JPCERT/CC Internet Threat Monitoring Report

July 1, 2024 - September 30, 2024

JPCERT Coordination Center

November 12, 2024

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

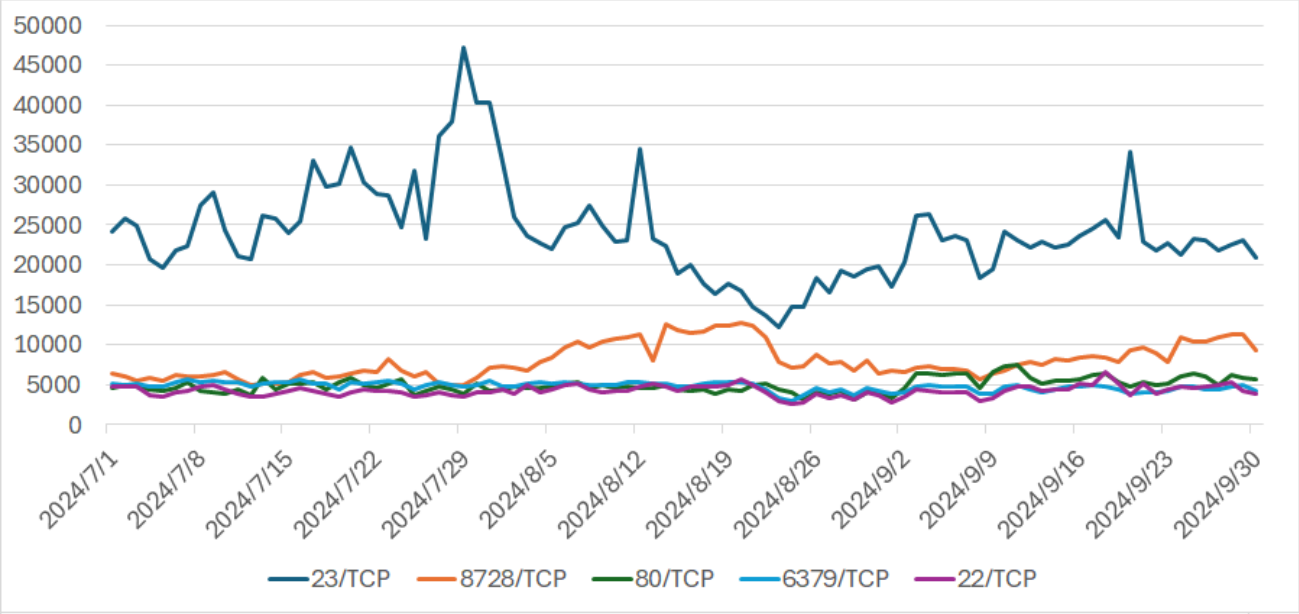
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that 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)	4
4	redis (6379/TCP)	3
5	ssh (22/TCP)	5

*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].



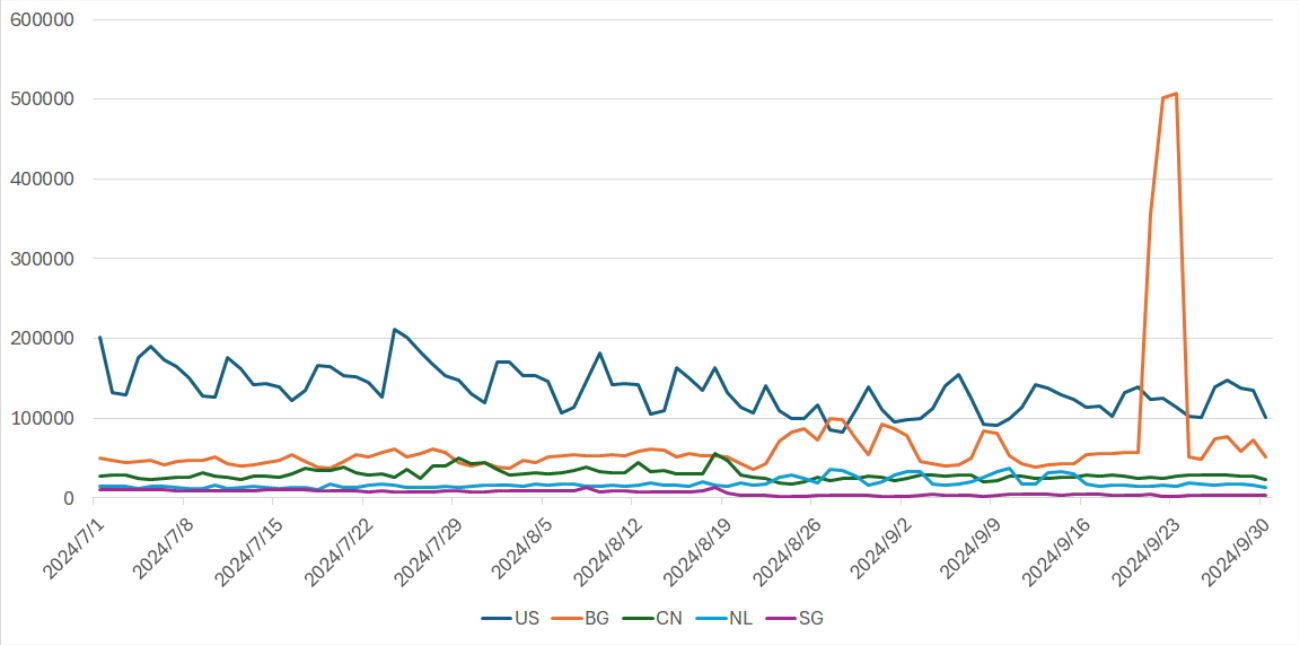
[Figure 1: Number of observed packets targeted to the top 5 services (destination port numbers) frequently scanned (July through September 2024)]

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 to fifth places were http (80/TCP), redis (6379/TCP) and ssh (22/TCP). Scanning activities targeting http increased from around September 3, pushing it above redis in the rankings. 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	Netherlands	4
5	Singapore	6

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



[Figure 2: Trend of source regions from July through September 2024]

The USA stayed at the top, with no changes in the subsequent rankings through the fourth place. Russia saw the number of packets go down around August 19 and changed places with Singapore in the rankings. As for the trend of other source regions, there was nothing in particular worth noting. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

2. Decline in the number of source IP addresses for packets originating in Japan and targeting Telnet (23/TCP)

This chapter will discuss trends in Telnet scans that have a specific parameter and originate from IP addresses in Japan. The number of sources of scans targeting Telnet (23/TCP) decreased throughout this quarter (Figure 3).

[Figure 3: Number of IP addresses in Japan for packets targeting Telnet]

A slowly declining trend was seen throughout the quarter, and by the final week of September, the number fell to around 40% of the level in the first week of July. The number of source IP addresses has also declined, and all remaining routers and digital video recorders have already been identified, with no new devices found. The backdrop to this may be that security measures for IoT devices have been widely adopted, but there is also the possibility that the attackers' interest has shifted elsewhere, or that the malware used by the attackers has stopped needlessly scanning third parties that have been modified. It is entirely possible that scanning activities could surge again in the future, so users of potential target devices are advised to continue to update their firmware and take measures to mitigate attacks. As stated in "3. Request from JPCERT/CC," JPCERT/CC provides relevant information to Internet service providers if any abnormal scanning activities are observed.

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

- 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 [July 1, 2024 - September 30, 2024]

- First version issued: December 6, 2024
- 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