Analysis of Clipboard Hijackers Spread via Pirated System Image Resources

Antiy CERT

Time of first release: 27 June

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

1 Overview

Recently, Antiy CERT has detected attacks propagating through mirror download stations. The attacker drops the Torrent resources into the image download station of the Windows operating system, and induces the user to install and use the seemingly pure system. In fact, an attack hides a malicious file in a specified path in advance, self-starts through a scheduled task, and finally executes a clipboard hijack to steal cryptocurrency.

The EFI system partition contains the operating system's boot loader and related files, which are generally invisible in Windows systems, and the files in the EFI partition are not normally scanned by security products. In this attack, the attacker uses the malicious software to mount the partition of the EFI system and copy the remaining malicious files into the partition to avoid detection by the security products.

The attacker can covertly implant the malware into the system, and then package it into a mirror file and put it into various download stations. Users should raise security awareness and avoid obtaining system mirror resources from unofficial channels, and there may be security risks in free resources that appear to be secure.

Table 1-1 Overview of attack activities 1-1

Overview of Attacks	Description
Main modes of transmission	Mirror Download Station
For the system	Windows operating system
Main Features	Using the system image to spread the malware; Using EFI System Partition to Evade the Detection of Security Products

It has been proved that Antiy IEP can effectively detect and kill malware.

2 Technical review

The attacker drops the Torrent resource into the system image download station, and induces the user to download and use the system image that has been tampered with maliciously. Such sites offer a large number of free images of the Windows operating system, with the potential for maliciously tampered images to be mixed in.

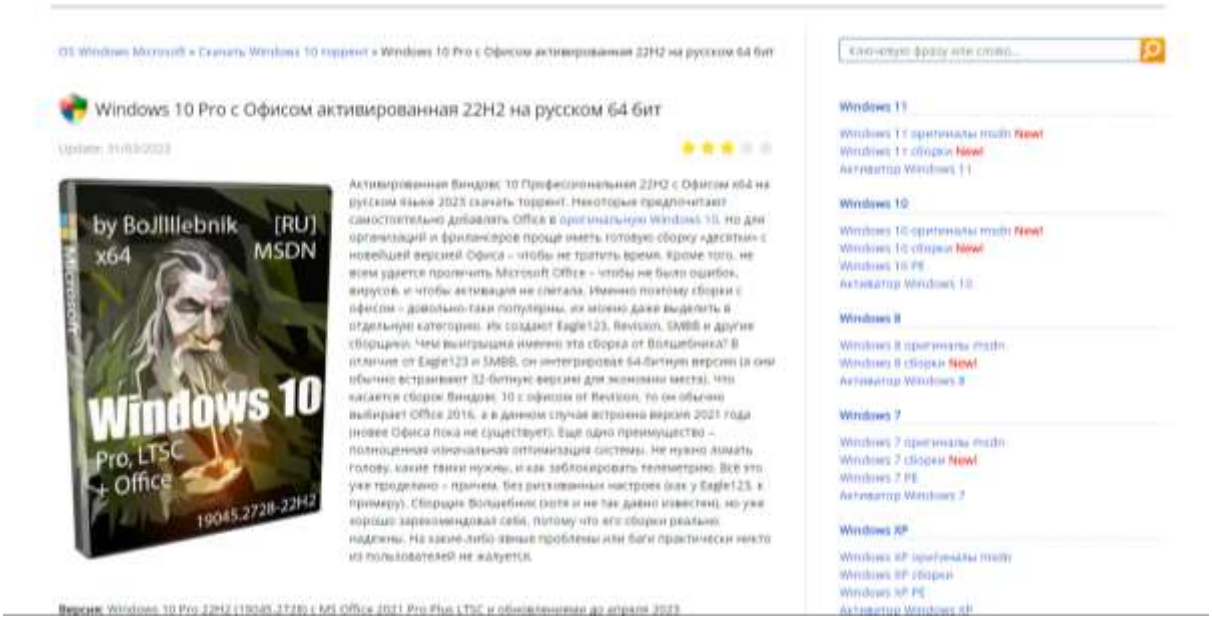

Figure 2-1 Attacker drops Torrent resources 2-1

The attacker previously placed the malicious program into% SystemRoot%\ Installer and created the corresponding scheduled task. After the user installs the Windows operating system with the maliciously tampered image, iscsicli. exe performs self-startup by scheduling tasks, mounts the EFI system partition and copies other malicious files into the partition. In order to avoid the detection of safety products. The malicious program eventually injects a malicious DLL that continuously monitors the contents of the clipboard and, when matched to the cryptocurrency wallet address, replaces it with the attacker's wallet address, thereby transferring the proceeds into the attacker's account.

