JPCERT/CC Internet Threat Monitoring Report

April 1, 2022 - June 30, 2022

JPCERT Coordination Center

July 28, 2022

JPCERT CC®

Table of Contents

1. Overview

JPCERT/CC has placed multiple sensors across the Internet for monitoring to continuously gather packets which are dispatched to indefinite nodes on the Internet. 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.

It is important that such monitoring is performed with a multidimensional perspective using multiple viewpoints. As such, JPCERT/CC works mainly with overseas National CSIRTs to deploy sensors at each organization and have them participate in the monitoring network.

Data collected through sensors around the world are analyzed, and if any problem is found, JPCERT/CC provides information to the National CSIRTs and other organizations in the relevant region and requests them to remedy the situation. Issues unique to Japan are addressed in the day -to-day operations of JPCERT/CC. This report will mainly show the analysis results of packets observed by sensors located in Japan during this quarter.

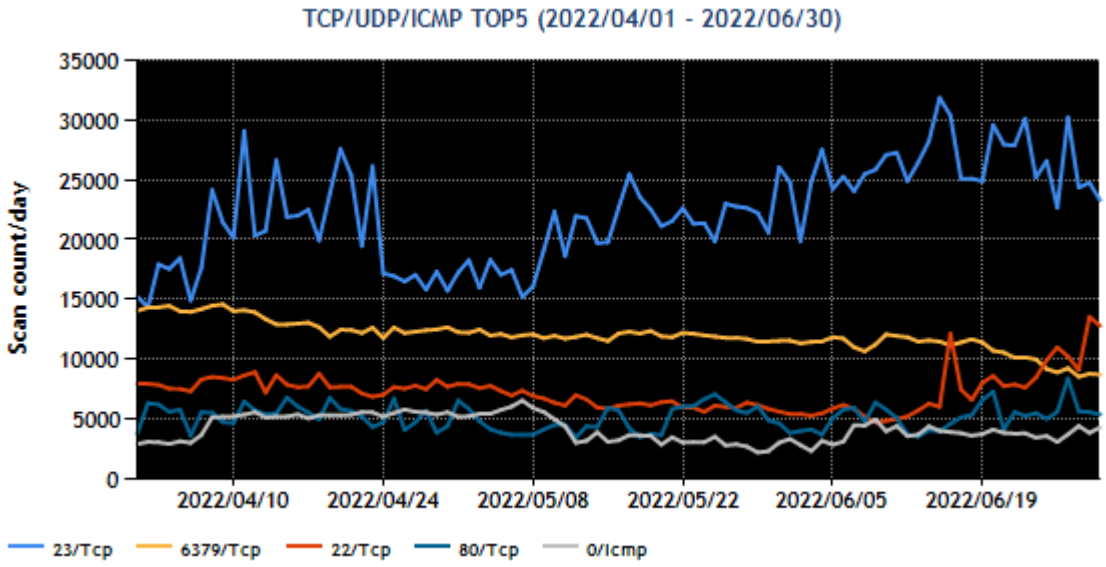
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP(telnet)	2
2	6379/TCP(redis)	1
3	22/TCP(ssh)	4
4	80/TCP (http)	6
5	Icmp	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 number of packets observed for each destination port number listed in [Chart 1]is shown in [Figure 1].



[Figure 1: Number of packets observed at top 5 destination ports from April through June 2022]

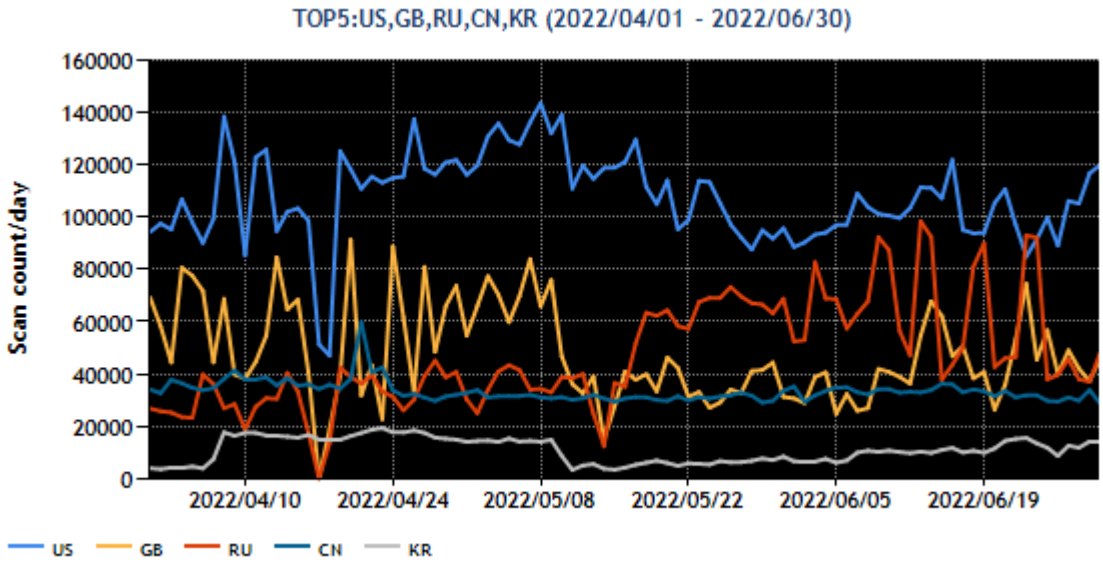
Port 23/TCP (telnet) received the greatest number of packets. Short periods of fluctuation were repeatedly observed between April and May. From around May 8, the weekly average numbers of packets kept increasing as the fluctuation continued. On the other hand, the number of packets targeted to port 6379/TCP appeared to decrease gradually during this quarter.

