JPCERT/CC Internet Threat Monitoring Report

April 1, 2021 ～ June 30 , 2021

JPCERT Coordination Center

July 26, 2021

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 aboutvulnerabilities, 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.

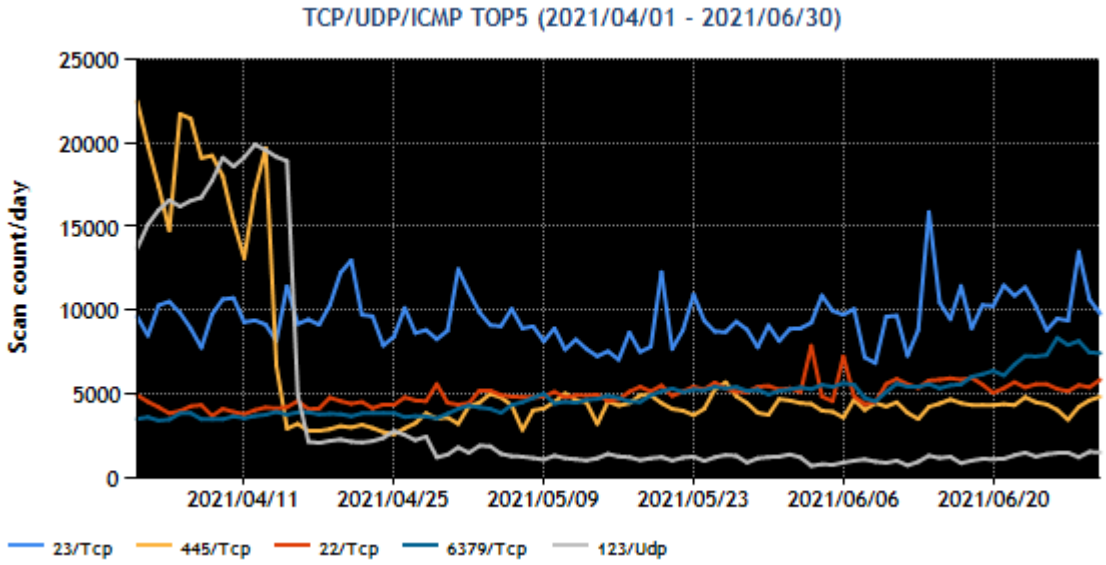
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1 : Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	445/TCP (microsoft-ds)	1
2	23/TCP (telnet)	2
3	123/UDP (ntp)	3
4	22/TCP (ssh)	4
5	6379/TCP	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 October through December 2020]

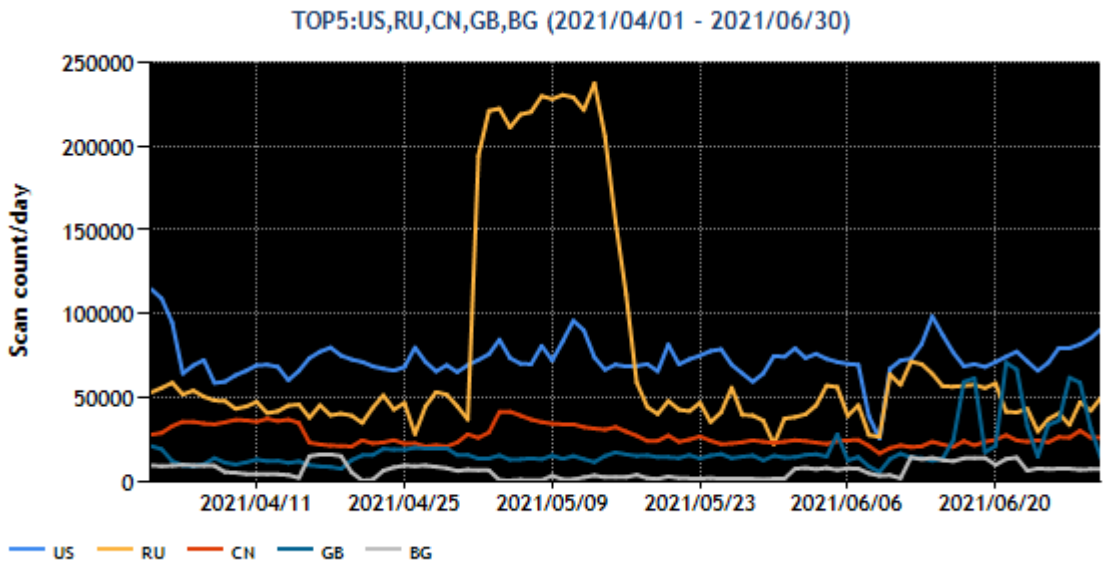
Port 23/TCP (telnet) received the greatest number of packets. The number of packets targeted to port 445/TCP (microsoft-ds) and port 123/UDP (ntp) fell sharply on April 13 and April 16, respectively. Among packets originating in Japan, a considerable number of packets targeted to port 9530/TCP (18th overall, 3rd in Japan) were observed during the quarter, although it did not rank among the top 5. This is discussed further in 2.1.

