JPCERT/CC Internet Threat Monitoring Report

January 1, 2025 - March 31, 2025

JPCERT Coordination Center

June 6, 2025

Table of Contents

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Coordination Activities for International Cooperation in Responding to Cyber Attacks for the 2024 Fiscal Year".

1. Overview

JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that are observed by the sensors, and these packets are categorized by the destination port number, source region, etc. Then this information is analyzed along with information about vulnerabilities, malware and attack tools to obtain information on attacking activities or preparatory activities. Data collected through sensors are analyzed, and if any problem subjected to an attack or used to carry out an attack is found, JPCERT/CC provides information to parties who may be able to solve the problem and asks them to take appropriate steps.

This report will provide an overview of the results of monitoring activities by JPCERT/CC's Internet threat monitoring system (TSUBAME) during this quarter and their analysis.

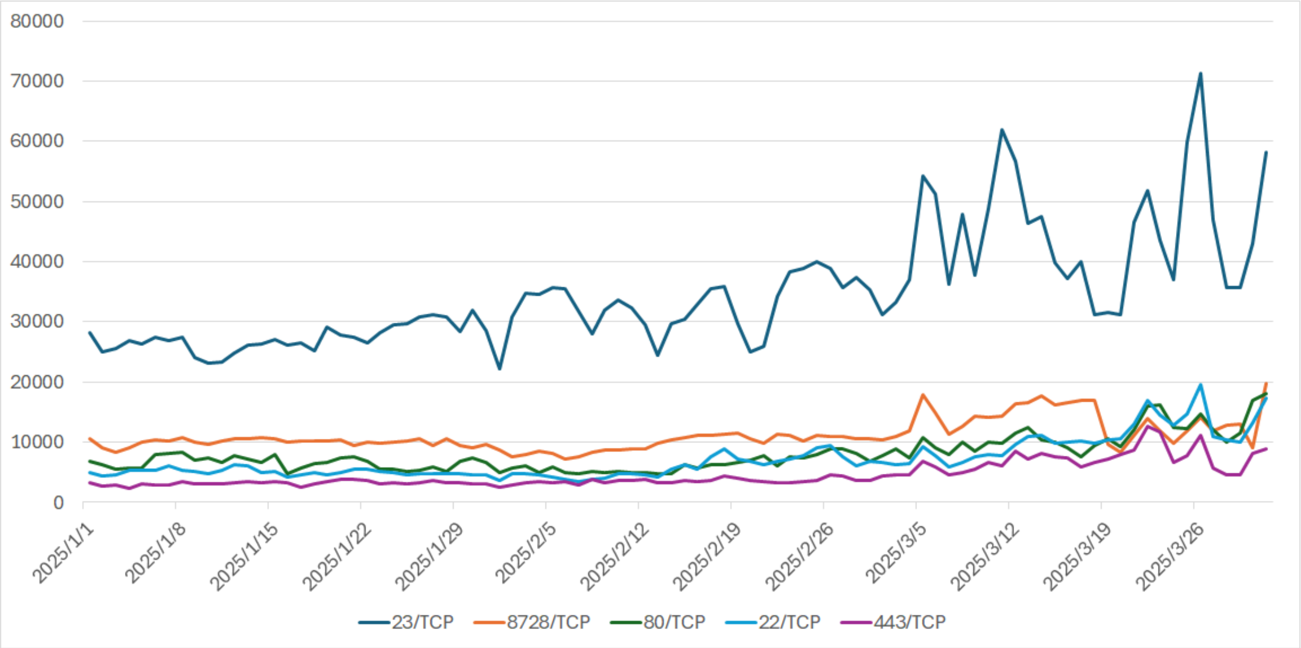
The top 5 services scanned in Japan during this quarter are shown in [Table 1].

[Table 1: Top 5 services frequently scanned in Japan]

Rank	Destination Port Numbers	Previous Quarter
1	Telnet (23/TCP)	1
2	8728/TCP	2
3	http (80/TCP)	3
4	ssh（22/TCP）	4
5	https（443/TCP）	6

*For details on services provided on each port number, please refer to the documentation provided by IANA(1). The service names listed are based on the information provided by IANA, but this does not always mean that the packets received are in a format relevant for that service / protocol.

The numbers of scan packets observed for the services listed in [Table 1] are shown in [Figure 1].