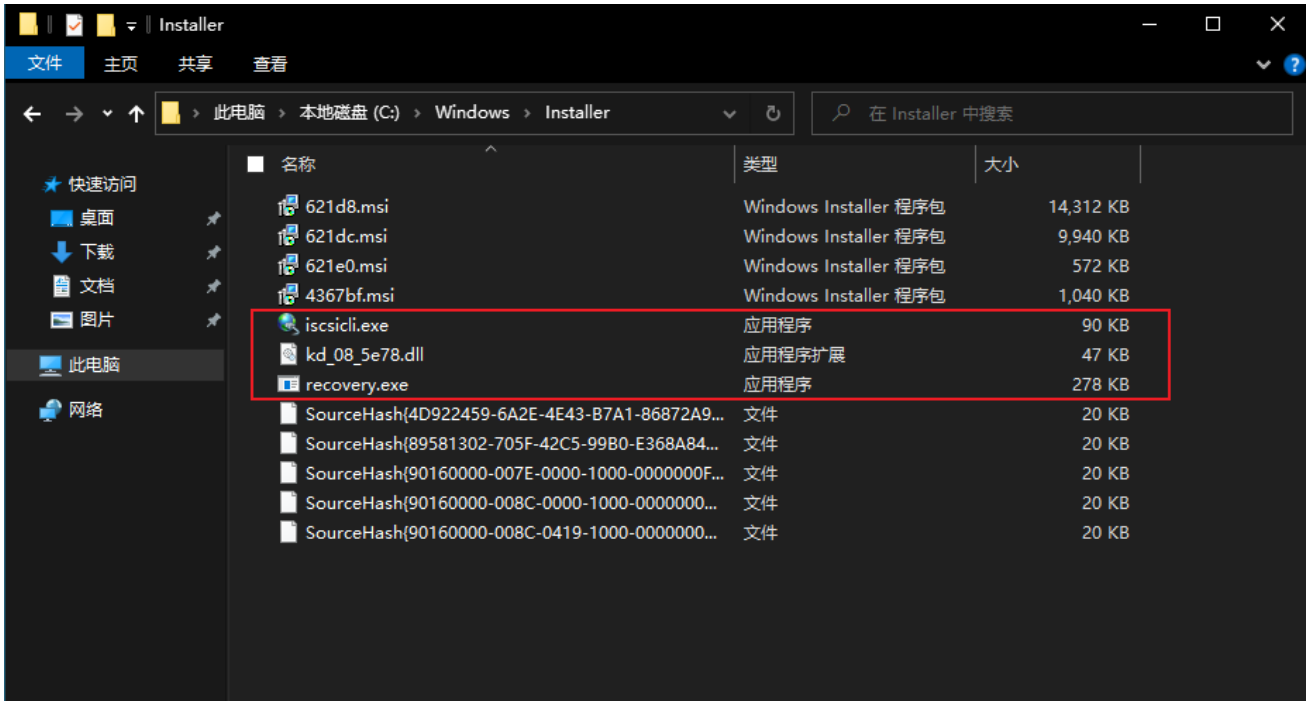

Figure 2-2 Malicious payload file 2

3 Sample analysis

3.1 Iscsicli.exe

The malicious program masquerades as a legitimate program in the operating system, and its digital signature is invalid.

