JPCERT/CC Internet Threat Monitoring Report

April 1, 2024 - June 30, 2024

JPCERT Coordination Center

August 9, 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

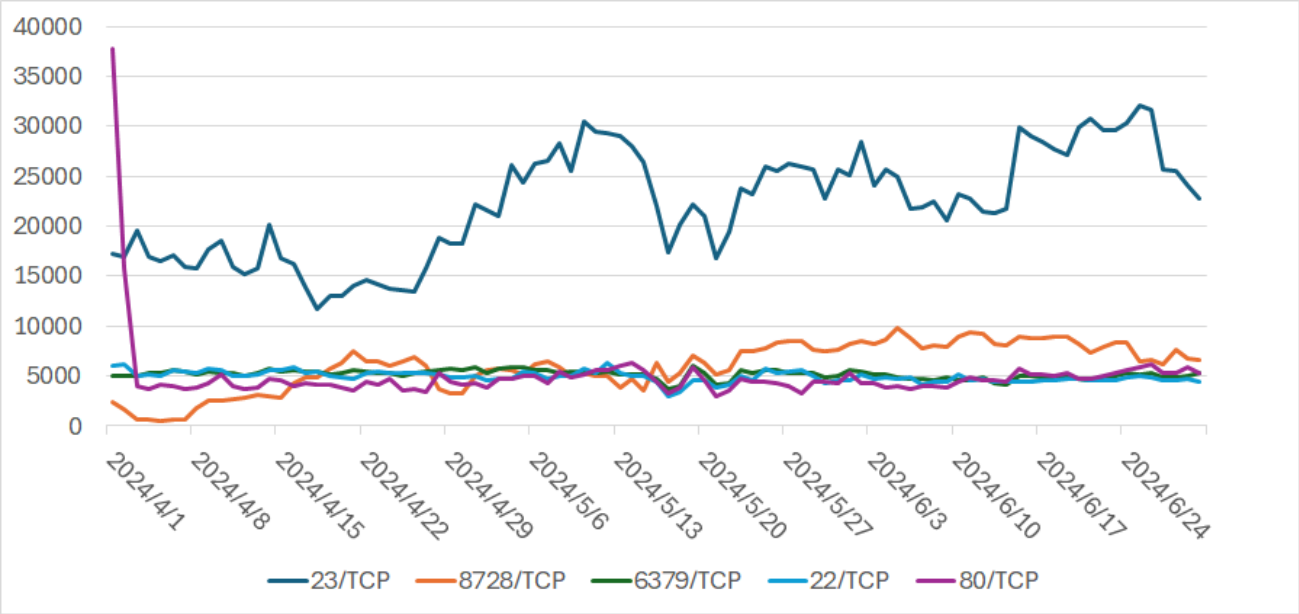
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that 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	9
3	redis (6379/TCP)	2
4	http (80/TCP)	4
5	ssh (22/TCP)	3

*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 packets observed for the top 5 services scanned listed in [Table 1] are shown in [Figure 1].



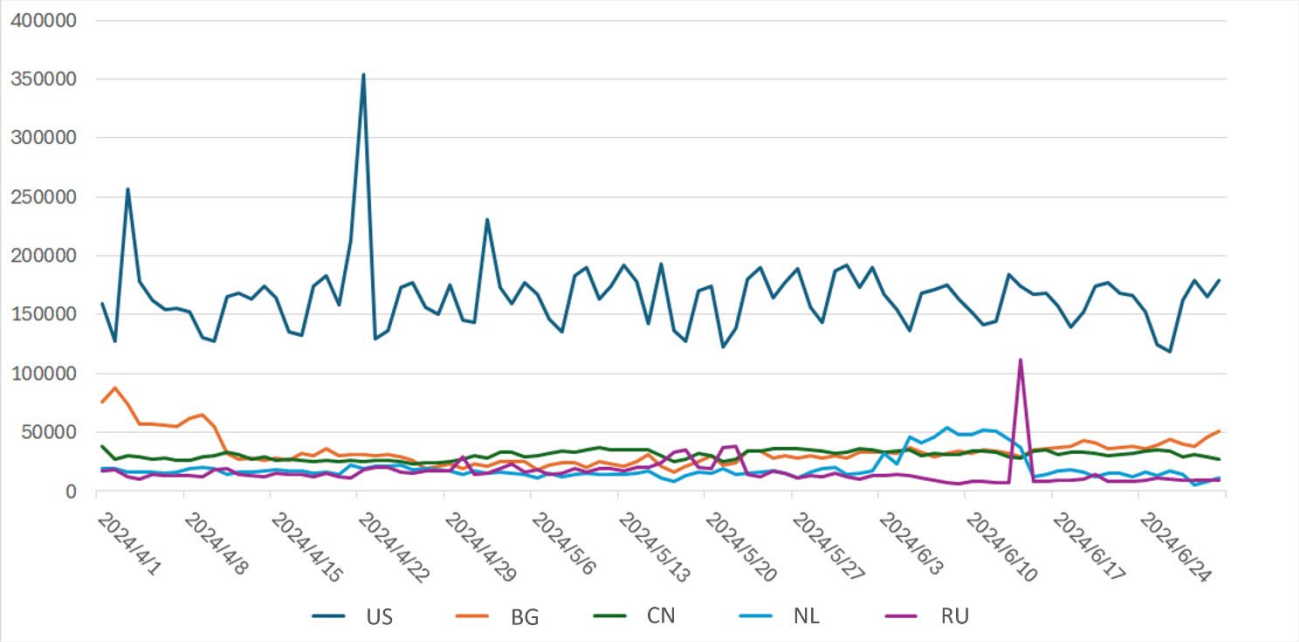
[Figure 1: Number of packets observed at top 5 destination ports from April through June 2024]

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 firth places were redis (6379/TCP), http (80/TCP) and ssh (22/TCP). 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	4
4	Netherlands	3
5	Russia	5

The numbers of packets sent from the source regions listed in [Table 2] are shown in [Figure 2].

