JPCERT/CC Internet Threat Monitoring Report

January 1, 2024 ～ March 31, 2024

JPCERT Coordination Center

May 2, 2024

JPCERT CC®

Table of Contents

1. Overview 3

2. Observation of scan packets originating in Japan 5

3. Request from JPCERT/CC 7

4. References 7

1. Overview

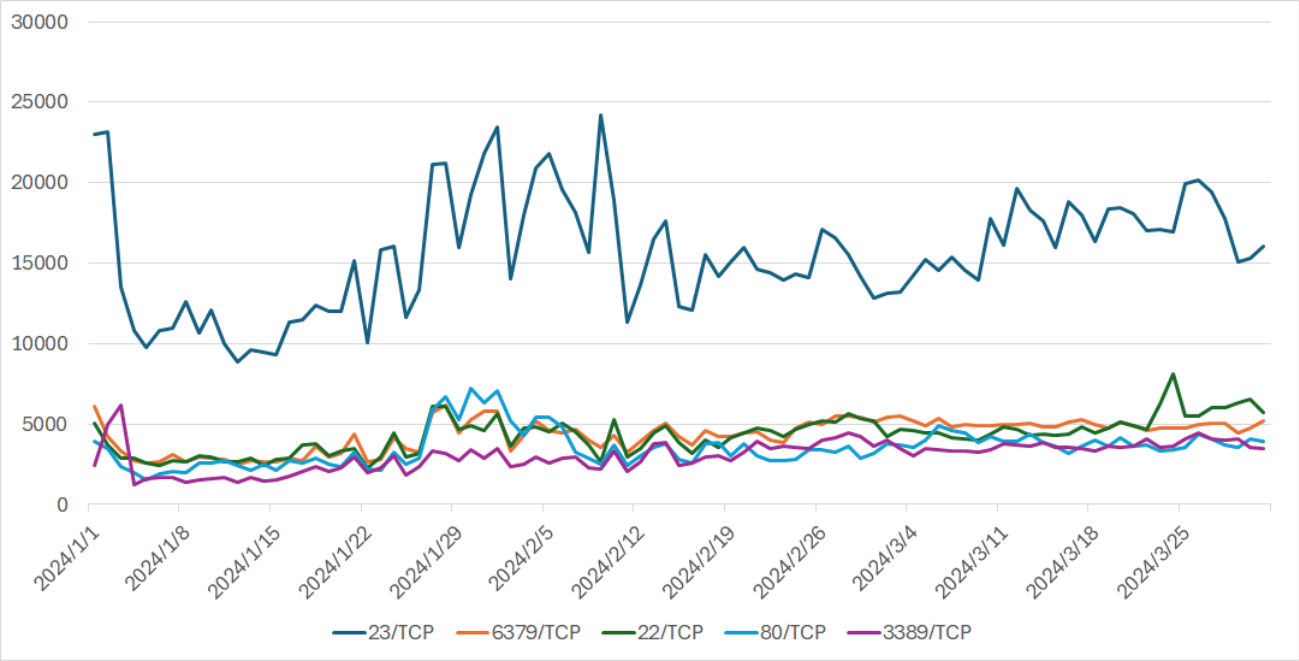
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that 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	redis (6379/TCP)	2
3	ssh (22/TCP)	3
4	http (80/TCP)	5
5	rdp (3389/TCP)	7

*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].