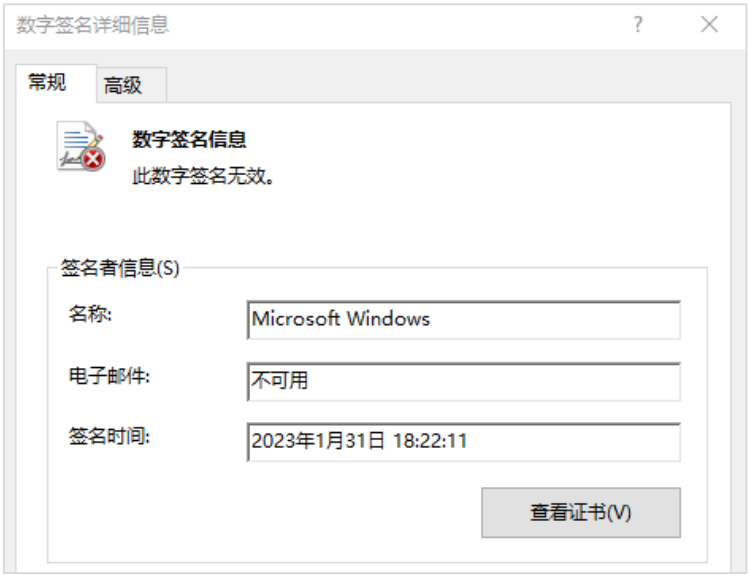

Figure 3-1 Invalid digital signatures 1

After the program runs, mount the EFI system partition in the M disk.

```
memcpy(v26, v23, v12);
strcpy((char *)v26 + v12, "\\System32\\cmd.exe /C mountvol M: /S");// C:\\Windows\\System32\\cmd.exe /C mountvol M: /S
*(_OWORD *)v96 = *(_OWORD *)Block;
v97 = v89;
v28 = (const char *)operator new(v89.m128i_i64[0] + 1);
v29 = v96;
v93 = Block[0];
v92 = _mm_srli_si128(v89, 8).m128i_u64[0];
if ( v92 >= 0x10 )
  v29 = (void **)Block[0];
v30 = v28 - (const char *)v29;
do
{
  v31 = *(_BYTE *)v29;
  *((_BYTE *)v29 + v30) = *(_BYTE *)v29;
  v29 = (void **)((char *)v29 + 1);
}
while ( v31 );
v32 = -1i64;
do
  ++v32;
while ( v28[v32] );
v33 = v32 + 1;
v34 = (wchar_t *)operator new(saturated_mul(v33, 2ui64));
mbstowcs(v34, v28, v33);
sub_140001F10(v34);                     // 执行命令
Sleep(100u);
```

Figure 3-2 Mounting EFI partition 2

The remaining two files are then copied to the newly mounted partition, the files in the original path are deleted, the recovery .exe in the new path is executed, and the EFI partition is finally unloaded.

Table 3-1 Copy payload file1

Original route	New path
C:\ Windows\ Installer\ recovery.exe	M:\ EFI\ Microsoft\ Boot\ recovery.exe
C:\ Windows\ Installer\ kd _ 08 _ 5e78.dll	M:\ EFI\ Microsoft\ Boot\ kd _ 08 _ 5e78.dll

3.2 Recovery.exe

After recovery. exe runs, create a process that executes% SystemRoot%\ System32\ Lsaiso. exe, and use remote thread injection technology to load kd _ 08 _ 5e78.dll.

```
if ( !lpBuffer )
  return 0;
v4 = GetModuleHandleW(L"kernel32.dll");
if ( !v4 )
  return 0;
LoadLibraryW = (HMODULE (__stdcall *)(LPCWSTR))GetProcAddress(v4, "LoadLibraryW");
if ( !LoadLibraryW )
  return 0;
v6 = -1i64;
while ( *((_WORD *)lpBuffer + ++v6) != 0 )
  ;
v8 = 2 * v6 + 2;
v9 = VirtualAllocEx(hProcess, 0i64, v8, 0x3000u, 4u);
v10 = v9;
if ( !v9 )
  return 0;
if ( !WriteProcessMemory(hProcess, v9, lpBuffer, v8, 0i64) )
{
  VirtualFreeEx(hProcess, v10, v8, 0x10000u);
  return 0;
}
v12 = -1;
v13 = CreateRemoteThread(hProcess, 0i64, 0i64, (LPTHREAD_START_ROUTINE)LoadLibraryW, v10, 0, 0i64);
v14 = v13;
if ( v13 )
{
  v12 = WaitForSingleObject(v13, 0x64u);
  CloseHandle(v14);
}
VirtualFreeEx(hProcess, v10, 0i64, 0x8000u);
```