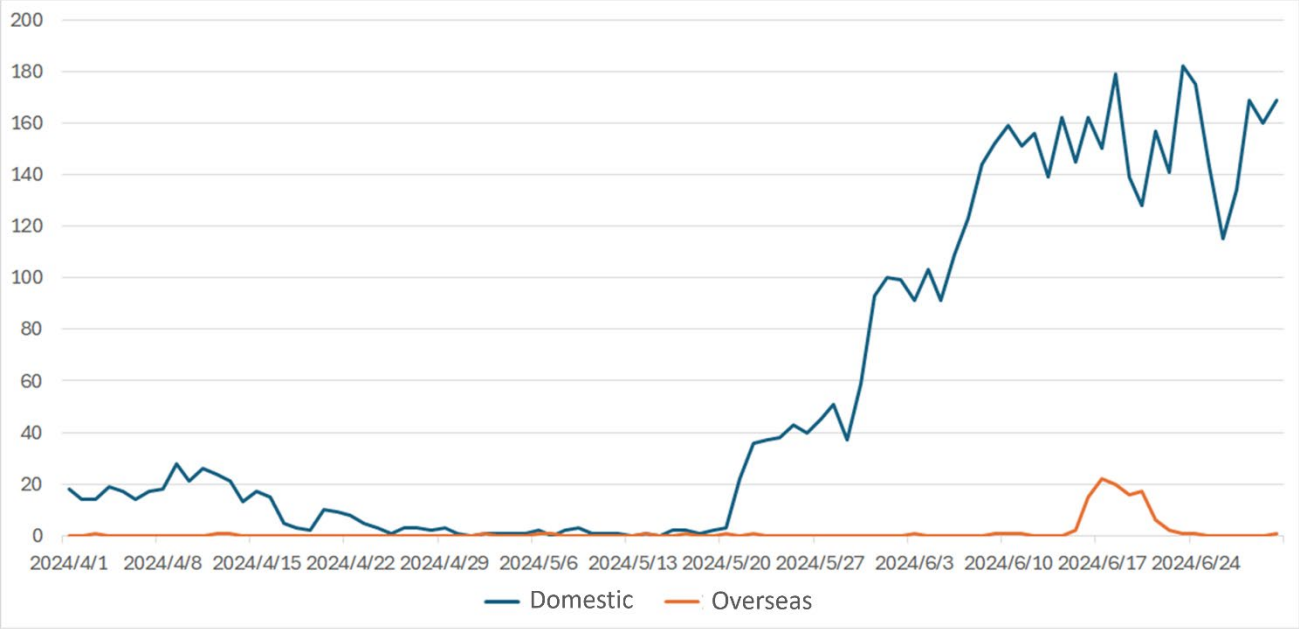


[Figure 2: Number of observed packets of the top 5 source regions from April through June 2024]

The USA stayed at the top, followed by Bulgaria. Although the Netherlands saw a temporary surge in the middle of June, otherwise it remained below China in the number of packets observed, making China the third largest source region. As for other regions, there was no change in particular worth noting. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

2. Number of Telnet scans that have a specific TCP parameter and originate from IP addresses in Japan

This chapter will discuss trends in Telnet scans that have a specific parameter and originate from IP addresses in Japan. From around May 20, the number of sources of scans targeting telnet (23/TCP) increased in Japan. While similar scans were temporarily observed overseas around June 17, they were not seen during other periods (Figure 3).



[Figure 3: Sources of packets with a window size of 5656]

These scan packets did not have characteristics indicating Mirai-derived packets but were distinguished by the fact that their window size, which is a TCP parameter, was 5656.

Meanwhile, most scan sources did not allow identifying models via access to http, https, etc. Presumably, this was because the devices that were scan sources rebooted due to high load caused by malware or for other reasons, and their IP addresses at the time of investigation differed from those at the time of scan, which prevented them from being tracked.

Although models could not be identified in most cases, some scan sources were found to be broadband routers from Japanese manufacturers, and a number of products and firmware versions suspected of involvement were identified. Scans from the same IP address last only for a day or two, but this is probably because the devices are assigned with different IP addresses after reboot.

Based on these observations, JPCERT/CC infers the presence of active botnet campaigns using malware other than Mirai, and that they target the routers of a specific Japanese vendor. Details will not be provided here, but as stated in "3. Request from JPCERT/CC," information about observed scans has been shared with Internet service providers and product developers.

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 [April 1, 2024 - June 30, 2024]

- First version issued: September 5, 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