JPCERT/CC Internet Threat Monitoring Report

[July 1, 2021 - September 30, 2021]

JPCERT Coordination Center

October 19, 2021

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.

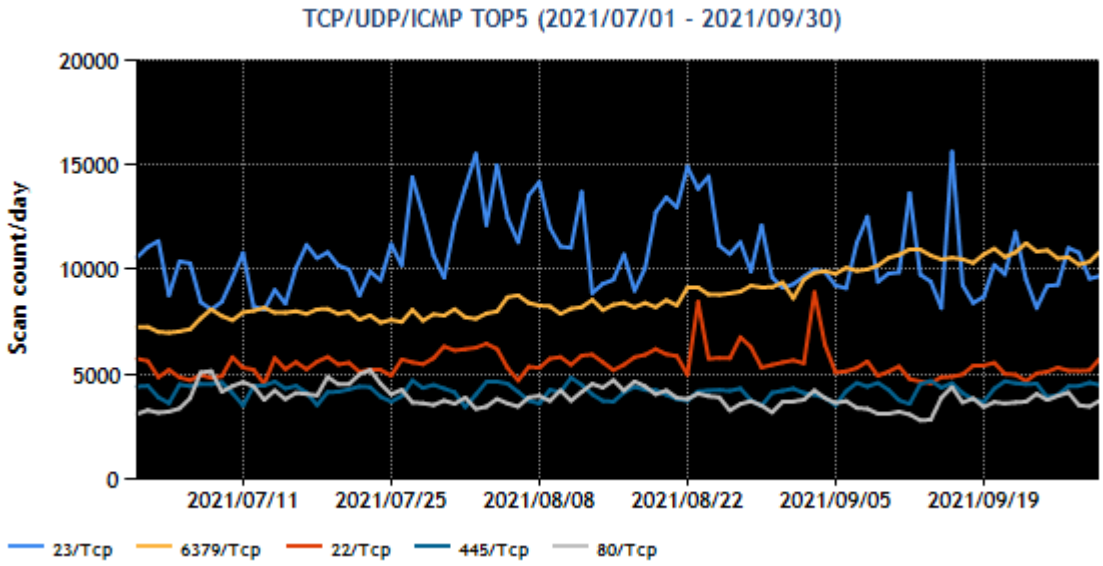
The top 5 destination port numbers for which packets were observed in Japan are listed in[Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP（telnet）	2
2	6379/TCP（redis）	5
3	22/TCP（ssh）	4
4	445/TCP（microsoft-ds）	1
5	80/TCP（http）	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 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 July through September 2021]

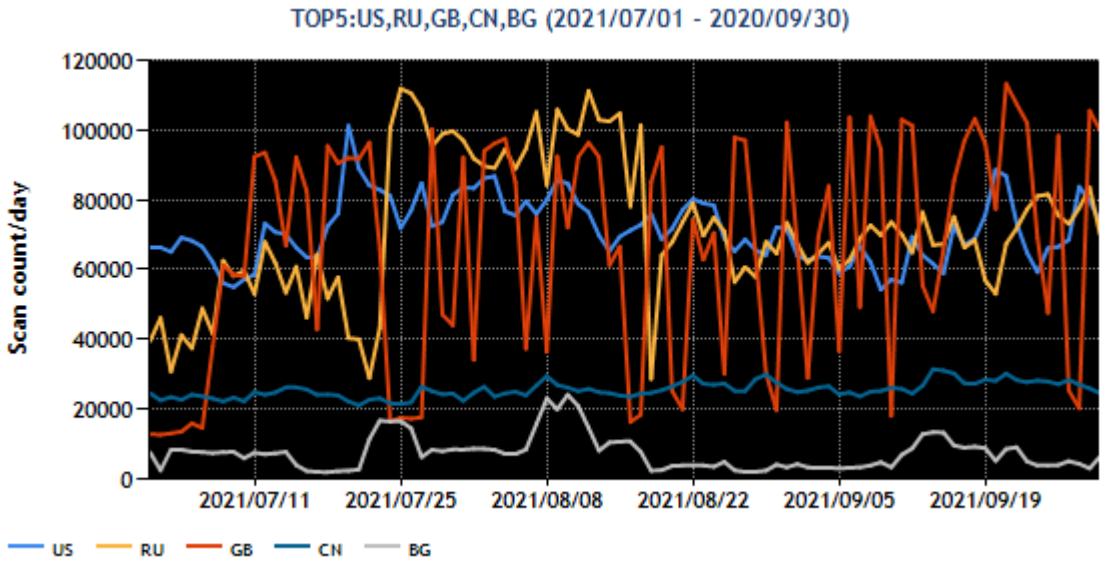
Port 23/TCP (telnet) received the greatest number of packets. There was a gradual rise in the number of packets targeted to port 6379/TCP. This will be discussed further in 2.1.

