JPCERT/CC Internet Threat Monitoring Report

October 1, 2021 ～ December 31, 2021

JPCERT Coordination Center
January 25, 2022

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.

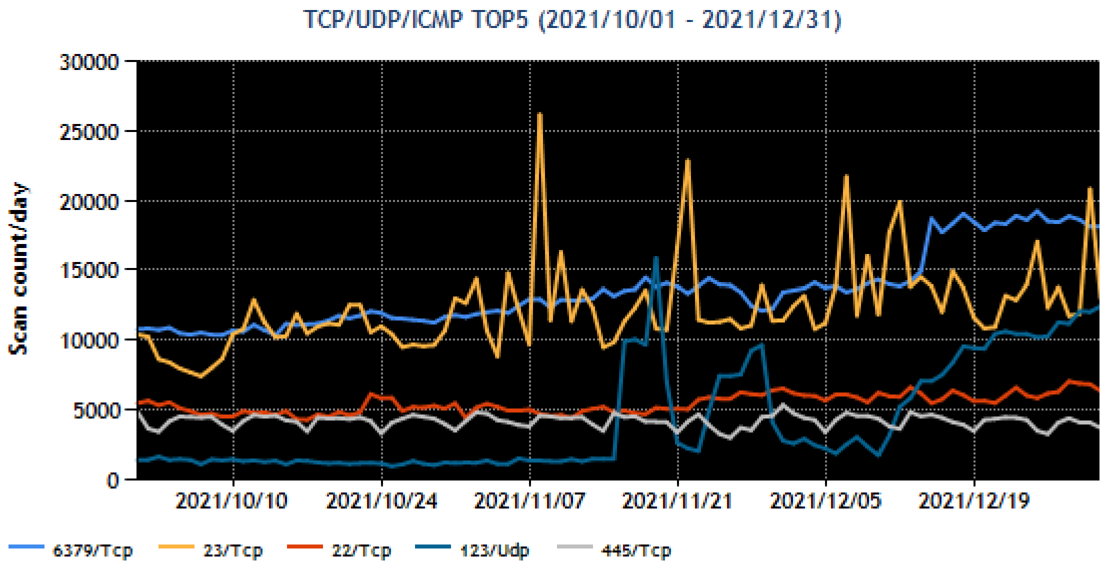
The top 5 destination port numbers for which packets were observed in Japan are listed in[Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	6379/TCP (redis)	2
2	23/TCP (telnet)	1
3	22/TCP (ssh)	3
4	123/UDP (ntp)	Not in top 5
5	445/TCP (microsoft-ds)	4

*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 2021]

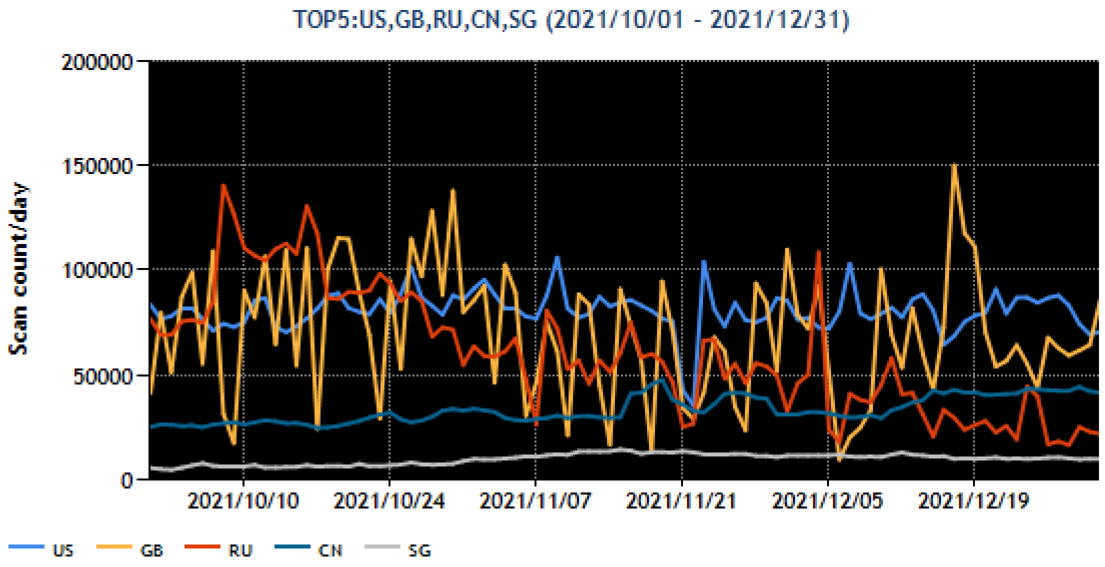
Port 6379/TCP (Redis) received the greatest number of packets. The number of packets targeted to port 6379/TCP increased by about 1.8 times during the period. These packets will be discussed further in 2.1. Port 23/TCP, which received the second most packets, saw a number of brief fluctuations. This was probably due to repeated attacks attempting to infect IoT and other devices with malware, causing the number of packets observed to increase for port 23/TCP.