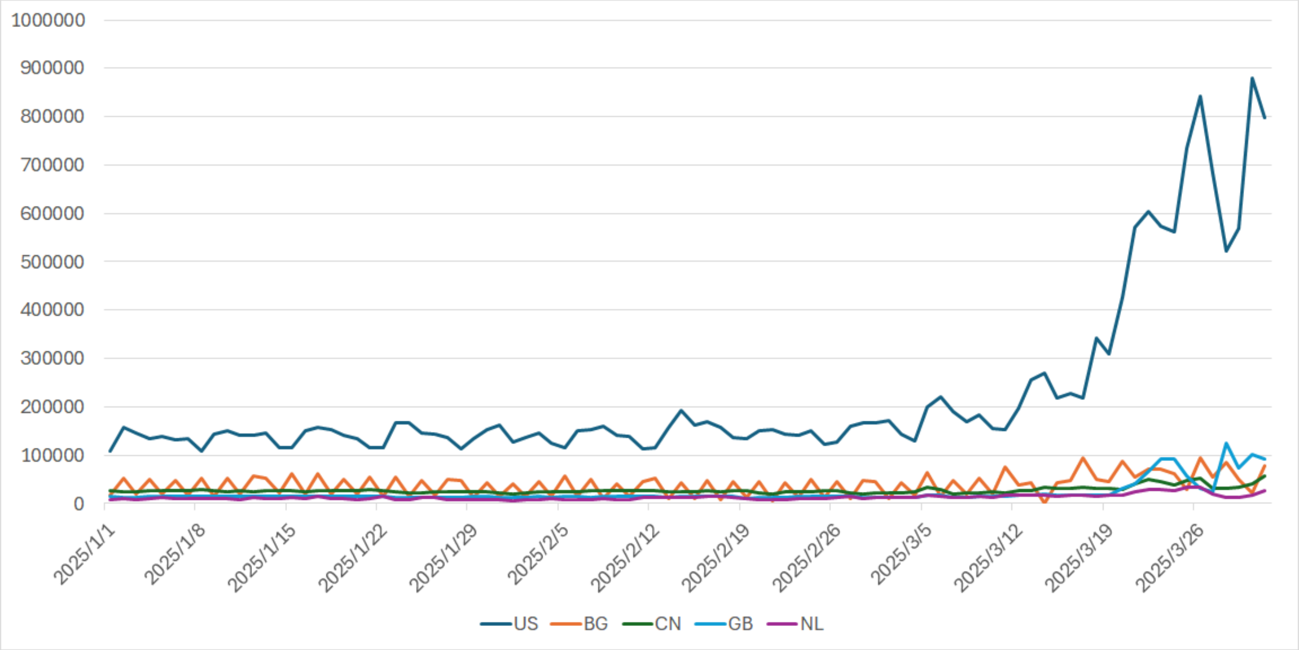
[Figure 1: Number of observed packets targeted to the top 5 services (destination port numbers) frequently scanned (January through March 2025)]

The service most frequently scanned this quarter was Telnet (23/TCP). The second place was 8728/TCP. While 8728/TCP is not on IANA's list, it is used by MikroTik's API for managing routers and is presumably being scanned to find them. The third and fourth places were http (80/TCP) and ssh (22/TCP). The fifth place was https (443/TCP), which has seen a growing number of scans since March. Next, the top 5 source regions where scanning activities targeting Japan were seen most frequently during this quarter are shown in [Table 2].

[Table 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	USA	1
2	Bulgaria	2
3	China	3
4	Great Britain	4
5	Netherlands	6

The trend of source regions for this quarter listed in [Table 2] are shown in [Figure 2].



