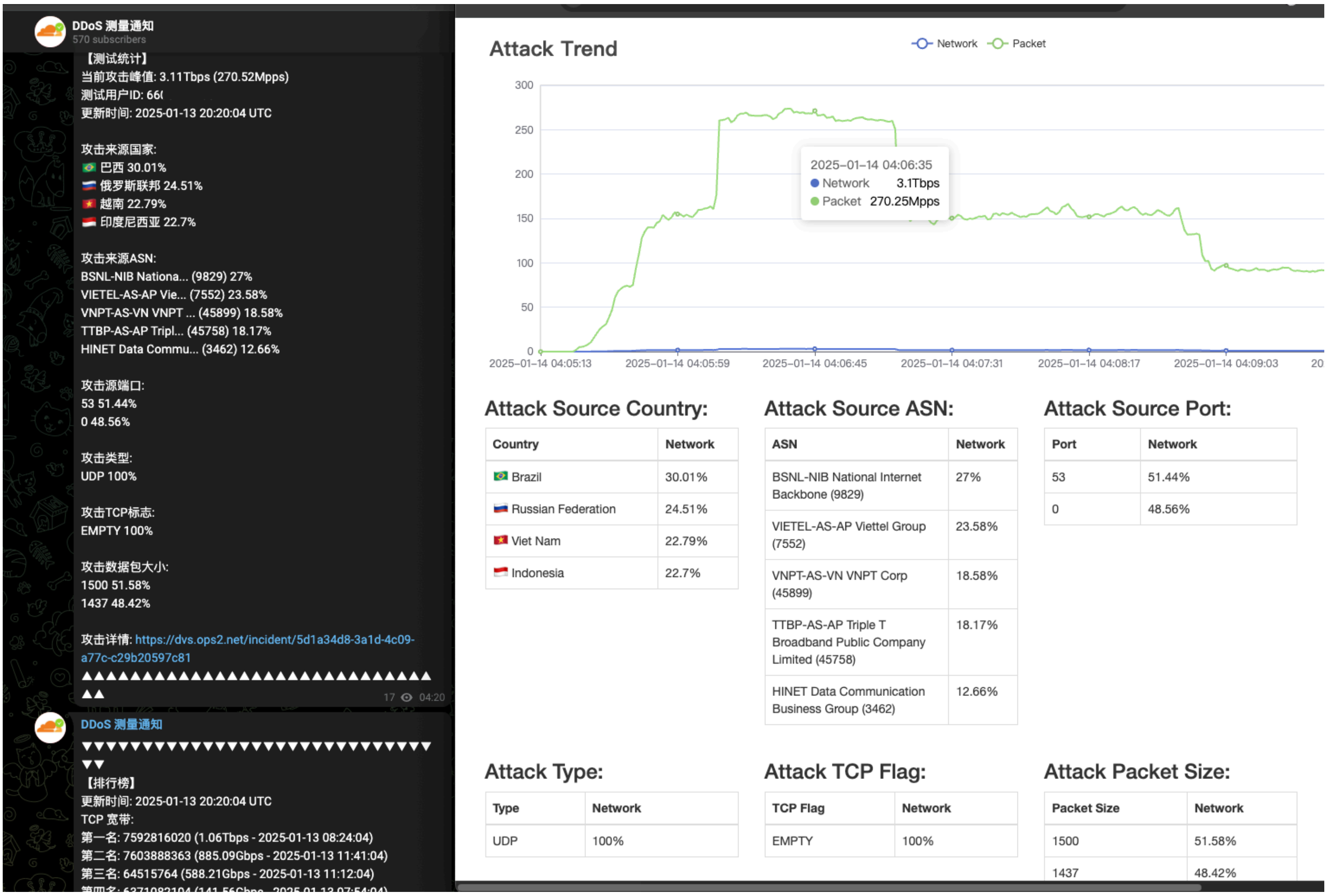
Botnet

Botnets Never Die: An Analysis of the Large Scale Botnet AIRASHI

Wang Hao, daji, Alex.Turing, Acey9

2025年1月15日 • 10 min read



DDoS 测量通知
570 subscribers

【测试统计】
当前攻击峰值: 3.11Tbps (270.52Mpps)
测试用户ID: 66(
更新时间: 2025-01-13 20:20:04 UTC

攻击来源国家:
🇧🇷 巴西 30.01%
🇷🇺 俄罗斯联邦 24.51%
🇻🇳 越南 22.79%
🇮🇩 印度尼西亚 22.7%

攻击来源ASN:
BSNL-NIB Nationa... (9829) 27%
VIETEL-AS-AP Vie... (7552) 23.58%
VNPT-AS-VN VNPT ... (45899) 18.58%
TTBP-AS-AP Tripl... (45758) 18.17%
HINET Data Commu... (3462) 12.66%