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	3
3	Russia	2
4	China	4
5	Singapore	9

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



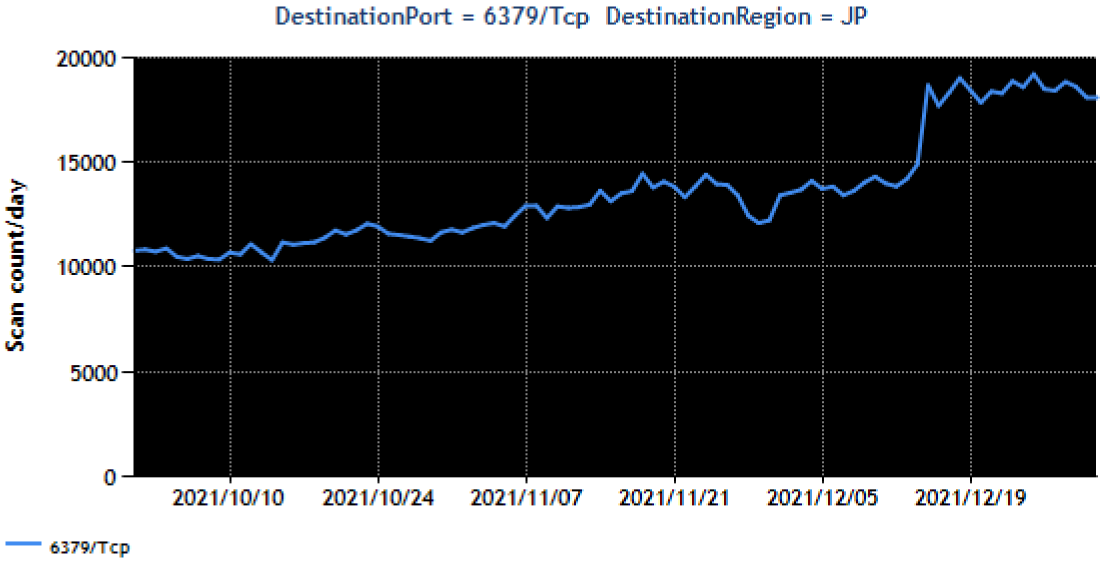
[Figure 2: Number of observed packets of the top 5 source regions from October through December 2021]

The United Kingdom (GB) saw the number of packets go up and changed places with Russia in the rankings. Another change in the rankings involved Singapore rising to fifth place due to an increase in packets targeted to port 6379/TCP.

