious payloads22

URL
Http [:] / frp.freefrp.net / images
Http [:] / / info.0a305ffb2a1d41f6870eac02f9afce89.xyz / images
Http [:] / datacache.cloudservicesdevc.tk / picturess / 2023
Http [:] / imgcache.cloudservicesdevc.tk / picturess / 2023
Http [:] / nbs2012.novadector.xyz / picturess / 2023

2.2 Execution flow of malicious program

The malicious programs deployed by this criminal gang obtain multiple payload files from the attacker's server. The obtained payload files are mainly divided into two categories, and their loading methods and execution processes are also different.

2.2.1 Type I of the payload file

1. Execute malicious Shellcode using the update program (tu _ rt.exe) of the NetSarang family of tools;
2. Using COM components to create scheduled tasks masquerading as related services of applications such as Xunlei, in order to implement persistence mechanism;
3. After multiple layers of decoding, the Gh0st remote control Trojan variant is released and executed in memory. The content of the downloaded setting.ini file is read to obtain the C2 address, and then a connection is established with the C2 address to remotely control the victim host.

2.2.2 Type II of the payload file

1. The malicious program decodes the instruction to merge the two downloaded payload files into TASLoginBase.dll.
2. Execute TASLoginBase.dll by using Tencent game related program (TASLogin.exe);
3. After multiple layers of decoding, the Gh0st remote control Trojan variant is released and executed in memory. The content of the downloaded setting.ini file is read to obtain the C2 address, and then a connection is established with the C2 address to remotely control the victim host.

3 Sample analysis

3.1 Type I of the payload file

After the sample program runs, the DLL file is retrieved from the C2 server and loaded into memory for execution. The DLL file then downloads multiple payload files from the specified URL and executes the 25638. exe program.

Table 3-1 List of downloaded files 1

File name	Functions
%ProgramData%**setting.ini**	Save the address of the C2 server
%ProgramFiles(x86)%**25638\25638.exe**	Update Program for Series Tools of NetSarang Company
%ProgramFiles(x86)%**25638\25638.dat**	The attacker adds malicious Shellcode in the file "_ TUProj. dat," and executes malicious Shellcode using "white plus black.
%ProgramFiles(x86)%**25638\Media.xml**	The DLL file that lost its header, used to create the scheduled task
%ProgramFiles(x86)%**svchost\svchost.exe**	Identical program to 25638. exe
%ProgramFiles(x86)%**svchost\svchost.dat**	Identical file to 25638. dat
%ProgramFiles(x86)%**svchost\Media.xml**	The DLL file that lost its header, used to decode update.log
%ProgramFiles(x86)%**svchost\update.log**	After multi-layer decoding, the final payload is obtained

25638.exe (originally named tu_rt.exe) is an update program for the series of tools of NetSarang Company. It has a normal digital signature. After running, it will use the built-in password to parse the dat file with the same name in the same directory, and execute the "_TUProj.dat" file within it. Attackers take advantage of this feature, adding malicious code to the "_TUProj.dat" file and using the white-on-black technique to execute the malicious Shellcode.