Next, the top 5 regions in the number of packets observed in Japan during this quarter, identified based on source IP addresses, are listed in [Chart 2].

[Chart 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	USA	1
2	Great Britain	2
3	Russia	4
4	China	3
5	Koria	6

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



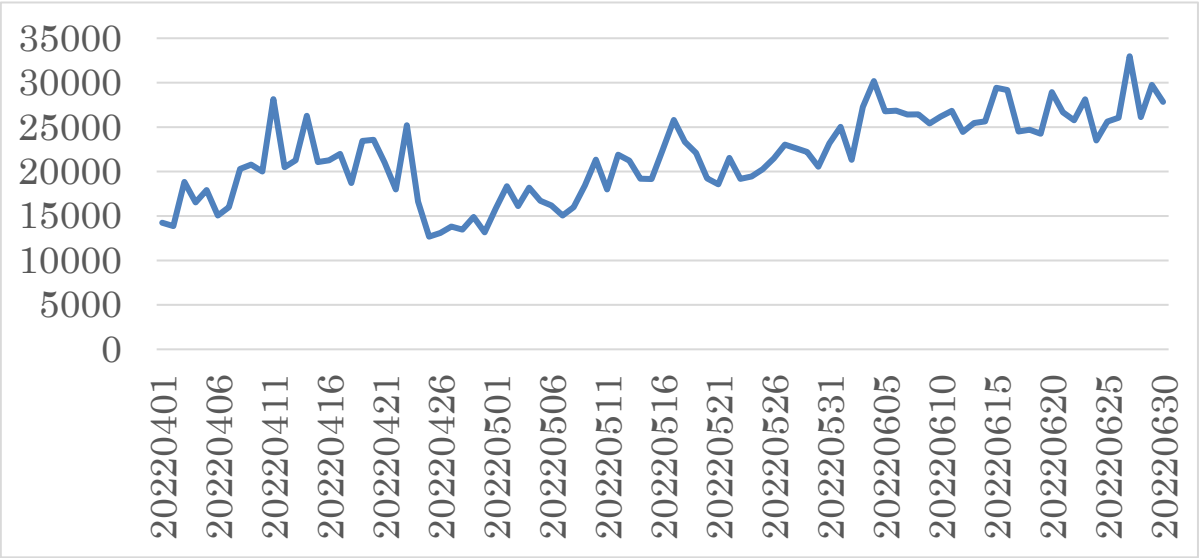
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2022]

Russia saw the number of packets go up from around May 18 and changed places with China in the rankings. Also, there was a temporary rise in the number of packets originating in South Korea between April and around May 6. While the number of packets later declined for a moment, it slowly increased through late June, ending up fifth in the rankings for this quarter.