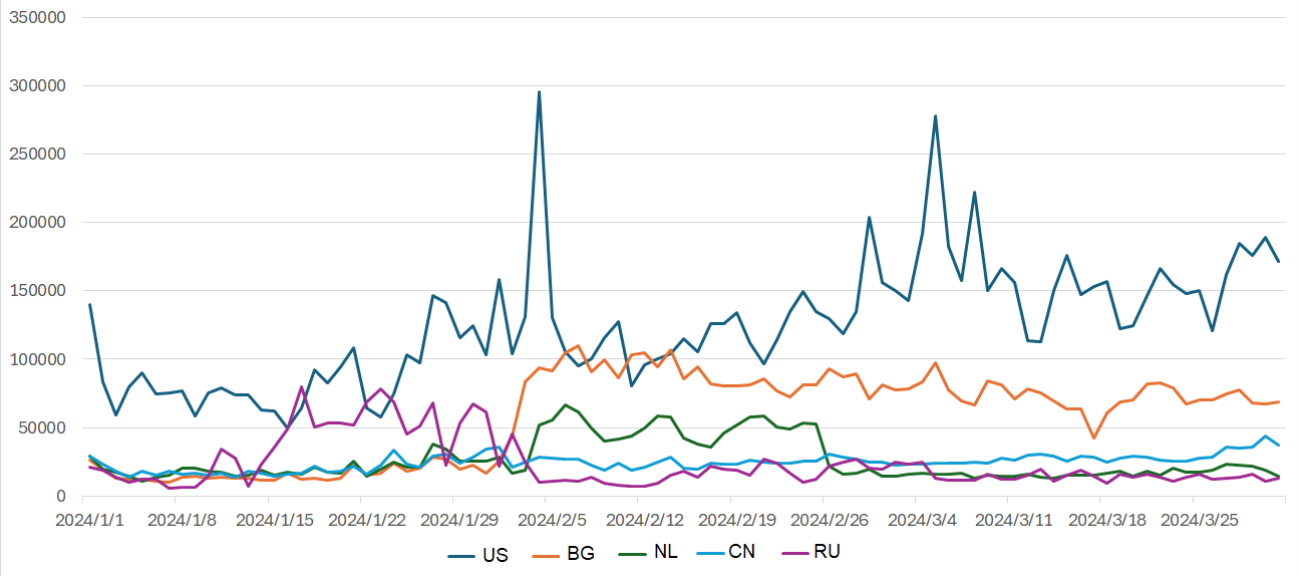
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2024]

The service most frequently scanned this quarter was telnet (23/TCP). The second and third places in the ranking remained unchanged. The fourth place was http (80/TCP), and the fifth place rdp (3389/TCP). These changes in the ranking were due to a significant drop in scans targeting http-alt (8080/TCP) and ICMP, while the numbers of scans for http and rdp remained roughly unchanged from the previous quarter. 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	5
3	Netherlands	4
4	China	2
5	Russia	6

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

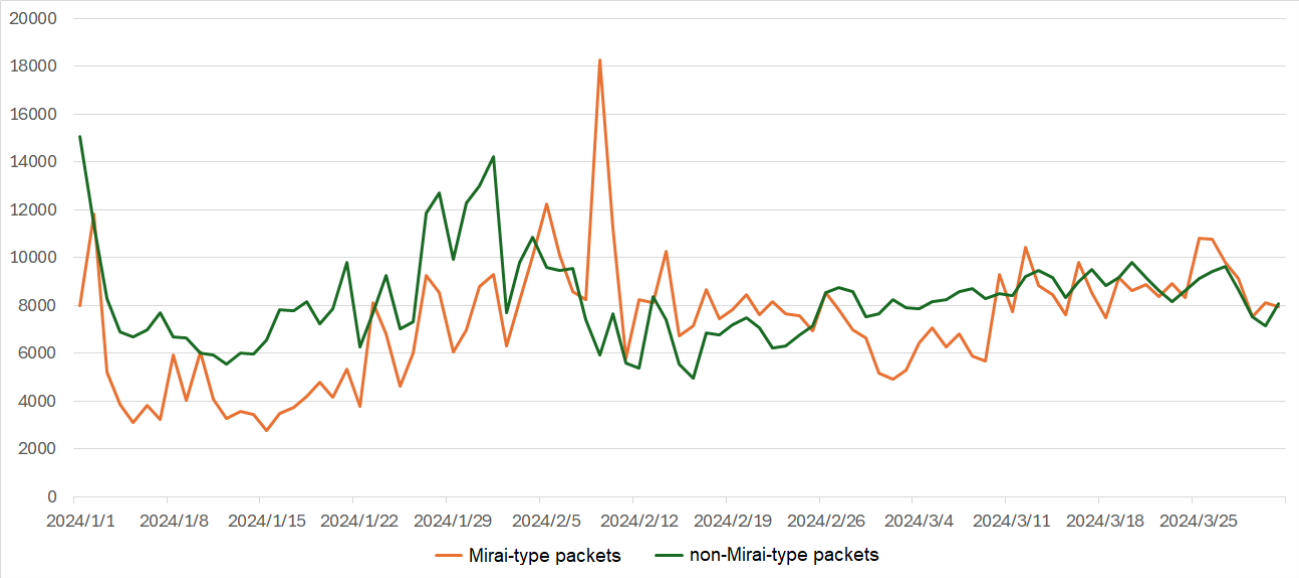


[Figure 2: Number of observed packets of the top 5 source regions from January through March 2024]