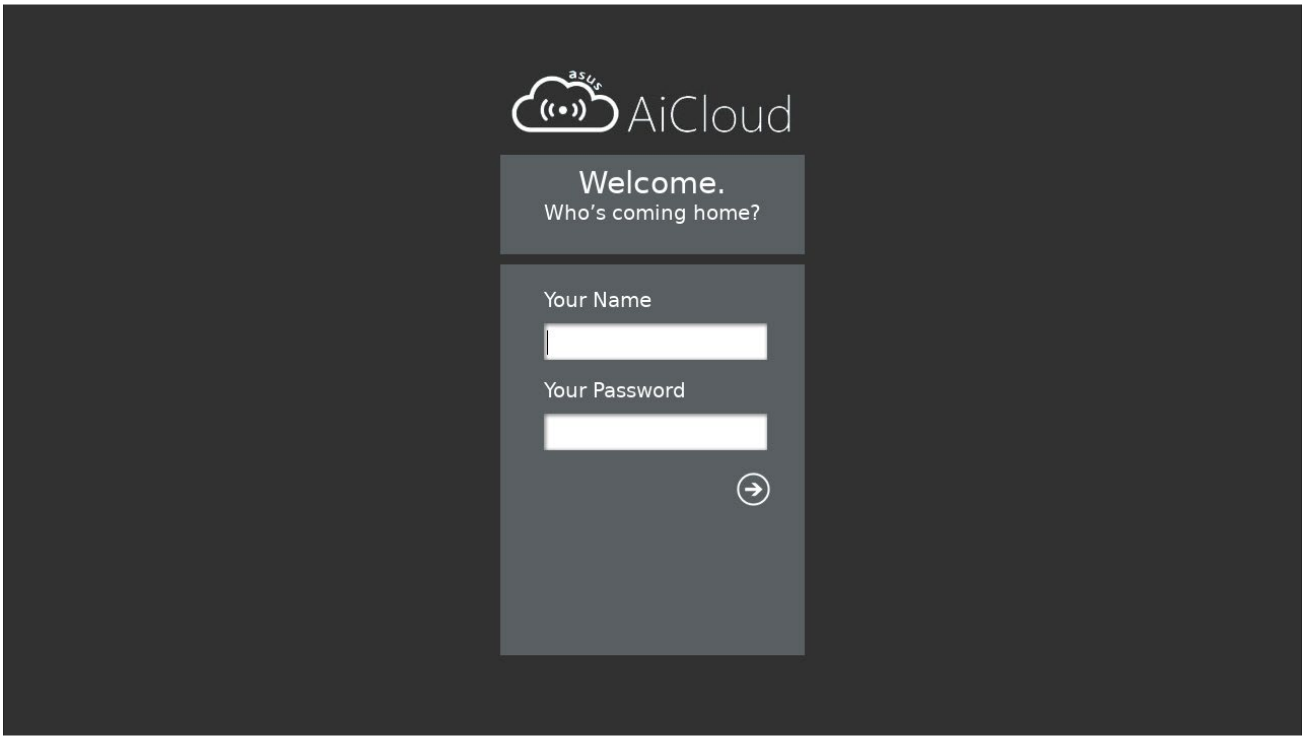
[Figure 2: Number of packets by source region (January through March 2025)]

The top four regions were the same as in the previous quarter, with the USA at the top. In particular, the US has seen an increase in packets sent from US cloud service providers from around March 18. No major changes were seen for the second to fourth places, and the Netherlands rose from the sixth to fifth place. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

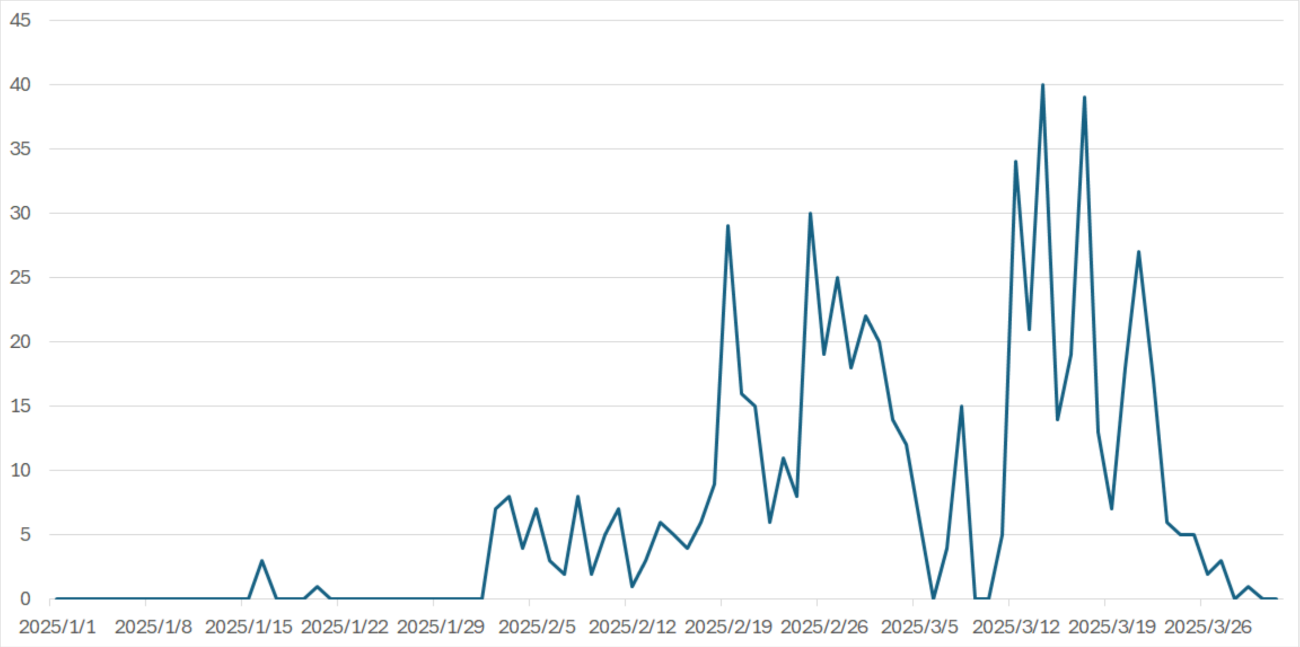
2. Observation of packets apparently sent from ASUS routers infected with malware