攻击源端口:
53 51.44%
0 48.56%

攻击类型:
UDP 100%

攻击TCP标志:
EMPTY 100%

攻击数据包大小:
1500 51.58%
1437 48.42%

攻击详情: https://dvs.ops2.net/incident/5d1a34d8-3a1d-4c09-a77c-c29b20597c81
▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲
▲▲
17 04:20

DDoS 测量通知
▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼
▼▼
【排行榜】
更新时间: 2025-01-13 20:20:04 UTC
TCP 宽带:
第一名: 7592816020 (1.06Tbps - 2025-01-13 08:24:04)
第二名: 7603888363 (885.09Gbps - 2025-01-13 11:41:04)
第三名: 64515764 (588.21Gbps - 2025-01-13 11:12:04)
第四名: 6371082104 (141.56Gbps - 2025-01-13 07:54:04)

Attack Trend

Attack Source Country:

Country	Network
🇧🇷 Brazil	30.01%
🇷🇺 Russian Federation	24.51%
🇻🇳 Viet Nam	22.79%
🇮🇩 Indonesia	22.7%

Attack Source ASN:

ASN	Network
BSNL-NIB National Internet Backbone (9829)	27%
VIETEL-AS-AP Viettel Group (7552)	23.58%
VNPT-AS-VN VNPT Corp (45899)	18.58%
TTBP-AS-AP Triple T Broadband Public Company Limited (45758)	18.17%
HINET Data Communication Business Group (3462)	12.66%

Attack Source Port:

Port	Network
53	51.44%
0	48.56%

Attack Type:

Type	Network
UDP	100%

Attack TCP Flag:

TCP Flag	Network
EMPTY	100%

Attack Packet Size:

Packet Size	Network
1500	51.58%
1437	48.42%

Overview

In August 2024, XLab observed a premeditated large-scale DDoS attack targeting the distribution platforms of the chinese game Black Myth: Wukong, namely Steam and Perfect World.This attack operation was divided into four waves, with the attackers carefully selecting the peak online hours of gamers in various time zones to launch sustained attacks lasting several hours. They simultaneously targeted hundreds of servers distributed across 13 global regions belonging to Steam and Perfect World, aiming to achieve maximum destructive impact. The botnet involved in this attack operation referred to itself as AISURU at the time. This article will analyze the variants of the AISURU botnet, known as AIRASHI.