2. Events of Note

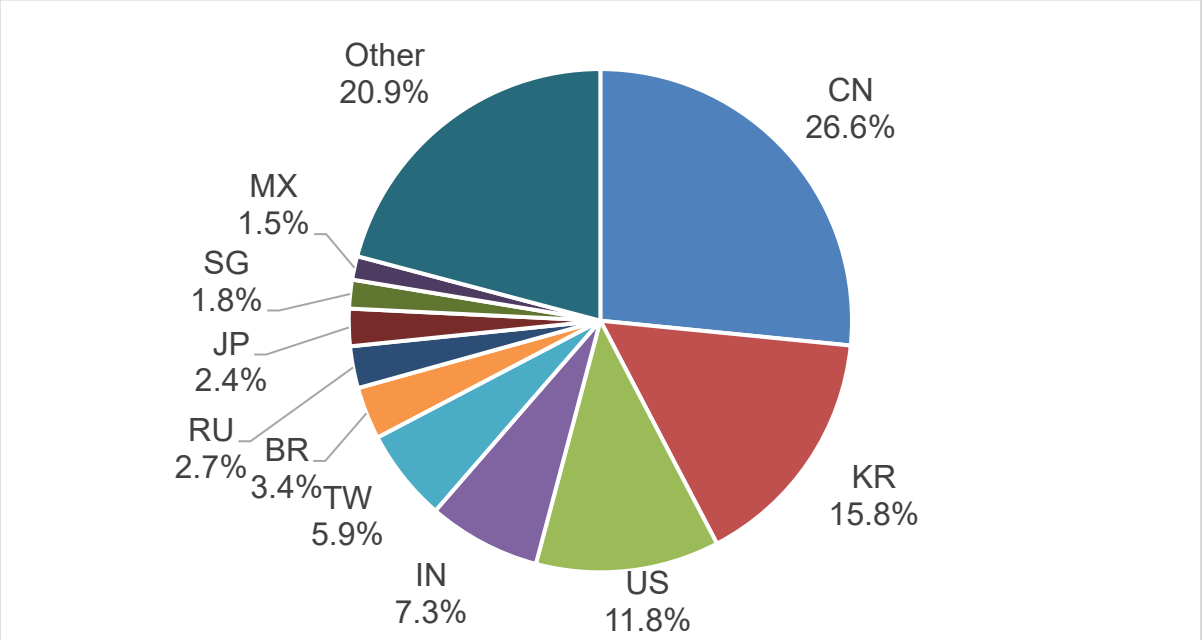
2.1. Increase in the number of packets with a distinctive feature of Mirai apparently sent from IoT devices

From early April to around April 25, there was a temporary rise in the number of packets with a distinctive characteristic of Mirai (i.e., initial sequence number = destination IP address). Later, a gradual increase in the number of these Mirai packets was observed from May 8 through the end of June. [Figure 3]



[Figure 3: Number of Mirai packets]

The breakdown of Mirai packets by source region for this quarter is shown in [Figure 4].

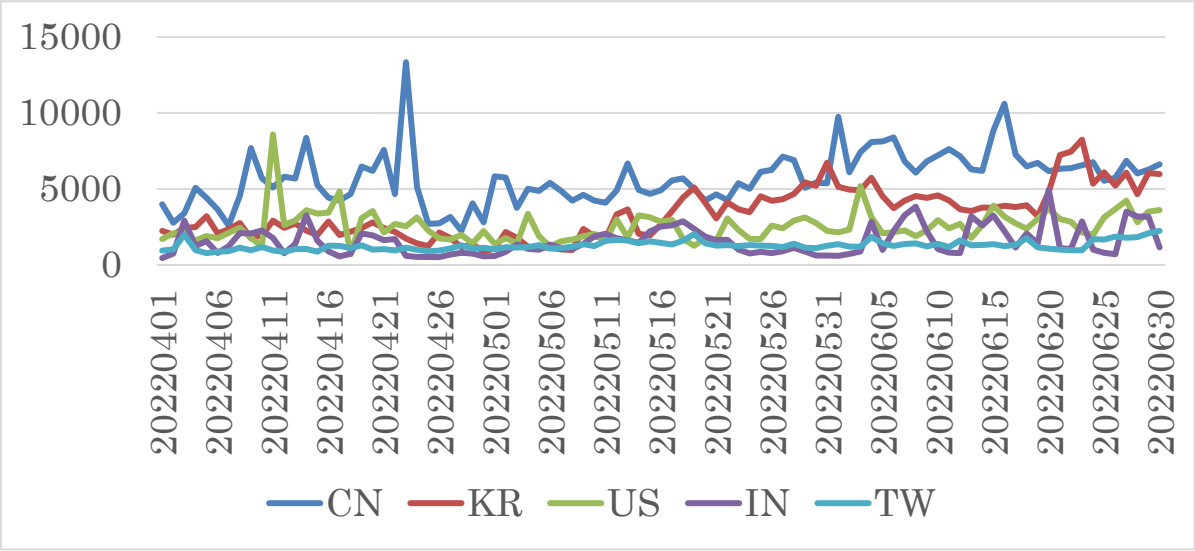


[Figure 4: Percentage of the total number of source addresses for Mirai packets]

When the total numbers of source addresses for Mirai packets and all observed packets are compared by regions, China, the United States, and South Korea ranked high for both, while some of the other regions such as India and Taiwan stood out only in the latter. Japan ranked eighth for the former and 19th for the latter.