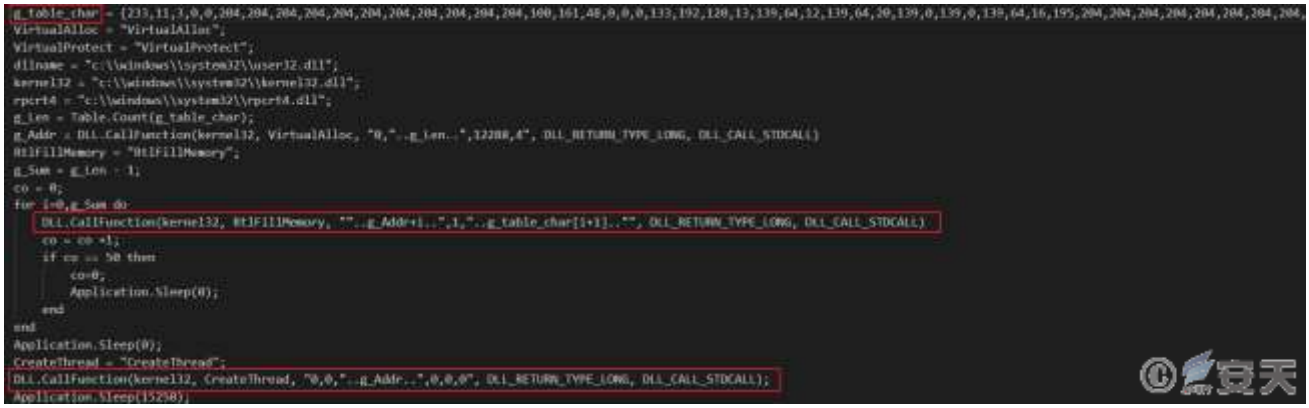

Figure 3-1 Execution of a malicious Shellcode 1

After the malicious Shellcode is executed, it reads the content of the Media.xml file in the same directory. It then restores the file header to that of a DLL file and loads it into memory for execution. The Media.xml files in the 25638 folder and the svchost folder are two different payload files. The former, after restoration, uses a COM component to create a scheduled task and disguises itself as a related service of Thunder; the latter, after restoration, reads the update.log file in the same directory, and after multiple layers of decoding, ultimately executes the Gh0st remote control Trojan variant.

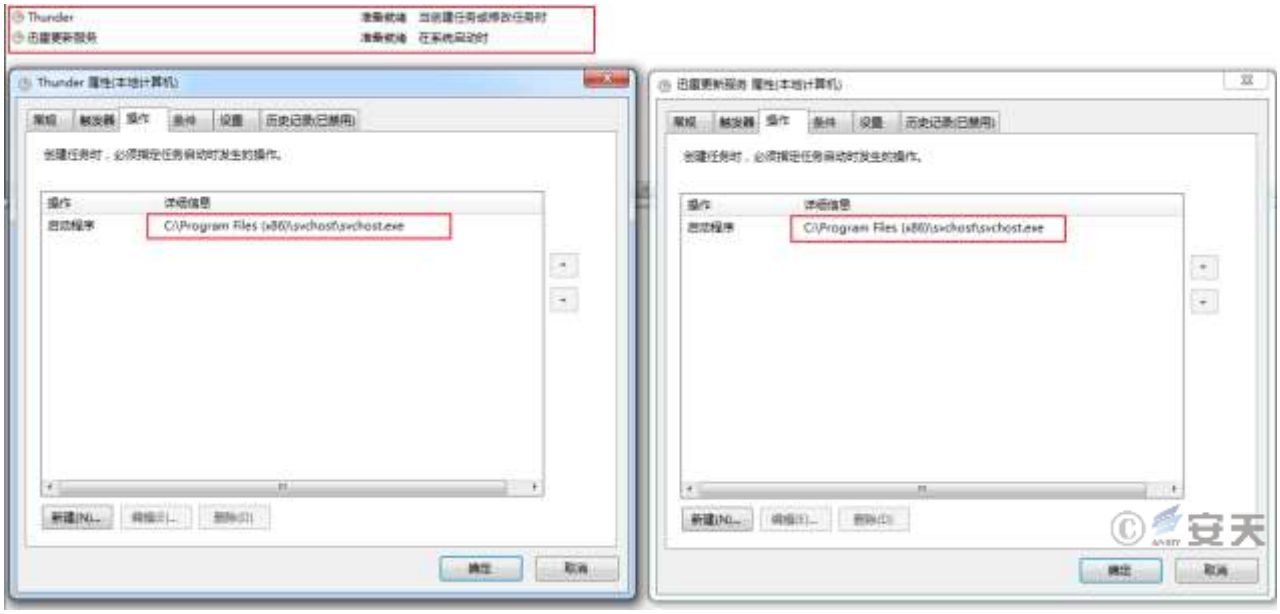

Figure 3-2 Creating a scheduled task using the COM component 2

3.2 Type II of the payload file

Some other malicious programs released by this gang will download another set of payload files.

Table 3-2 List of downloaded files2

File name	Functions
%ProgramData%**setting.ini**	Save the address of the C2 server
%Public%\Documents**update.lnk**	Shortcut to execute dllhosts.exe
%Public%\Documents**dllhosts.exe**	Tencent Game Related Programs
%Public%\Documents**MZ.txt**	After merging, it becomes a malicious TASLoginBase.dll file, and the malicious DLL is executed by using "white plus black.
%Public%\Documents**TAS.txt**	
%Public%\Documents**update.log**	After multi-layer decoding, the final payload is obtained

The malicious program decodes the instructions to merge the MZ.txt and TAS.txt files into the TASLoginBase.dll file. It then executes the dllhosts.exe program using the update.lnk shortcut. The original name of this program is TASLogin.exe and it has a digital signature, making it a normal program. The attacker loads the malicious TASLoginBase.dll file from the same directory using the "white plus black" method, reads the update.log file, and ultimately executes the Gh0st remote control Trojan variant.