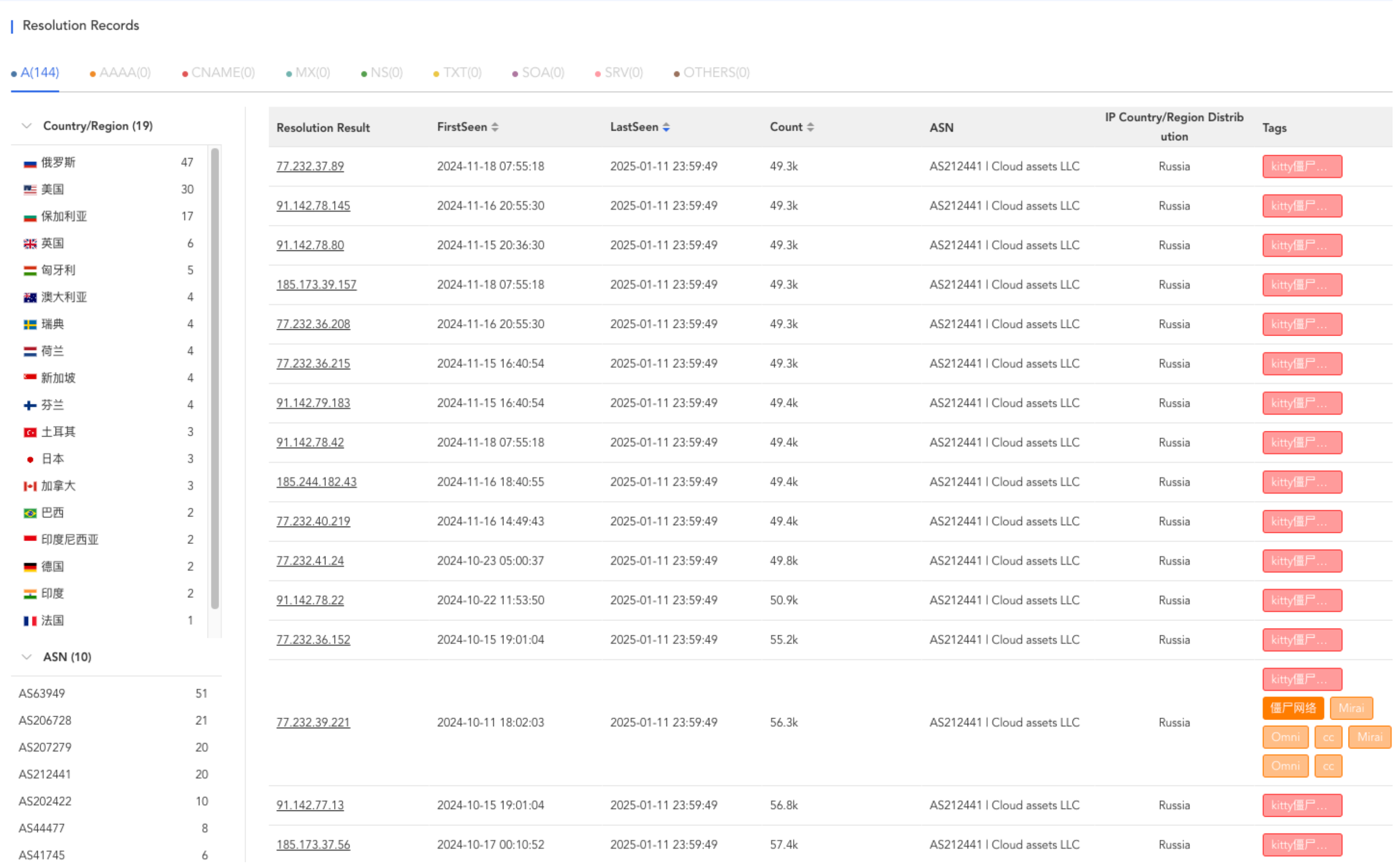
After the above-mentioned attack was exposed, the AISURU botnet temporarily ceased its attack activities in September. However, driven by profit motives, it was updated in October, and based on the sample characteristics, we named it kitty. By the end of November, a new variant reappeared and was updated again in the samples at the end of November, with the botnet renamed as: AIRASHI.

The current AIRASHI botnet has the following main characteristics:

- Uses a 0DAY vulnerability of cnPilot routers to spread samples.
- Sample strings are encrypted with RC4, while the CNC communication protocol has added HMAC-SHA256 verification and uses ChaCha20

encryption.

- CNC domain names include keywords such as xlabresearch, xlabsecurity, and foxthreatnointel, mocking XLAB and security researchers.
- Stable T-level DDoS attack capabilities.
- Rich IP resources for the command and control (CNC) end, with nearly 60 IPs resolved from domains, distributed across different countries and service providers. This may be intended to accommodate more bot endpoints and increase the difficulty of dismantling the botnet. The following image shows the Passive DNS records of AIRASHI CNC xlabsecurity.ru. It reveals that the CNC domain xlabsecurity.ru once resolved to 144 IPs distributed across 19 countries and 10 AS numbers (Autonomous System Numbers, ASN).



