# JPCERT/CC Internet Threat Monitoring Report

## April 1, 2023 - June 30, 2023

JPCERT Coordination Center

August 16, 2023

JPCERT CC®

## Table of Contents

## 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.

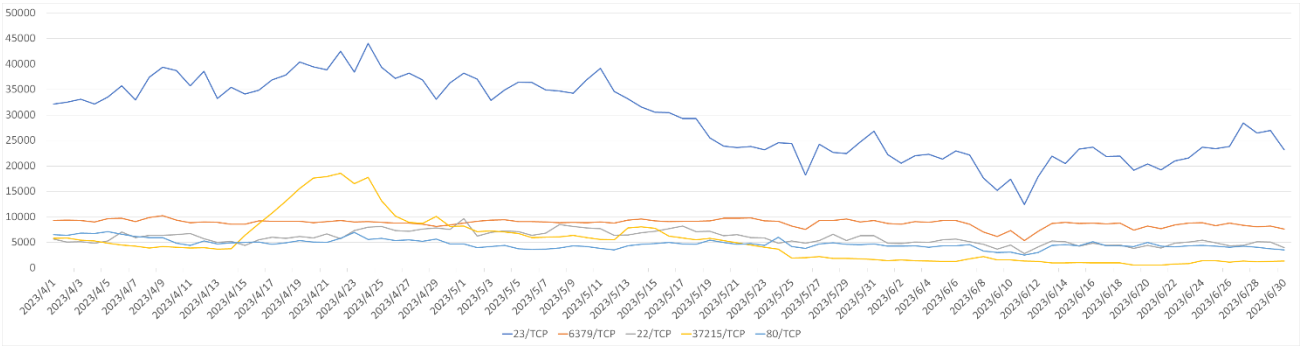
The top 5 services scanned in Japan during this quarter are shown in [Table 1].

[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) | 4 |
| 4 | 37215/TCP | 3 |
| 5 | http (80/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 packets observed for the top 5 services scanned listed in [Table 1] are shown in [Figure 1].



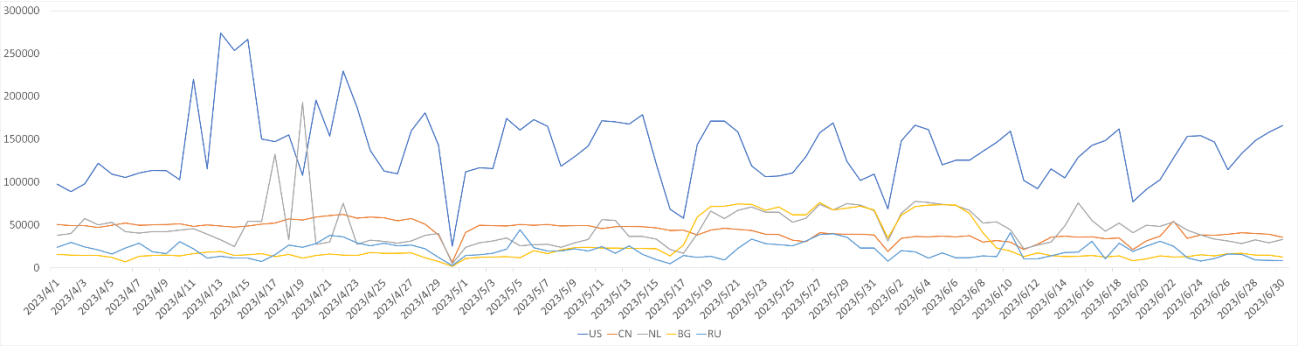

[Figure 1: Number of packets observed at top 5 destination ports from April through June 2023]

The service most frequently scanned this quarter was telnet (23/TCP), followed by redis (6379/TCP). Scanning of port 37215/TCP, the fourth on the list, can be assumed to be related to activities intended to spread Mirai infections. Mirai is a type of malware that scans for devices that it has a chance to infect, attacks such devices, and then uses them as a springboard for new attacks or scans. These scanning activities increased sharply from around April 14 to the end of April, then gradually decreased after a period of fluctuations. Packets with a distinctive characteristic of Mirai (i.e., initial sequence number = destination IP address) ("Mirai-type packets") are used to scan various services other than port 37215/TCP, and correlations were seen in the fluctuation patterns of the frequency of those scans. These observations are discussed in "2.1. Trends of Mirai-type packets in Japan."
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 | China | 2 |
| 3 | Netherlands | 3 |
| 4 | Bulgaria | 6 |
| 5 | Russia | 4 |

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 2023]

With regard to the source regions, it should be noted that the number of packets originating in Bulgaria temporarily increased from around May 18 to June 8, pushing it up to third place in the rankings. As for other 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. Events of Note