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]. While there were no significant changes in the rankings, sudden changes were seen for the United Kingdom (GB), resulting in a shift in its ranking.

[Chart 2 : Top 5 source regions]

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

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



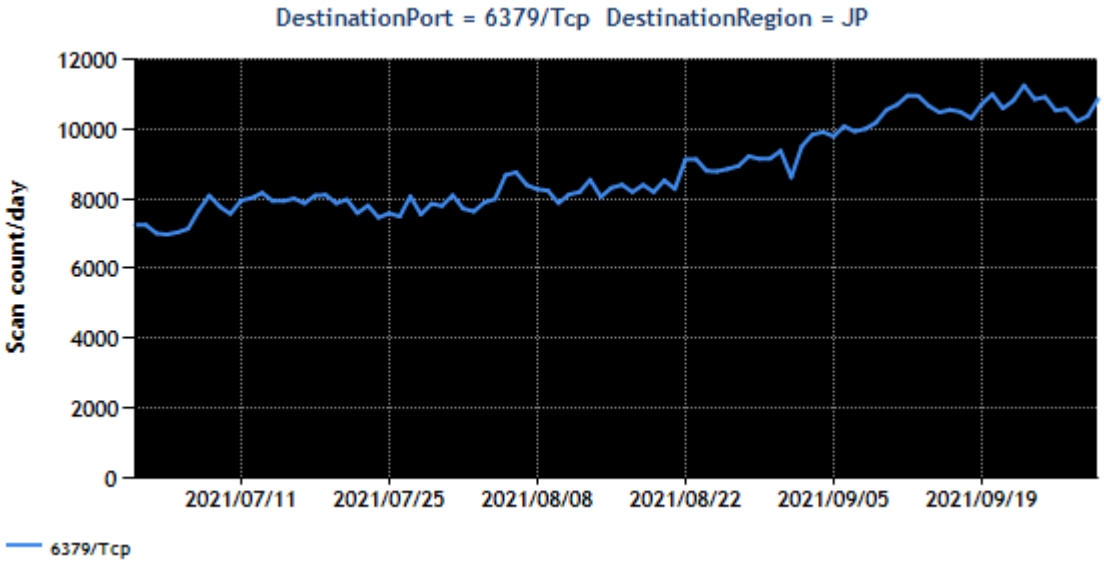
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2021]

The top source region for the number of packets observed this quarter was the USA, followed by Russia. The United Kingdom, where temporary fluctuations in the number of packets were observed repeatedly, changed places with China to rank third. Packets from China and Bulgaria continue to be observed as well.