Resolution Records

Country/Region (19)	
俄罗斯	47
美国	30
保加利亚	17
英国	6
匈牙利	5
澳大利亚	4
瑞典	4
荷兰	4
新加坡	4
芬兰	4
土耳其	3
日本	3
加拿大	3
巴西	2
印度尼西亚	2
德国	2
印度	2
法国	1

ASN (10)	
AS63949	51
AS206728	21
AS207279	20
AS212441	20
AS202422	10
AS44477	8
AS41745	6

Resolution Result	FirstSeen	LastSeen	Count	ASN	IP Country/Region Distribution	Tags
77.232.37.89	2024-11-18 07:55:18	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
91.142.78.145	2024-11-16 20:55:30	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
91.142.78.80	2024-11-15 20:36:30	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
185.173.39.157	2024-11-18 07:55:18	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.36.208	2024-11-16 20:55:30	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.36.215	2024-11-15 16:40:54	2025-01-11 23:59:49	49.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
91.142.79.183	2024-11-15 16:40:54	2025-01-11 23:59:49	49.4k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
91.142.78.42	2024-11-18 07:55:18	2025-01-11 23:59:49	49.4k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
185.244.182.43	2024-11-16 18:40:55	2025-01-11 23:59:49	49.4k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.40.219	2024-11-16 14:49:43	2025-01-11 23:59:49	49.4k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.41.24	2024-10-23 05:00:37	2025-01-11 23:59:49	49.8k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
91.142.78.22	2024-10-22 11:53:50	2025-01-11 23:59:49	50.9k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.36.152	2024-10-15 19:01:04	2025-01-11 23:59:49	55.2k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
77.232.39.221	2024-10-11 18:02:03	2025-01-11 23:59:49	56.3k	AS212441 | Cloud assets LLC	Russia	kitty僵尸... 僵尸网络 Mirai Omni cc Mirai Omni cc
91.142.77.13	2024-10-15 19:01:04	2025-01-11 23:59:49	56.8k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...
185.173.37.56	2024-10-17 00:10:52	2025-01-11 23:59:49	57.4k	AS212441 | Cloud assets LLC	Russia	kitty僵尸...

xlabsecurity.ru Passive DNS records

Exploitation Details

Relying on the capabilities of XLab's large-scale threat awareness system, we observed that AIRASHI samples mainly spread through NDAY vulnerabilities and TELNET weak passwords, while also possessing the ability to exploit 0DAY vulnerabilities. Since June of last year, we have observed AIRASHI using a 0DAY vulnerability in cnPilot routers spread its samples. Regarding this 0DAY vulnerability, we contacted the manufacturer in June of last year, but received no response. To prevent abuse of the vulnerability, this article will not disclose information about it. The vulnerabilities exploited by AIRASHI are as follows:

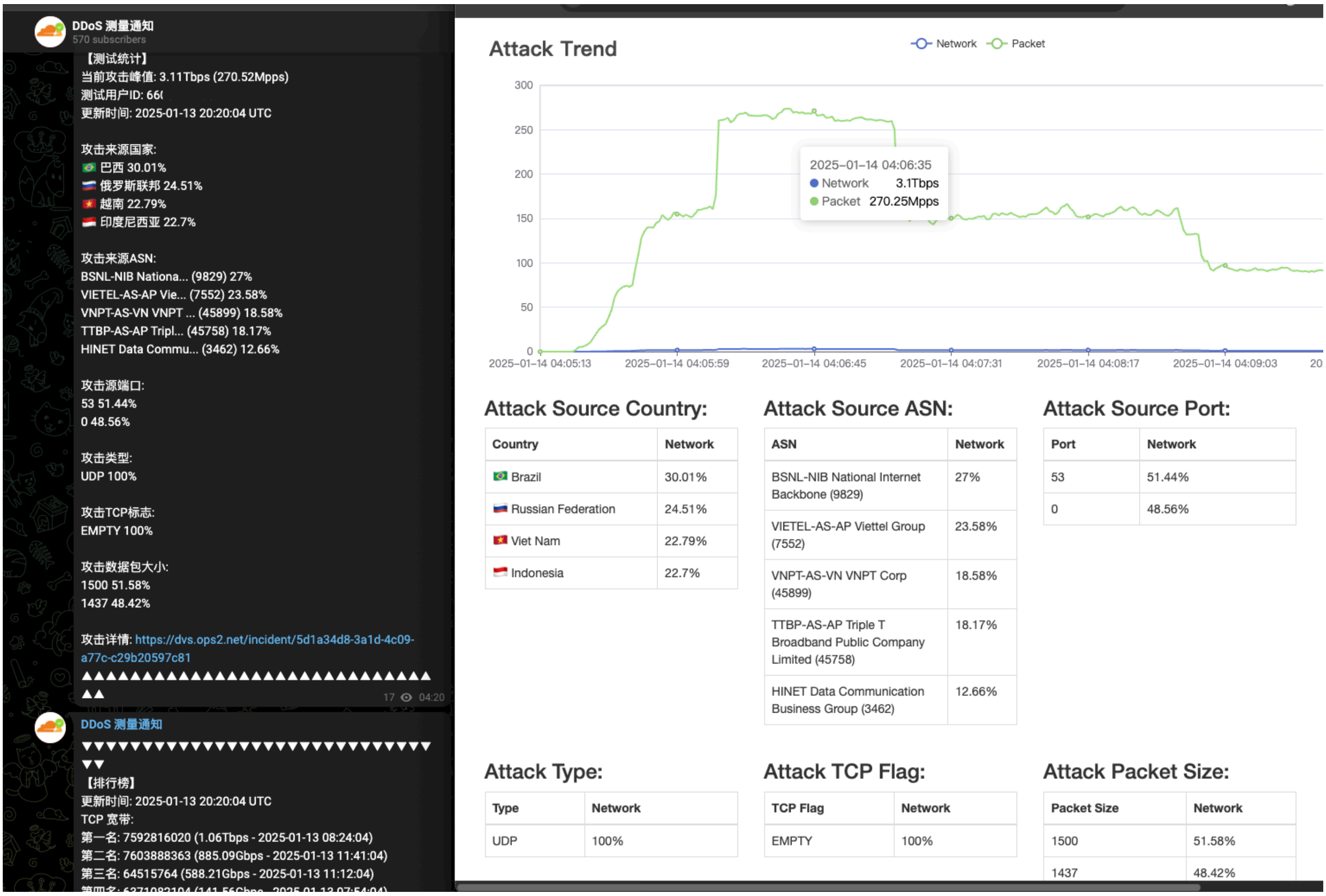
VULNERABILITY
AMTK Camera cmd.cgi Remote Code Execution
Google Android ADB Debug Server - Remote Payload Execution
AVTECH IP Camera / NVR / DVR Devices
cve_2013_3307
cve_2016_20016
cve_2017_5259
cve_2018_14558
cve_2020_25499
cve_2020_8515
cve_2022_40005
cve_2022_44149
cve_2023_28771
Gargoyle Route run_commands.sh Remote Code Execution
LILIN Digital Video Recorder Multiple Remote Code Execution
CVE-2022-3573
cnPilot 0DAY
OptiLink ONT1GEW GPON 2.1.11_X101
Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE

DDoS Capabilities and DDoS Activities

DDoS Capabilities

Botnet operators often showcase their attack capabilities through social media platforms such as Telegram, Discord, or forums, with the goal of attracting potential customers or intimidating competitors. To prove the attack capabilities of their botnets, some operators use third-party botnet attack measurement services for validation. They direct their botnets to attack servers provided by these measurement services. The measurement services then collect and analyze information such as the size of attack traffic, packet rates, geographic locations of the attack sources, ASNs, and attack methods. After receiving these statistics, the botnet operators post them on their social media platforms to demonstrate the power of their botnets.

The AIRASHI botnet uses this exact method to prove its attack capabilities. The image below shows one of their attack capability demonstrations：



DDoS 测量通知
570 subscribers

【测试统计】
当前攻击峰值: 3.11Tbps (270.52Mpps)
测试用户ID: 66(
更新时间: 2025-01-13 20:20:04 UTC

攻击来源国家:
🇧🇷 巴西 30.01%
🇷🇺 俄罗斯联邦 24.51%
🇻🇳 越南 22.79%
🇮🇩 印度尼西亚 22.7%

攻击来源ASN:
BSNL-NIB Nationa... (9829) 27%
VIETEL-AS-AP Vie... (7552) 23.58%
VNPT-AS-VN VNPT ... (45899) 18.58%
TTBP-AS-AP Tripl... (45758) 18.17%
HINET Data Commu... (3462) 12.66%