Figure 3-3 Loads a malicious DLL file in the "white plus black" mode 3

3.3 Read the configuration file to get the C2 address

The Gh0st remote control Trojan variant used by the gang obtains the C2 address according to the downloaded% ProgramData%\ setting.ini file, so as to remote control the victim host.

```
dword_100F5778 = *((_DWORD *)v1 + 360);
dword_100F577C = *((_DWORD *)v1 + 361);
word_100F5816 = *((_WORD *)v1 + 799);
LOWORD(dword_100F5818) = *((_WORD *)v1 + 800);
CFile::CFile((CFile *)v43, aCProgramdataSe, 0);// C:/ProgramData/setting.ini
v3 = CFile::GetLength((CFile *)v43);
v4 = operator new(0x12Cu);
CFile::Read((CFile *)v43, v4, v3);
CFile::Close((CFile *)v43);
```


Figure 3-4 Read the setting.ini file to get the C2 address 4

4 Recommendations for protection

In order to effectively prevent such attacks and enhance the level of security protection, Antiy recommends the following protective measures to be taken by government and business organizations:

4.1 Identify phishing mail

1. Check the sender of the email: Be vigilant of emails sent by non-affiliated organizations with the same subject.
2. Check the recipient's address: Be cautious of mass emails. Contact the sender for confirmation.
3. Check the sending time: Be vigilant of emails sent outside working hours.
4. Check the email subject: Be cautious of emails with keywords such as "order", "bill", "wage subsidy", "purchase" in the subject.
5. Check the wording of the body: Be vigilant of emails with overly general greetings such as "Dear", "Dear User", "Dear Colleague".
6. Check the purpose of the body: Be cautious of emails asking for email account and password under the pretext of "system upgrade", "system maintenance", "security settings".
7. Check the content of the body: Be vigilant of web links attached, especially short links.
8. Check the content of the attachment: Before viewing, use anti-virus software to scan and detect viruses in the attachment.

4.2 Protection of website dissemination

1. It is recommended to use the genuine software downloaded from the official website. If there is no official website, it is suggested to download from a trusted source, and scan it with anti-virus software after downloading;

2. It is recommended to use the sandbox environment to execute suspicious files, and then use the host computer to execute the files with security. Based on the combination of deep static analysis and dynamic loading of sandbox, Antiy PTA can effectively detect, analyze and identify all kinds of known and unknown threats.

4.3 Government, enterprise and institutional protection

1. Install the endpoint protection software: Install the anti-virus software, and it is recommended to install the Antiy IEP;

2. Strengthen password strength: Avoid using weak passwords, and recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;

3. Deployment of Intrusion Detection System (IDS): Deployment of traffic monitoring software or equipment to facilitate the discovery, tracing and tracking of malware. Taking network traffic as the detection and analysis object, Antiy PTD can accurately detect a mass of known malware and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

4. Security service: In case of malware attack, it is suggested to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer; 7 * 24 service hotline: 400-840-9234.

Based on experience, the email protection module of Antiy Endpoint Detection and Response System (Antiyi EDR) can accurately identify this phishing email; the Antiy IEP can effectively detect and eliminate malicious downloaders and remote control Trojans and other malicious software, as well as provide practical protection for the user's terminal.

Figure 4-1 The EDR email protection module of Antiy IEP accurately identifies the phishing email - The Client1

Figure 4-2 The EDR email protection module of Antiy IEP accurately identifies the phishing email - Server