Figure 3-3 Remote thread injection 3

3.3 Kd _ 08 _ 5e78.dll

After the DLL executes, it scans the processes running on the current system for the existence of some security tools.

```
lpString2[0] = L"Tas
lpString2[1] = L"pro
lpString2[2] = L"pro
lpString2[3] = L"pro
lpString2[4] = L"Pro
lpString2[5] = L"Pro
lpString2[6] = L"Pro
lpString2[7] = L"Pro
lpString2[8] = L"Sys
lpString2[9] = L"Dap
lpString2[10] = L"my
lpString2[11] = L"TM
lpString2[12] = L"TM
lpString2[13] = L"De
lpString2[14] = L"De
lpString2[15] = L"Sy
lpString2[16] = L"Sy
lpString2[17] = L"Wh
lpString2[18] = L"Ex
lpString2[19] = L"Ul
lpString2[20] = L"DT
lpString2[21] = L"Ki
lpString2[22] = L"To
lpString2[23] = L"sp
```

Figure 3-4 Check the process name 4

If that above process is not run in the current system, the content in the clipboard is obtained, and the begin character and the length of the content are detected according to the format of the encrypted money wallet address,

If there is a match, that wallet address of the cryptocurrency in the clipboard is replace with the wallet address of the attacker, thereby transfer the cryptocurrency.

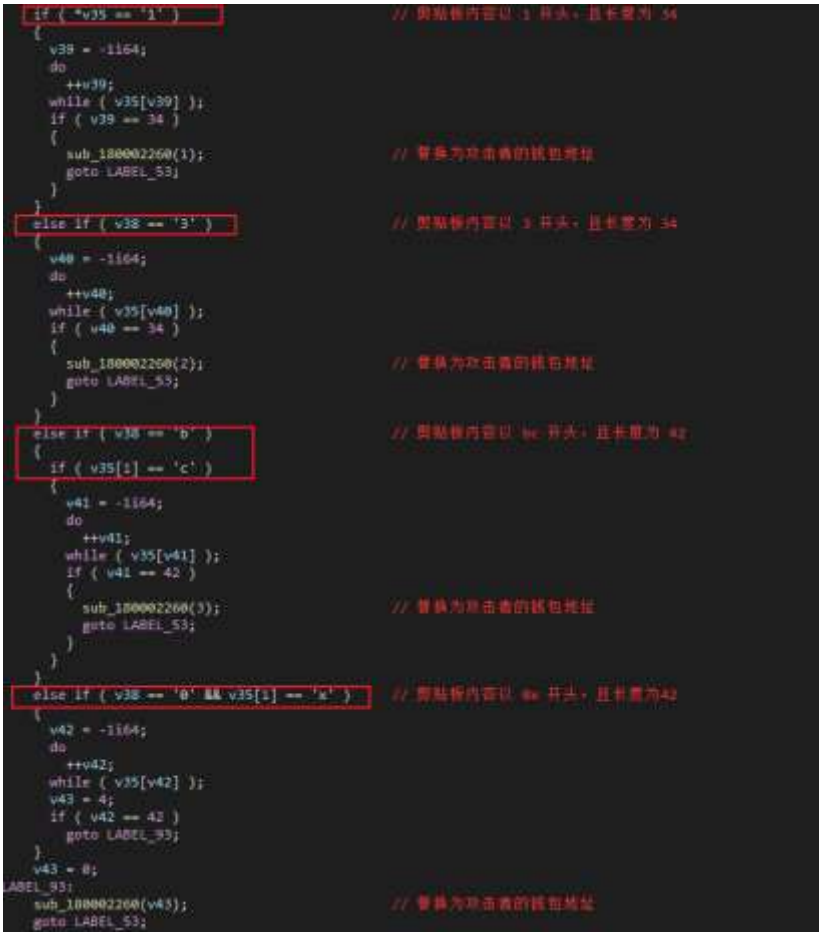

Figure 3-5 Alternative wallet address 3

This Clipboard hijacker replaces the corresponding relationship between the user's wallet and the attacker's wallet as shown in the following table.