攻击源端口:
53 51.44%
0 48.56%

攻击类型:
UDP 100%

攻击TCP标志:
EMPTY 100%

攻击数据包大小:
1500 51.58%
1437 48.42%

攻击详情: https://dvs.ops2.net/incident/5d1a34d8-3a1d-4c09-a77c-c29b20597c81
▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲▲
17 04:20

DDoS 测量通知
▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼▼
【排行榜】
更新时间: 2025-01-13 20:20:04 UTC
TCP 宽带:
第一名: 7592816020 (1.06Tbps - 2025-01-13 08:24:04)
第二名: 7603888363 (885.09Gbps - 2025-01-13 11:41:04)
第三名: 64515764 (588.21Gbps - 2025-01-13 11:12:04)
第四名: 6371082104 (141.56Gbps - 2025-01-13 07:54:04)

Attack Trend

Attack Source Country:

Country	Network
🇧🇷 Brazil	30.01%
🇷🇺 Russian Federation	24.51%
🇻🇳 Viet Nam	22.79%
🇮🇩 Indonesia	22.7%

Attack Source ASN:

ASN	Network
BSNL-NIB National Internet Backbone (9829)	27%
VIETEL-AS-AP Viettel Group (7552)	23.58%
VNPT-AS-VN VNPT Corp (45899)	18.58%
TTBP-AS-AP Triple T Broadband Public Company Limited (45758)	18.17%
HINET Data Communication Business Group (3462)	12.66%

Attack Source Port:

Port	Network
53	51.44%
0	48.56%

Attack Type:

Type	Network
UDP	100%

Attack TCP Flag:

TCP Flag	Network
EMPTY	100%

Attack Packet Size:

Packet Size	Network
1500	51.58%
1437	48.42%

The statistics displayed on the image are as follows:

- Current attack peak: 3.11 Tbps (270.52 Mpps)
- Test user ID: 66XXXXXXXX (This ID corresponds to the Telegram channel administrator of the AIRASHI botnet)
- Last updated: 2025-01-13 20:20:04 UTC
- Attack source

The operator of AIRASHI has been posting their DDoS capability test results on Telegram. From historical data, it can be observed that the attack capacity of the AIRASHI botnet remains stable around 1-3 Tbps.

DDoS Activities

The attack targets of the AIRASHI botnet are spread globally across various industries, with the primary targets located in regions such as China, the United

States, Poland, and Russia. There is no clear, strong targeting strategy. The botnet typically attacks several hundred targets each day.

Sample Analysis

The AIRASHI botnet sample is frequently updated and has multiple versions. Some versions, in addition to supporting the main DDoS functionality and operating system command execution, also support proxy services. The following analysis focuses on kitty and AIRASHI, examining technical details of the botnet from aspects such as **string decryption, C2 retrieval, communication protocols, and supported commands.**

Part1: kitty-socks5

The kitty sample began spreading in early October 2024. Compared to previous AISURU samples, it has simplified the network protocol. By the end of October, it started using SOCKS5 proxies to communicate with the C2 server, and it encoded 250 proxies and 55 C2 addresses in the string table.

0x1: Decryption of strings

There are no significant changes in the string decoding method; it still uses xor_bytes. However, the key has been modified to **DEADBEEFCAFEBABE1234567890ABCDEF**, and the number of entries in the string table has been reduced to 7.

0x2: How to get C2

In terms of C2 retrieval, the method of obtaining the C2 IP through HTTP was removed in early October. The C2 string is still split using the | character, and as before, each domain is mapped to over 20 IP addresses.

eg: `dvrhelpers.su|ipcamlover.ru|xlabresearch.ru|xlabsecurity.ru`

However, after the addition of SOCKS5 at the end of October, the string table was updated to include proxy entries. Both the C2 and proxy entries are now encoded using multiple sets of IP-PORT byte sequences.

eg: `\x7f\x00\x00\x01\x00\x50` represents `127.0.0.1:80`

0x3: Network Protocol

In terms of the network protocol, it still uses a switch-case structure for handling different stages, similar to the Fodcha botnet.