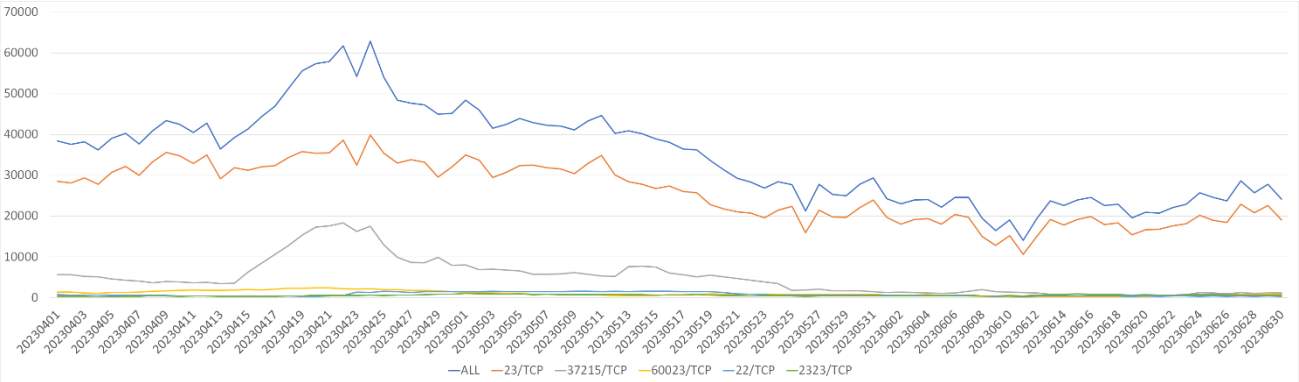
### 2.1. Trends of Mirai-type packets observed by sensors in Japan

This quarter, packets with characteristics apparently related to Mirai's infection campaign continued to be observed. JPCERT/CC found that there were 974 different destination port numbers. The ports scanned and their proportions are shown in [Table 3].

[Table 3: Ports scanned by Mirai-type packets and their proportions]

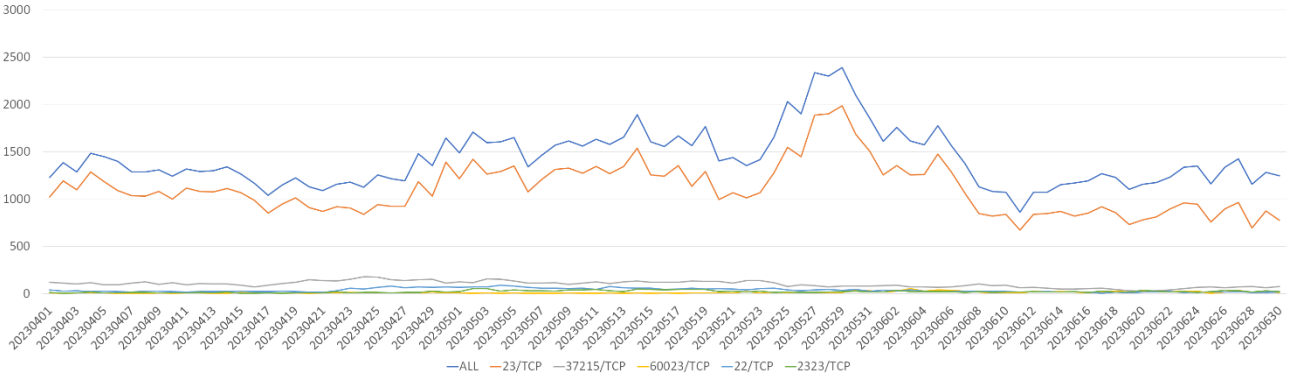
| Rank | Destination Port Numbers | Previous Quarter |
|---|---|---|
| 1 | 23/TCP | 74.08% |
| 2 | 37215/TCP | 14.27% |
| 3 | 60023/TCP | 3.01% |
| 4 | 22/TCP | 2.25% |
| 5 | 2323/TCP | 1.79% |
| 6 | 52869/TCP | 0.88% |
| 7 | 5555/TCP | 0.67% |
| 8 | 56575/TCP | 0.65% |
| 9 | 80/TCP | 0.51% |
| 10 | 2222/TCP | 0.38% |
| Not in the top 10 | | 1.51% |

Of the services scanned by Mirai-type packets, telnet (23/TCP) accounted for 74%. Marked changes were seen in the frequency of all service scans. Changes in the numbers of packets originating overseas and targeted to the destination port numbers shown in [Table 3] and the combined number of packets targeted to all the ports are shown in [Figure 3].




[Figure 3: Mirai-type packets originating overseas]

The number of packets targeted to port 37215/TCP started increasing from around April 14, and it has been decreasing since peaking out at around April 20. The number of packets targeted to port 60023/TCP also peaked out at around April 20, slowly decreasing afterward.
Next, changes in the numbers of Mirai-type scanning packets originating in Japan are shown in [Figure 4].




[Figure 4: Mirai-type packets originating in Japan]

By comparing scans originating overseas and those originating in Japan, the most frequently scanned service this quarter was telnet (23/TCP) in both cases. As for port 37215/TCP, while scans originating in Japan (see [Figure 4]) slightly increased in April, no notable changes were observed in scans originating overseas (see [Figure 3]), and both gradually declined subsequently.
The number of packets targeted to port 60023/TCP showed minor fluctuations in April, and they remain elevated since mid-May. These changes are believed to reflect the changing models of devices scanned as potential targets of attack.
As stated above, JPCERT/CC assumes that the attackers are scanning for devices and launching attacks to infect them with malware by using code derived from Mirai and changing the target devices. With this assumption, JPCERT/CC tried to analyze the temporal changes in the scanned services in an attempt to identify changes in the devices the attackers are targeting, but these changes could not be extrapolated from this analysis.
Nevertheless, attacks using Mirai derivatives are still carried out today, and various services are being scanned. To clarify the actual situation, JPCERT/CC investigated the source IP addresses in Japan to identify the types of devices involved in these scans. This investigation largely identified the models operating at some of the sources. These were old wireless LAN routers and digital video recorders with known vulnerabilities. With regard to the problematic devices identified, JPCERT/CC's incident handling team provided information to ISP's abuse contact and elsewhere, and requested them to ask users to take appropriate steps.

## 3. 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.