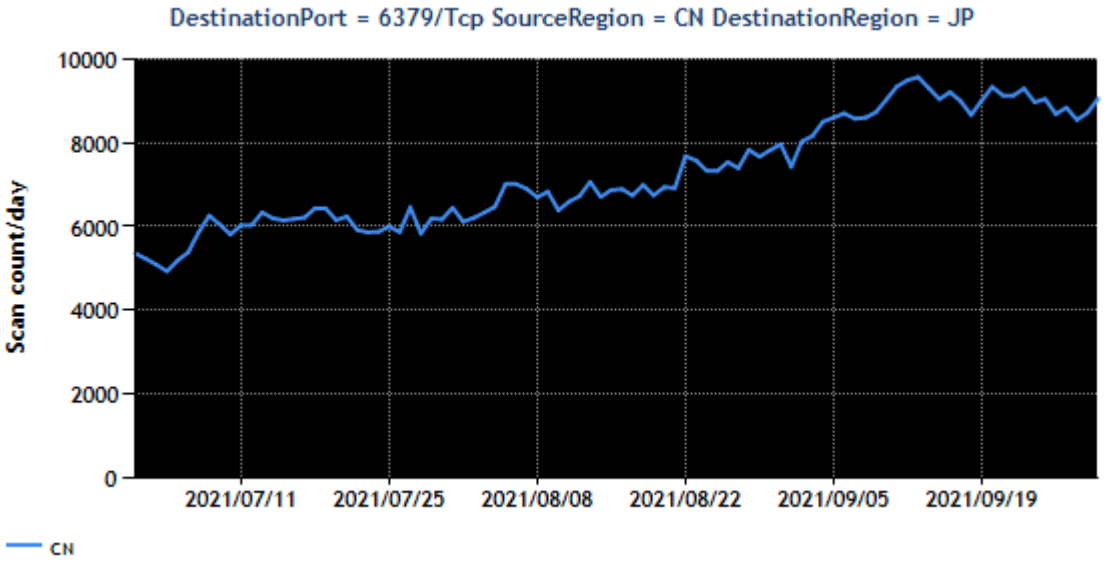
2. Events of Note

2.1. Increase in the number of packets targeted to port 6379/TCP

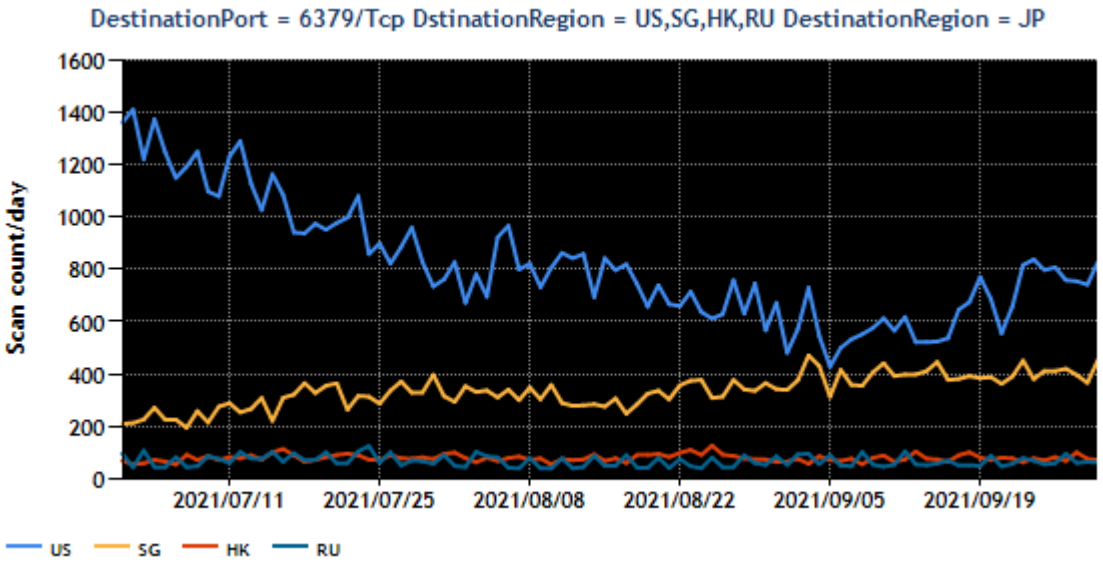
Packets targeted to port 6379/TCP (Redis) were observed (Figure 3) throughout this quarter. 6379/TCP is a port number that is often used as a listening port for Redis in-memory databases.
Over 80% of the packets targeted to port 6379/TCP originate in China, with regions like the USA, Singapore, Hong Kong and Russia accounting for the rest of the observed packets (Figure 4,Figure 5).



[Figure 3: Number of observed packets targeted to port 6379/TCP]



[Figure 4: Number of observed packets originating in China and targeted to port 6379/TCP]



[Figure 5: Number of observed packets originating in the top 2 to 4 regions excluding China and targeted to port 6379/TCP]

The number of packets targeted to port 6379/TCP from China is gradually increasing, and the number of packets at the end of this quarter was about 1.5 times as many as on the first day of the quarter. Packets originating in Singapore also showed a similar rate of increase. Packets originating in other regions did not show significant changes throughout the quarter. This quarter, JPCERT/CC observed packets targeted to port 6379/TCP sent from about 20 IP addresses in Japan. Shortly after the information was provided to operators managing the relevant IP addresses, JPCERT/CC confirmed that the packets were no longer being sent.

As for some of the sources where packets targeted to port 6379/TCP were observed with TSUBAME sensors, JPCERT/CC confirmed that they were sending suspicious requests based on observation with a honeypot on a Redis server. JPCERT/CC checked the payload and found code for breaching authentication, stealing information, obtaining external files, and manipulating operating systems.

JPCERT/CC recommends those operating Redis servers to check whether the servers have access control and proper authentication set up, and also to regularly check access logs as part of their operation. JPCERT/CC checked the packet sources using the data of SHODAN and other scan data service providers but found no common elements, such as the use of specific operating systems or software. If the packets targeted to port 6379/TCP were sent from hosts infected with malware as a result of an attack targeting certain vulnerabilities, there should be an increase in the number of hosts sending packets targeted to port 6379/TCP in various regions including Japan, but no such changes were observed. For this reason, the background to this event can be narrowed down to cases where a server was hacked and is being used as a springboard for attacks, or cases where an attacker is preparing infrastructure, rather than a malware

infection. Beyond that, the cause is unclear at the moment. In any case, it is important for server administrators to see if there are any unintended accesses to their servers and take proper countermeasures.

3. Events of Note

(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 2021.