However, the communication process has been simplified. The latest sample uses a SOCKS5 proxy (with authentication) to access the C2 server.

```
username: jjktkegl
password: 2bd463maabw5
```

The original key exchange process has been removed, and the communication traffic is no longer encrypted. The startup packet is replaced with **Kitty-Kitty-Kitty**, and every 2 minutes, a heartbeat packet **cat** is sent to the C2 server, which responds with **meow!**.

The command types still focus primarily on DDoS, with the addition of a reverse shell functionality. The command format hasn't changed significantly. It still follows the **cmdtype+payload** structure, but the value of cmdtype has been updated. Additionally, DDoS-related commands now include a new AttckID field.

CMDTYPE	DESC
0x13	reverse shell
0x2c	stop attack
0x4b	start attack

CMDTYPE	DESC
0xaf	exit

Part2: AIRASHI

Currently, three types of AIRASHI samples have been discovered:
1. AIRASHI-DDoS: First identified in late October, this sample primarily focuses on DDoS attacks but also allows arbitrary command execution and reverse shell access.
2. Go-Proxisdk: First discovered in late November, this is a proxy tool based on muxado written in Go.
3. AIRASHI-Proxy: First identified in early December, this is a heavily modified version of the AIRASHI-DDoS source code, using a private protocol to implement proxy functionality.

AIRASHI shares some similarities with AISURU. If kitty is a streamlined version of AISURU, then AIRASHI seems to be an upgraded version. Since October, it has been continuously updated. After developing the simple Go-Proxisdk, the custom protocol proxy tool AIRASHI-Proxy was developed, indicating an attempt to surprise us with entirely new features.

0x1: RC4

AIRASHI and AISURU share some common characteristics in string decryption. Both continue to use a 16-byte key, and the decryption algorithm employed is RC4. The output string is **snow slide**, and special strings are separated using the | character. The decryption method is the same for both the Proxy and DDoS versions, but the Proxy version contains significantly fewer strings.

Interestingly, some unused strings appear to be responding to our previous blog: It includes a YouTube link to a conga dance track and a dance invitation. Additionally, there's a request for xlab and foxnointel to name this variant "AIRASHI".

```
0 'snow slide'
1 'telnetd|upnpc-static|udhcpc|/usr/bin/inetd|ntpclient|boa|lighttpd|httpd|goahead|
2 '/dvrEncoder|/dvrRecorder|/dvrDecoder|/rtspd|/ptzcontrol|/dvrUpdater'
3 'cve-2021-36260.ru'
4 'honeybooterz.cve-2021-36260.ru'
5 'stun.l.google.com:19302'
6 '/proc/'
7 '/proc/self/exe'
8 '/proc/net/tcp'
9 '/proc/mounts'
10 '/cmdline'
11 '/exe'
12 '/status'
13 '/fd/'
14 'PPid:'
15 '/bin/|/sbin/|/usr/|/snap/'
16 'wget|curl|tftp|ftpget|reboot|chmod'
17 '/bin/login'
18 '/usr/bin/cat'
19 'processor'
20 '/proc/cpuinfo'
21 '/bin/busybox echo AIRASHI > /proc/sys/kernel/hostname'
22 '/bin/busybox AIRASHI'
23 'AIRASHI: applet not found'
24 'abcdefghijklmnopqrstuvw012345678'
25 'come on, shake your body xlab, do the conga'
26 'i know you can't control yourself any longer'
27 'https://www.youtube.com/watch?v=ODKTITUPusM'
28 'dear researcher (xlab, foxnointel, ...), please refer to this malware as AIRASH
```

0x2: How to Get C2

AIRASHI uses three different methods to get C2:
1. AIRASHI-DDoS (Early development, late October): The most basic method, using DNS servers to resolve the C2's A record.
2. AIRASHI-Proxy: Retrieves the C2's TXT record from the DNS server and decodes the plaintext IP and port.
3. AIRASHI-DDoS (Late November): Uses DNS servers to retrieve the C2's TXT record, then base64-decrypts and decrypts 4 bytes of the IP using ChaCha20. The port is hardcoded in the sample.