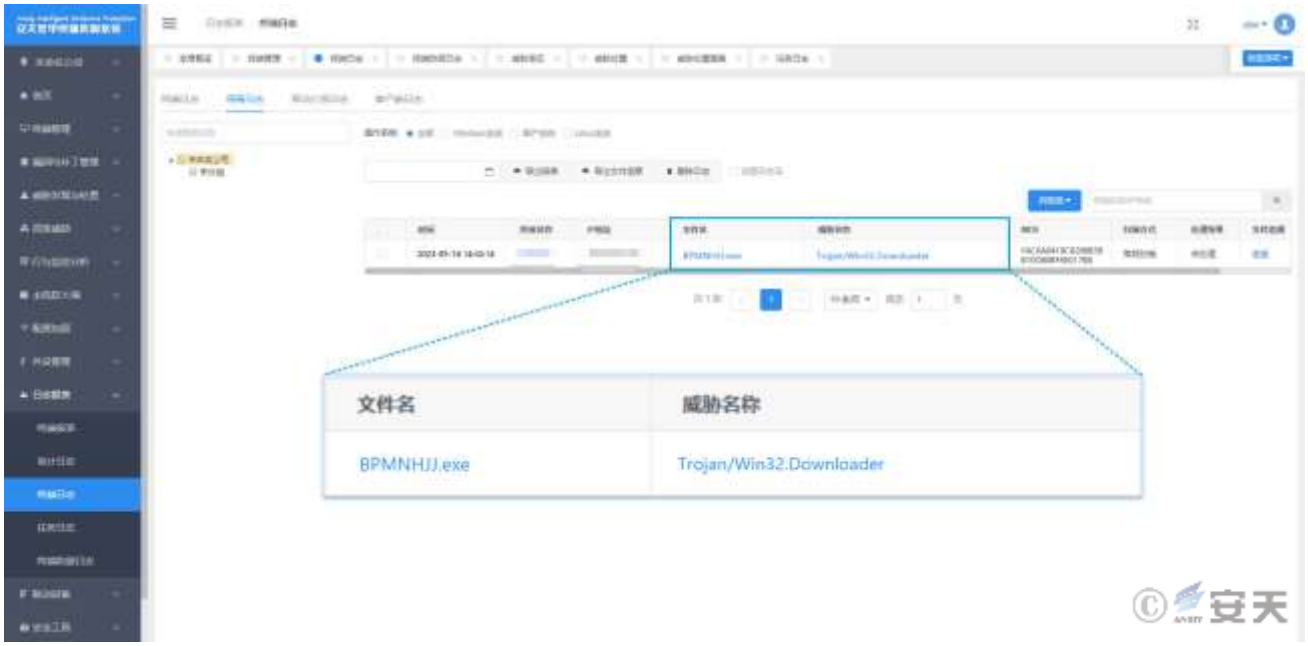

Figure 4-3 The effective protection of the user system implemented by Antiy IEP2

5 ATT&CK Mapping graph of the event

For the attacker to deliver the complete process of secret Trojan, Antiy combing the attack event corresponding to the ATT&CK mapping graph shown in the following figure.