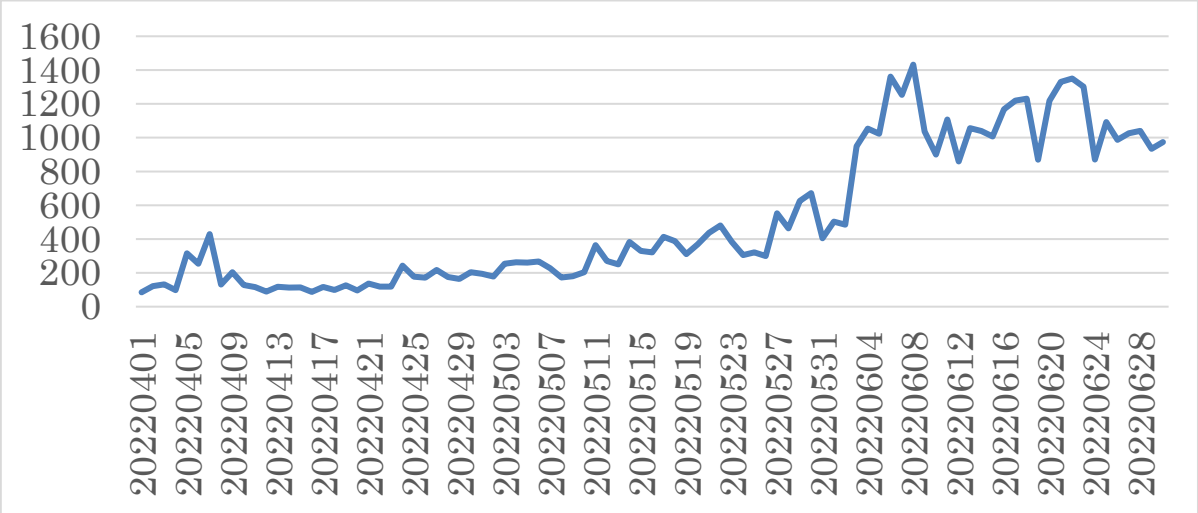
[Figure 5] shows the daily shifts in the numbers of observed Mirai packets by source region. It can be seen

that the timing of fluctuation differs by region. For example, China observed a large number of packets between early April and April 25. Then later, the number of packets increased gradually from May to around the mid-June. In South Korea, there were no major fluctuations in April, but there was a sharp increase starting from around May 11, more than doubling from early April. In Taiwan, the number increased significantly from around June 26.



[Figure 5: Number of packets by source region (top5)]

Next, trends in the numbers of Mirai packets originating in Japan are shown in [Figure 6].



[Figure 6: Number of packets by source region (Japan)]

After a temporary spike in early April, the number remained low for a while before trending upward(2) from

around April 25. In particular, there was a sharp growth[3] in June, marking a fivefold increase compared to early April.
JPCERT/CC investigated the source nodes for Japan and the top 5 source regions of these packets with SHODAN and other tools. According to the information obtained, JPCERT/CC found that CCTV video recorders seemingly accounted for about 60% of the source IP addresses in Japan, South Korea, and Taiwan. As for China and the United States, compromised Linux servers accounted for most, and CCTV video recorders made up only a small portion.

At present, a number of scenarios can be inferred for the possible attacks that the CCTV video recorders were subjected to, causing them to be infected with malware and send packets, but we have yet to determine the likely cause.

In Japan, we have been providing information to operators managing the source IP addresses of Mirai packets in an attempt to obtain information about device models and attack flows.
We are also encouraging Japanese businesses that sell and install the identified CCTV video recorders to share information with relevant organizations with the aim of improving security related to the use of the products.
As for devices that will be newly installed, we recommend the use of CCTV video recorders certified under RBSS (Recognition of Better Security System)[4], a standard developed by the Japan Security Systems Association to specify the devices and capabilities required for security systems. In addition, users are advised to change the default password of these devices, regularly update the firmware, and take proper security measures to restrict access.

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

(2)NICTER Analysis Team Twitter July 8, 2022
https://twitter.com/nicter_jp/status/1545264938306146306

(3)NICTER Analysis Team Twitter June 9, 2022
https://twitter.com/nicter_jp/status/1534722508729229312

(4)JAPAN SECURITY SYSTEMS ASSOCIATION
https://www.ssaj.or.jp/rbss/index.html

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 2022.