- DNS_TXT_CHACHA20_KEY: `8E12DF8893A638354D851BCB46B5B7DC451C6F52066305AC641DE60C80D11850`
- DND_TXT_CHACHA20_NONCE: `941A247DDD53819F755FD59B`

It is worth noting that on December 3rd, both the A record and TXT record for C2 resolution existed simultaneously for AIRASHI-DDoS, and there was a corresponding relationship after decryption. This might have been done to ensure compatibility with previous versions, but it renders the encryption and encoding largely meaningless.

0x3: Network Protocol

AIRASHI uses a completely new network protocol that involves HMAC-SHA256 and CHACHA20 algorithms. HMAC is used to verify the integrity of the message, while the negotiated CHACHA20_KEY is used to encrypt and decrypt the message. In the Proxy version, HMAC is not used for message verification in the protocol part, but the rest of the protocol remains consistent with the DDoS version.

- **Communication With C2**
  Each message is divided into two parts: a 32-byte HMAC checksum of the message and the message itself.
  As shown in the diagram, the Header part of the message is sent first to confirm the message type and length. If the message length is not zero, the Payload part is then sent.
  The communication process, like before, is controlled by a switch-case structure using status codes, and it is divided into 4 steps:
  1. Key Negotiation
  - Obtain a 32-byte CHACHA20_KEY and a nonce. Subsequent messages are encrypted using CHACHA20 and the CHACHA20_KEY is used as the key for HMAC-SHA256.
  2. Key Confirmation
  - A message with type 1 is encrypted using CHACHA20 and sent. The

returned message type is verified to ensure it is also type 1.

3. Send Startup Packet

- The architecture type is obtained by reading the ELF header. The structure of the startup packet is as follows:

`c struct login{ uint8 uk1; uint8 uk2; uint8 uk3; uint32 stunIP; uint32 botid_len; char botid[botid_len]; uint16 cpu_core_num; uint16 arch_type; }`

4. Check-In Confirmation

- The C2 returns a message with type 2.

The actual traffic generated is as follows:

- **Message Type**

  AIRASHI-DDoS supports a total of 13 message types, and the corresponding handling functions are stored in an array within the bot's code. Some of the handling functions for certain message types are still incomplete, suggesting that they may still be under development.

AIRASHI-DDoS supports the following 13 message types, with some reserved for future development:

MSG_TYPE	DESC
0	Get Net Key
1	Confirm Net Key
2	Confirm Login
3	Heartbeat
4	Start Attack
5	Exit
6	Killer Report
7	unknown
8	unknown
9	Disable Killer
10	Enable killer
11	Exec Command

MSG_TYPE	DESC
12	Reverse Shell

On the other hand, AIRASHI-Proxy supports only 5 message types, with the first 4 types being identical to those in AIRASHI-DDoS.

MSG_TYPE	DESC
0	Get Net Key
1	Confirm Net Key
2	Confirm Login
3	Heartbeat
4	Unknown
5	Prxoy

Detection

Due to the active exploitation of the cnPilot router 0Day vulnerability, we are unable to provide further details. However, we are providing Snort rules to assist defenders in identifying vulnerability attempts and potential infections in their environment.

```
alert tcp any any -> any any (msg:"0DAY exploit #1 attempt"; content:"execute_scrip
```

Contact Us

Readers are always welcomed to reach us on twitter.

IOC

C2

```
xlabresearch.ru
xlabsecurity.ru
foxthreatnointel.africa
```

SHA1

```
3c33aa8d1b962ec6a107897d80d34a5d0b99899e
0339415f8f3e2b1eb6b24ed08c3a311210893a6e
95c8073cc4d8b80ceddb8384977ddc7bbcb30d8c
12fda6d480166d8e98294745de1cfdcf52dbfa41
08b30f5ffa490e15fb3735d69545c67392ea24e9
c8b8bd5384eff0fe3a3a0af82c378f620b7dc625
```

Downloader

```
190.123.46.21   Panama|Panama|Panama    AS52284|Panamaserver.com
190.123.46.55   Panama|Panama|Panama    AS52284|Panamaserver.com
95.214.52.167   Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
162.220.163.14  United States|New Jersey|Secaucus       AS19318|Interserver, Inc
```

What do you think?

5 Responses

Upvote Funny Love Surprised Angry Sad

0 Comments

1 Login ▾

G

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share

Best Newest Oldest

RSS

Powered by Ghost