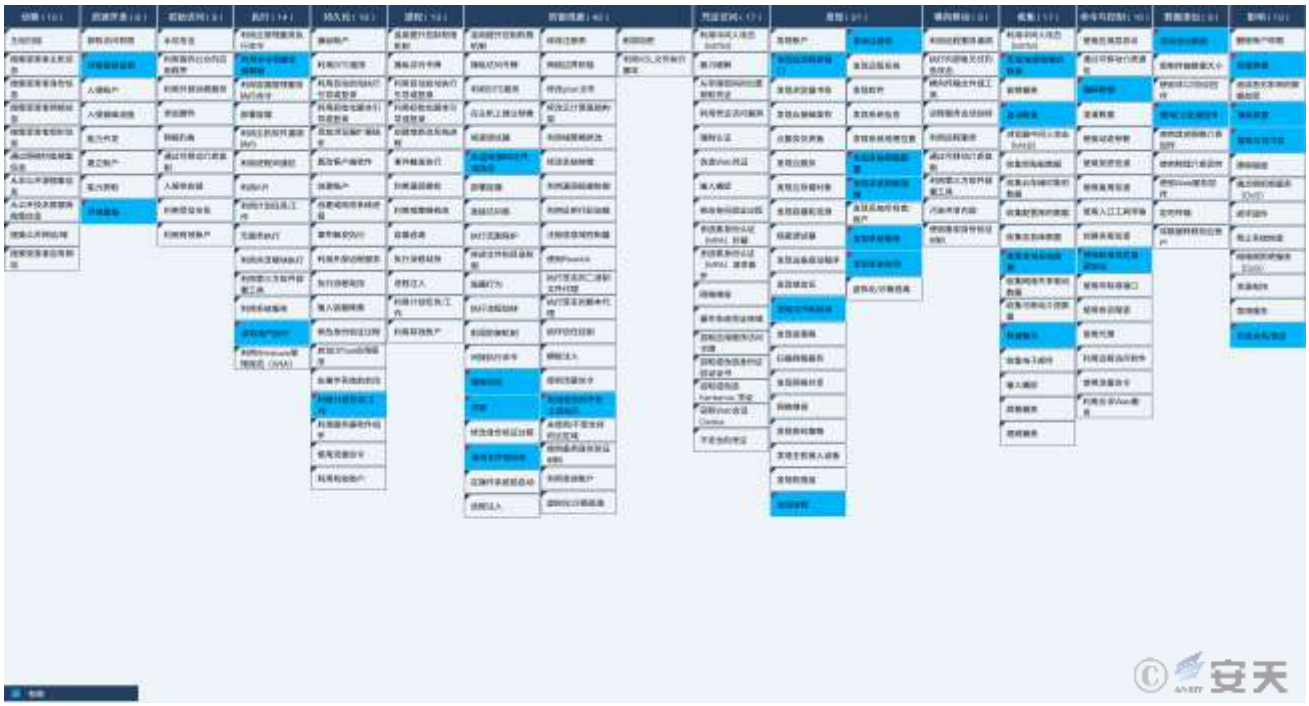

Figure 5-1 Mapping of Technical Features to ATT&CK 1

The technology points used by the attacker are shown in the table below.

Table 5-1 Description of ATT&CK technical behavior corresponding to the event 51

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Access to infrastructure	Gets the C2 server
	Environmental preparation	Managed malicious payload
Execution	Using command and script interpreters	Execute a program using commands and script files
	Inducing the user to execute	Use the phishing file to induce the user to execute
Persistence	Utilization of planned tasks / jobs	Create a scheduled task using a COM component
Defensive evasion	Anti-obfuscate / decode files or information	Decode payload information
	Remove beacons	Delete the downloaded payload file
	Counterfeit	Impersonating other applications
	Confusion of documents or information	Mix up load information
	Implement using a trusted development tool	"White plus black" mode to load malicious payload
Findings	Discover the application window	Discover the application window
	Find files and directories	Find files and directories
	Discovery Process	Traversal to find the security product process
	Query the registry	Query the registry
	Discovery system network configuration	Discovery system network configuration
	Discover the system network	Discover the system network connection

	connection	
	Discovery of system services	Discovery of system services
	System discovery time	System discovery time
Collection	To compress / encrypt the collected data	Encrypt the collected data
	Automatic collection	Automatic collection of host information
	Collect local system data	Collect local system data
	Temporary storage of data	Temporary storage of data
Command and control	Encoded data	Encoded data
	Standard non-application layer protocols are used	Use the TCP protocol
Data seeps out	Automatically seeps out data	Automatically seeps out data
	The C2 channel is used for backtransmission	The C2 channel is used for backtransmission
Impact	Damage data	Delete the specified data
	Manipulation of data	Manipulation of data
	Tampering with the visible content	Tampering with the visible content
	System shutdown / restart	System shutdown / restart

6 IoCs

IoCs
Fac6a0419c8288b58b1edb0bf6e017b8
9dbe476cafd45cc08ae2b1e6e5ed1739
9050ac019b4c8dddbc5e250bb87cf9f2
4ae5e8bdd68861df10f01fe268859588
3668799602e1e5b94bf893141b4b76e6
Aabd7d9de6c3c6fc4f639b8d664ae87c
8c4862a32095d0b71fcf8fb0b244161a

E22b83f968d67ec368d899246ff8cab7
6655b2bd93e70a2804e983b279ab473
Ac6ad5d9b99757c3a878f2d275ace198
B1b63759909a89f90f90f736cb35f188747
Efbb79c0088e0f0e41d42becbcf2ca87
8305b3aaa33fb9ca2e07e165b2030a33
Http [:] / frp.freefrp.net / images
Http [:] / / info.0a305ffb2a1d41f6870eac02f9afce89.xyz / images
Http [:] / datacache.cloudservicesdevc.tk / picturess / 2023
Http [:] / imgcache.cloudservicesdevc.tk / picturess / 2023
Http [:] / nbs2012.novadector.xyz / picturess / 2023
Http [:] / / luthj.sbs / home.html
Http [:] / swqe.sbs / home.html
Http [:] / / ajvloi.com / home.html
Http [:] / / mrty.sbs / home.html
Http [:] / iyhf.sbs / home.html
Http [:] / bhre.sbs / home.html
Http [:] / iyhf.sbs / home.html
Https [:] / / klianvpn.xyz
Http [:] / www.cuoso.vip
61.160.221.100
154.13.6.172
43.154.83.246
123.99.198.123
154.39.239.48
45.204.2.166

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.