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	Russia	2
3	China	4
4	Great Britain	3
5	Bulgaria	9

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



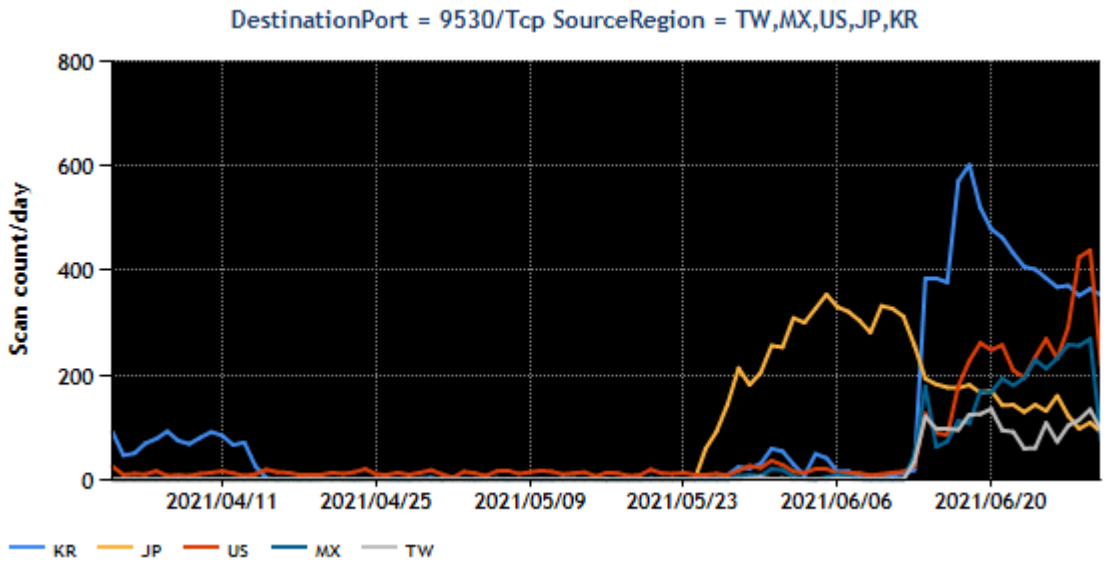
[Figure 2 : Number of observed packets of the top 5 source regions from April through June 2021]

The top source region for the number of packets observed this quarter was the USA. Russia, which ranked 2nd, saw more than a fourfold increase in the number of packets observed during the 2 weeks from May 2. This temporary rise was due to packets sent from a small number of IP addresses in Russia. Packets were observed for various ports, not only to those used for services in general. The United Kingdom (GB), ranking 4th, went through a period of wild fluctuations in June.

2. Events of Note

2.1. Increase in the number of packets targeted to port 9530/TCP

There was a temporary surge in the number of packets targeted to port 9530/TCP originating in Japan from around May 23, 2021 (Figure 3). From around June 14, many packets originating in South Korea, the USA, Mexico and Taiwan were observed. Japan ranked second in the number of packets observed as a source region during this quarter.



[Figure 3: Number of observed packets targeted to port 9530/TCP (originating in Japan)]

JPCERT/CC investigated about 1,250 source IP addresses in Japan for the packets targeted to port 9530/TCP that were observed by SHODAN and other means between May 22 and June 30. As a result, characteristics of the Logitec broadband routers[(2)] were identified, and it was found that the routers at about 80% of the sources were connected to the Internet with the vulnerability (CVE-2014-8361) left unaddressed.

As part of incident response activities, JPCERT/CC notified the findings to administrators who manage the source IP addresses of the packets targeted to port 9530/TCP in Japan. Some of the administrators responded with a message similar to the following.

> "We contacted the users and found that they were using a Logitec router. As this was a model with a vulnerability that needed to be addressed, we asked them to purchase a new router, and they later notified us that they had arranged for a new one."

JPCERT/CC is contacting sources of packets observed with sensors that apparently have not addressed the vulnerability (CVE-2014-8361). Users of these routers are asked to cooperate by updating the firmware

or taking other security measures when contacted by JPCERT/CC or an ISP.

Sources of packets overseas were cameras, routers, or other types of devices. There is not much correlation between their distribution and region, therefore it is assumed that such devices are widely used in certain regions overseas. JPCERT/CC made preparations to provide information to National CSIRTs that correspond to each source with the expectation that they will conduct investigations and take appropriate steps. Packets targeted to port 9530/TCP are still observed as of July, and thus JPCERT/CC will continue to investigate them.

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) JPCERT/CC Internet Threat Monitoring Report [January 1, 2021 - March 31 , 2021]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2020Q4_en.pdf

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 2021.