JPCERT CC®

JPCERT Coordination Center

JPCERT/CC Internet Threat Monitoring Report

October 1, 2024 - December 31, 2024

JPCERT Coordination Center

February 28, 2025

JPCERT CC®

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

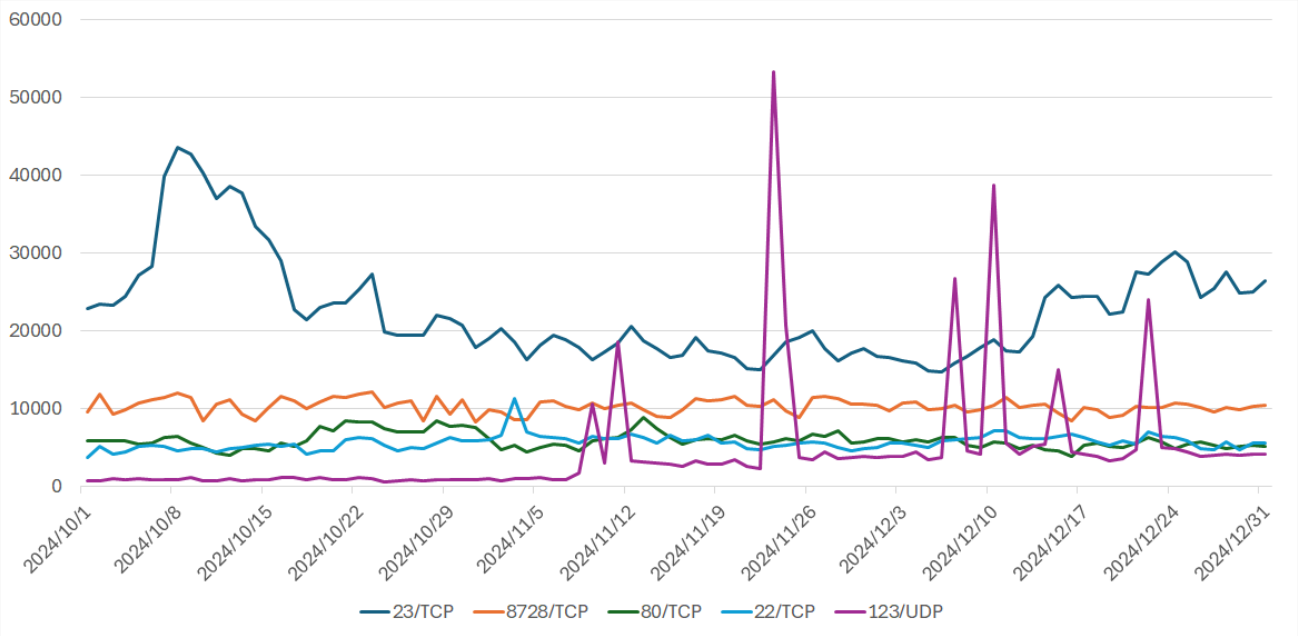
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that 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 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)	5
5	ntp (123/UDP)	Not in top 10

*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].



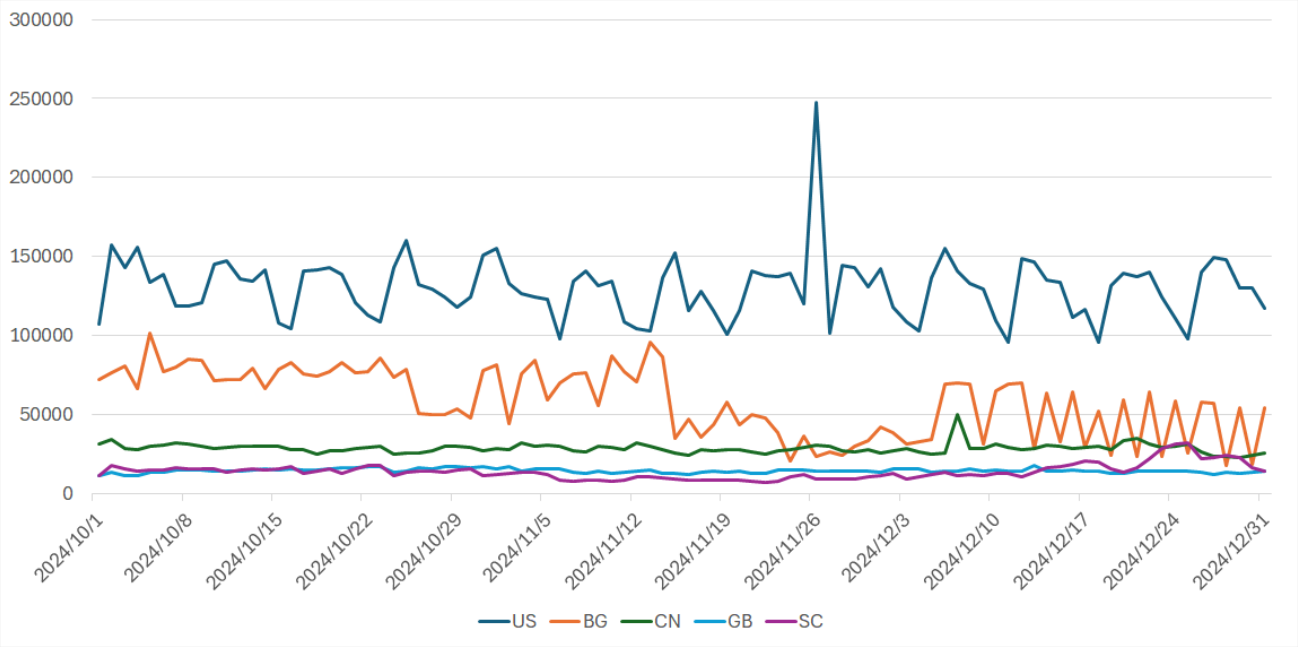
[Figure 1: Number of observed packets targeted to the top 5 services (destination port numbers) frequently scanned (October through December 2024)]