Table 3-2 Replace the correspondence between the user wallet and the attacker wallet 2

User's wallet address	Type of cryptocurrency	Attacker's wallet address
A wallet address beginning with 1 and of length 34	Btc	1ae3pkjhtiv4aqliymtcnqyevmpmvmbdm
A wallet address beginning with 3 and of length 34	Btc	31ngg2flhw7tydw22bdrugwnv9r9hvygkv

Bc begins with a wallet address of length 42	Btc	Bc1qs5w5kt9qnr8wxd9n7etydmxjddqge4dnd7yxp
Wallet address starting with 0x and length 42	Eth	0xafd445d4bf54c0a5a3b6043b3fb76e42d68230ab

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 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, the PTA can effectively detect, analyze and identify all kinds of known and unknown threats.

4.2 Terminal protection

1. Install the terminal protection system: Install the anti-virus software, and it is recommended to install the terminal protection system of Antiy IEP;
2. Strengthen password strength: Avoid using weak passwords; it is recommended to use 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple accounts.

4.3 Timely initiate emergency response in case of attack

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

It has been proved that Antiy IEP can effectively detect and kill malware.

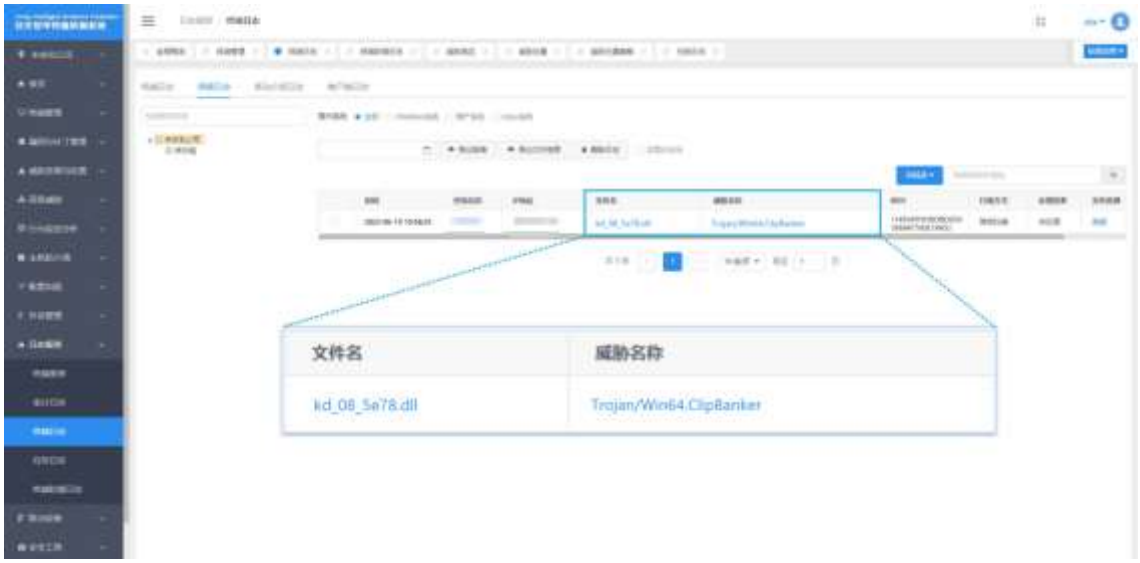

Figure 4-1 The effective protection of the user system implemented by Antiy IEP1

5 ATT&CK mapping graph of event

For the attacker to deliver the complete process of clipboard hijacker, the ATT&CK mapping graph corresponding to this attack event is shown in the following figure.