Previous observation has revealed that many of the packets observed by TSUBAME are sent from devices infected with malware. To identify the types of devices involved and deliberate effective countermeasures, JPCERT/CC is collecting information such as by accessing packet sources with browsers.

In these activities, ASUS routers' login screen (Figure 3), which was only rarely seen previously, started to be observed nearly everyday from February 2025 (Figure 4). This chapter will discuss the investigation conducted to study the background.



[Figure 3: ASUS router's login screen]



[Figure 4: Number of IP addresses presumed to be used by active ASUS routers]

Figure 3 shows the login screen that is displayed when a unique ASUS router feature called AiCloud is active. AiCloud enables remotely accessing USB storage devices connected to the router via the Internet like a NAS, accessing shared folders on a LAN, and powering on a computer with Wake-on-LAN.

Typically, Mirai and other malware that target IoT devices like routers are not capable of permanently maintaining the infected state. For this reason, when the infected router reboots due to being overloaded by scanning activities, for example, the router will no longer be in an infected state. This can be inferred by the fact that about 90% of the packets sent from the IP addresses of active ASUS routers ceased to be observed within 48 hours.

However, new instances of ASUS routers' login screen continued to be detected for two months from February through March. This is presumably because attack campaigns exploiting vulnerabilities in ASUS routers in an attempt to infect devices with malware continued to occur during this period.

Organizations other than JPCERT/CC have also reported observing attack campaigns exploiting vulnerabilities in ASUS routers, and NICT has issued a document(2) to alert users. JPCERT/CC has published observation status and information on countermeasures on CyberNewsFlash(3), encouraging users to address vulnerabilities disclosed by ASUS on January 2, 2025.

Internet-connected devices are not just accessible to users but subject to access attempts by attackers as well. Be sure to take necessary precautions when using these devices, such as keeping the firmware up-to-date, using proper authentication methods, setting strong passwords, and disabling the service if not needed.

3. Request from JPCERT/CC

JPCERT/CC may contact users of IP addresses sending suspicious packets and ask them to take certain action via Internet service providers. If you ever receive such requests, we hope you understand the purpose of our investigation activities and, if possible, provide information such as products used, firmware versions, and any evidence of intrusion. There are a number of unknown scanning activities, including those discussed in this report. Your information may offer valuable insights leading to clarification.

4. References

（1）IANA（Internet Assigned Numbers Authority）
Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-portnumbers.xhtml

（2）NICT
Security alert concerning attacks exploiting vulnerabilities in ASUS WiFi routers' AiCloud feature <Japanese only>
https://blog.nicter.jp/2025/04/asus_aicloud/

（3）JPCERT/CC
Observation of communication from ASUS WiFi routers with active AiCloud <Japanese only>
https://www.jpcert.or.jp/newsflash/2025041701.html

If you would like to cite or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). Company names and product names in this document are the trademarks or registered trademarks of the respective companies.
For the latest information, please refer to JPCERT/ CC's website.

- JPCERT Coordination Center (JPCERT/CC)
  https://www.jpcert.or.jp/english/
- Sharing incident information and requesting
  coordinationinfo@jpcert.or.jp, https://www.jpcert.or.jp/form/
- Inquiries about vulnerability information handling
  vultures@jpcert.or.jp
- Inquiries about ICS security
  icsr@jpcert.or.jp
- Inquiries about secure coding seminars
  secure-coding@jpcert.or.jp
- Inquiries about citing published documents, requesting a presentation, etc.
  pr@jpcert.or.jp
- PGP public keys
  https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Internet Threat Monitoring Report [January 1, 2025 - March 31, 2025]

- First version issued: June 6, 2025
- Issued by:
  Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
  8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023, Japan