The service most frequently scanned this quarter was Telnet (23/TCP). The second place was 8728/TCP. While this port number is not on IANA's list, it is a listening port used by MikroTik's API for the administration of routers. The third and fourth places were http (80/TCP) and ssh (22/TCP). The fifth place was ntp (123/UDP), which saw a number of surges. 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	6
5	Seychelles	9

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

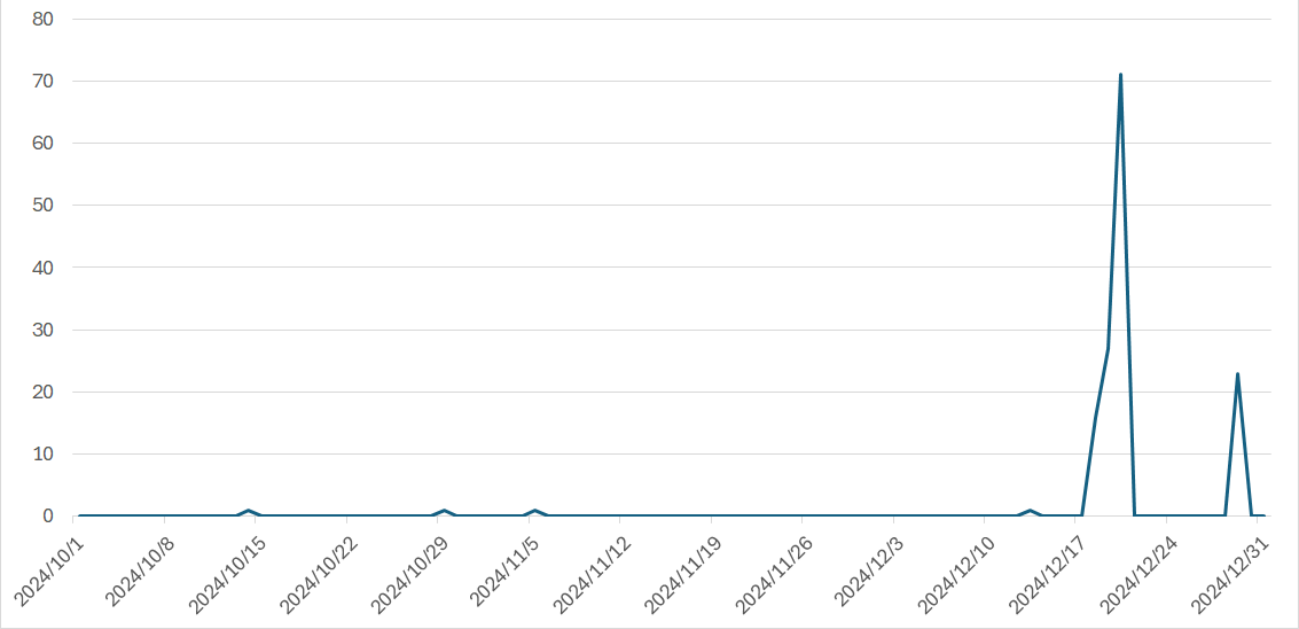


[Figure 2: Number of packets by source region (October through December 2024)]

The top three regions were the same as in the previous quarter, with the USA at the top. Packets originating in the Netherlands started to decrease gradually from around November 26, causing the country to fall to sixth place and the UK to take its place at the fourth spot. In Seychelles, which ranked fifth, packets targeting a number of destination ports temporarily increased. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

2. Observation of attack packets using open resolvers as springboards

This chapter will discuss the observation in December of attack packets using open resolvers in Japan as springboards. These attack packets are characterized by the fact that they are sent from port 53/UDP, which is used by DNS. See the figure below for trends in the number of IP addresses used by attack packets originating in Japan (Figure 3).



[Figure 3: Number of IP addresses used by DNS packets sent from Japan (October through December 2024)]

During the quarter, no attack packets were observed on most days, but sharp increases were seen temporarily from December 18 to 20 and on December 29. JPCERT/CC examined source IP addresses using SHODAN and other means and found that nearly all of them were open resolvers. These hosts had one of the following characteristics.

1. A server running Linux, MacOS, etc. and behaving as a resolver, with no access restrictions set against resolvers
2. A router product designed for SOHO and businesses that does not have any access restrictions set
3. A router product designed for general users that is connected and used with the WAN port mistaken for a LAN port

Users of these products are encouraged to configure devices and servers appropriately and check access restrictions, particularly against access via the Internet (accesses to the WAN port). In many cases, the hosts were confirmed to be resolvers, and their administration interface and API ports were accessible from WAN. It is important to make sure devices and servers are configured only as intended and do not allow

any unintended connections. Users are encouraged to check the settings and configuration by comparing them with the user's manual. JPCERT/CC provides a service for assessing whether a server or device is an open resolver (2). Please use it after setting up a server or installing a network device.
The packets observed this time had characteristics including the use of DNSSEC, which makes them relatively large. Also, while TSUBAME sensors are installed around the world, the packets were only observed by those installed on the network of a certain cloud provider. We chose to discuss this event in this report since it could have been part of a campaign attempting DDoS attacks against the cloud provider by sending DNS queries spoofing its IP addresses.

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) JPCERT/CC
Open resolver check site <Japanese only>
https://www.jpcert.or.jp/magazine/security/openresolver.html

- 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 [October 1, 2024 - December 31, 2024]

- First version issued: February 28, 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