The USA stayed at the top. Bulgaria climbed to second place due to an increase in the number of packets seen since early February. The Netherlands also saw a temporary increase from early to late February, moving it up to third place. 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. Observation of scan packets originating in Japan

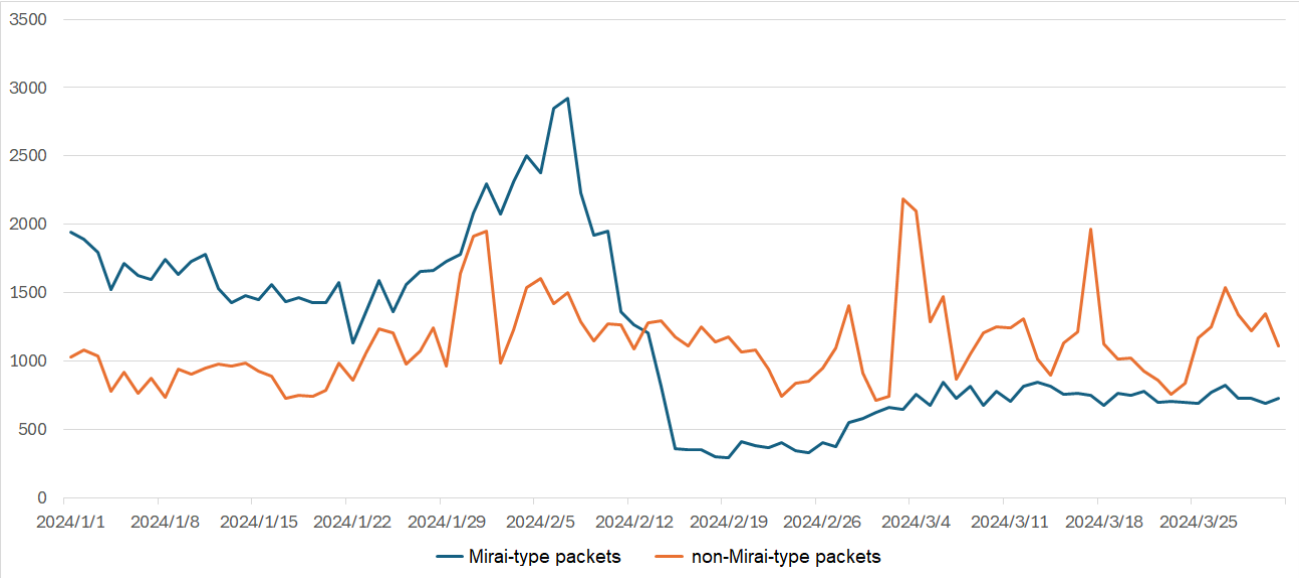
This chapter will discuss recent trends in scans targeting Telnet. Many of the scan packets targeting Telnet are derived from Mirai. Whether a scan packet is derived from Mirai ("Mirai-type packet") can be determined by checking for two characteristics: Packets scanning for various other services like 2323/TCP can be observed simultaneously from the same source, and the destination IP address matches the sequence number. Recently, scan packets that target Telnet but do not have Mirai characteristics ("non-Mirai-type packets") are seen frequently. For Mirai-type packets and non-Mirai-type packets observed by sensors in Japan, the numbers of packets originating overseas are shown in [Figure 3].



[Figure 3: Scans targeting Telnet between January and March 2024 (originating overseas)]

Although there are slight differences in the timing of changes between Mirai-type packets and non-Mirai-type packets, broadly speaking, both decreased temporarily in early January, before increasing from around January 16 to early February. Subsequently, major changes were no longer seen, with the two types of packets roughly converging in number toward the end of March. Since no signs of waning can be seen, both infection campaigns are assumed to be continuing overseas.

Next, the trend for scan packets originating in Japan is shown in [Figure 4].



[Figure 4: Scans targeting Telnet between January and March 2024 (originating domestic)]

At the beginning of January, twice as many Mirai-type packets as non-Mirai-type packets were observed. After growing for about a week into February, the number of Mirai-type packets fell sharply toward the end of February, then increased slightly again before more or less leveling off.
An investigation of the sources of Mirai-type packets and non-Mirai-type packets revealed that they were routers, digital video recorders, and other IoT products, although the products differed by timing. It is assumed that there is malware other than Mirai behind these packets, and activities to build botnets are increasing. In Japan, it seems that infection campaigns of malware other than Mirai are actively underway, gradually forming new unique botnets.

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) Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

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 2023.