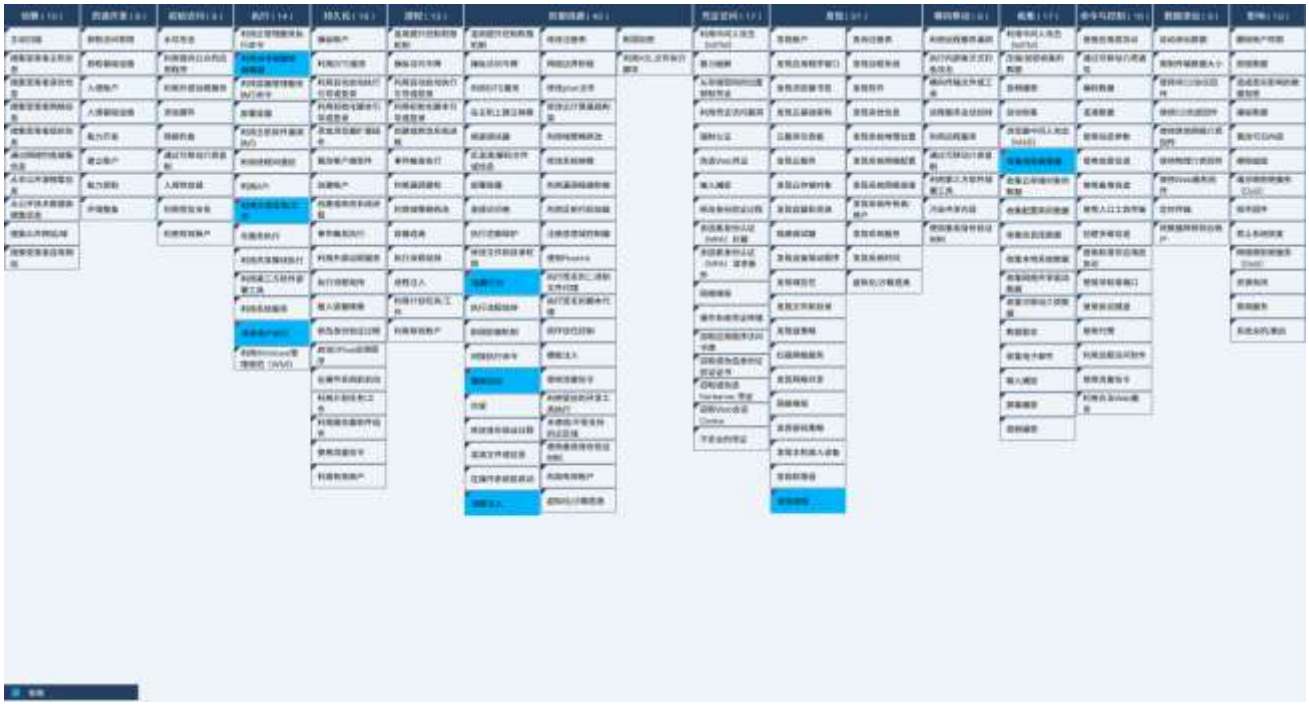

Figure 5-1 Mapping of technical features to ATT&CK 1

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 1

ATT&CK stages / categories	Specific behavior	Notes
Execution	Using command and script interpreters	Execute the CMD command
	Utilization of planned tasks / jobs	Using a scheduled task to execute a malicious program
	Inducing the user to execute	Inducing users to install a system image that has been maliciously tampered with
Defensive evasion	Concealment	Using partition of EFI system to hide malicious files
	Remove beacons	Delete the file in the original path
	Process injection	Injecting a malicious DLL into a legitimate process
Findings	Discovery Process	Detects whether a process with the specified name is running
Collection	Collect clipboard data	Monitor the contents of the clipboard to replace the cryptocurrency wallet address

6 IoCs

IoCs
Bfec28e480dfc 2814A2C762D0ADEE018
340de61434140809c7b2b5745c910508
114fe45f65bdbe6dd1b6847500e1b452
1ae3pkjhtiv4aqliymtcnqyevmpmvmbdm
31ngg2flhw7tydw22bdrugwnv9r9hvygkv
Bc1qs5w5kt9qnr8wxd9n7etydmxjddqge4dnd7yxp
0xafd445d4bf54c0a5a3b6043b3fb76e42d68230ab

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.