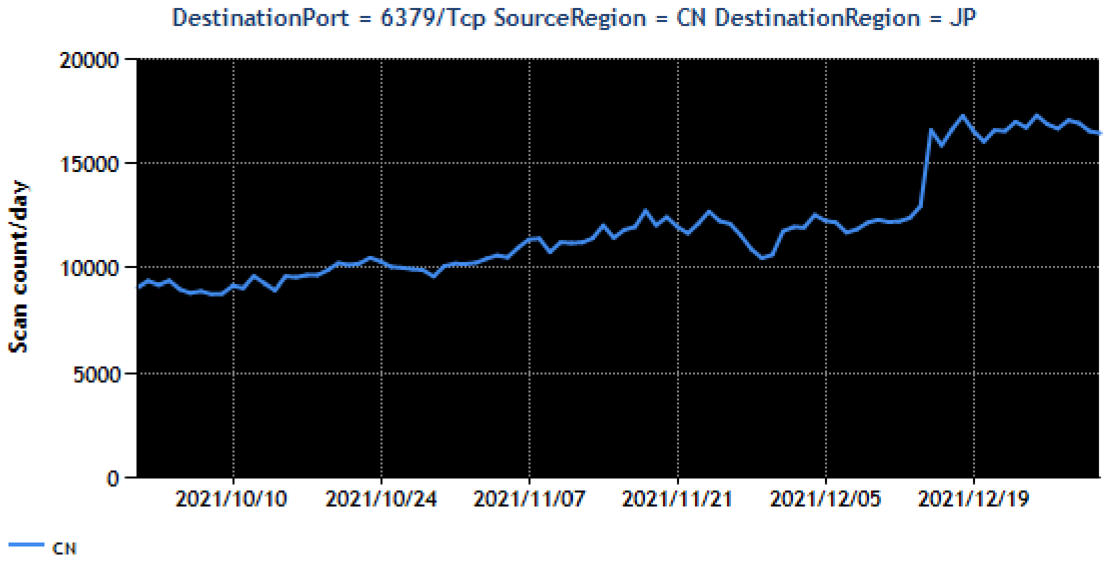
2. Events of Note

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

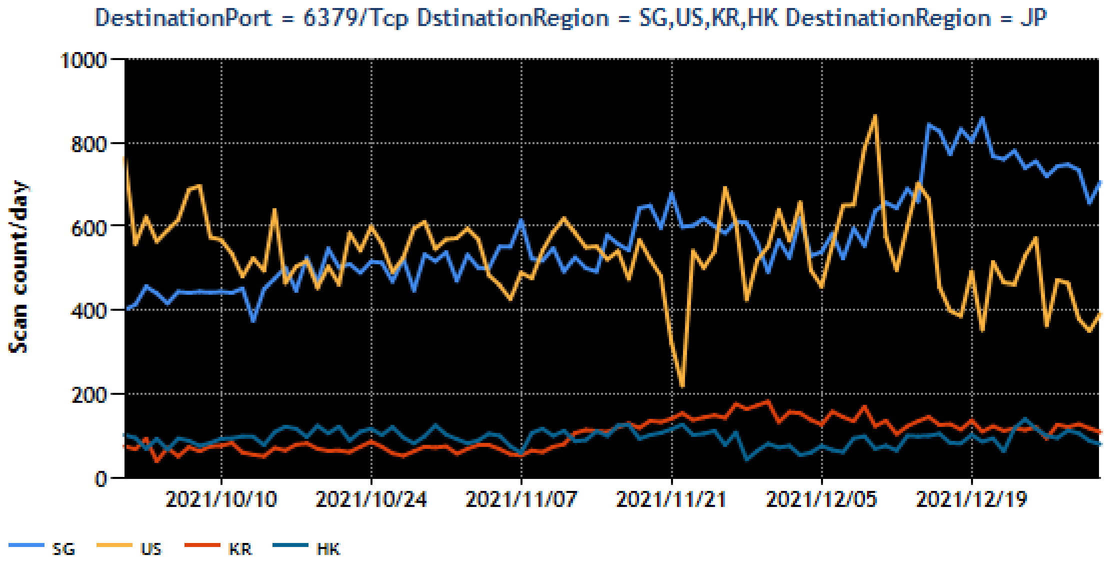
Large numbers of packets targeted to port 6379/TCP (Redis) were observed (Figure 3) throughout this quarter. 6379/TCP is a port number that is often used as a listening port for Redis in-memory databases. Over 88% of the packets targeted to port 6379/TCP originate in China, with regions like Singapore, the USA, South Korea and Hong Kong accounting for the rest of the observed packets (Figure 4,Figure 5). During this quarter, the number of packets targeted to port 6379/TCP from China increased by about 1.5 times despite temporary declines, while those originating in Singapore grew by about 1.3 times.



[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 5 source regions excluding China and targeted to port 6379/TCP]

Packets originating in other regions did not show significant changes throughout the quarter. Of the total source IP addresses of packets targeted to port 6379/TCP, the percentage accounted for by China increased from about 80%(2) in the previous quarter to 88%. The number of source IP addresses also increased.

To determine whether the packet sources are only conducting scans or actually carrying out attacks, JPCERT/CC compared TSUBAME's observation data with logs collected with a honeypot emulating Redis that JPCERT/CC is operating. As a result, it was found that more than half of the IP address group that accessed the honeypot a certain number of times were also observed with TSUBAME. Since these packets were attempting to perform some kind of process on the Redis honeypot, it is assumed that many of the sources of the packets observed with TSUBAME were not just scanning for Redis servers but were trying to infect them with malware.

Although JPCERT/CC has continued to provide logs and other information on a daily basis to overseas organizations that manage networks, urging them to take necessary steps with respect to the source IP addresses of packets targeted to port 6379/TCP, these efforts have not led to clear improvements as far as it can be seen from observations with TSUBAME. For this reason, JPCERT/CC considers undertaking activities aimed at addressing this situation, such as providing information to CSIRTs operating in relevant regions. JPCERT/CC also observed packets targeted to port 6379/TCP sent from 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.

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, but no such changes were observed. For this reason, it can be concluded that these attacks are not carried out using self-propagating malware. They can be narrowed down to cases in which compromised servers are exploited as a springboard, or cases in which the attacks are launched from infrastructure prepared by the attacker. Beyond that, nothing is known at the moment. It is important for server administrators to see if there are any unintended accesses to their servers, and make sure they are not exploited by third parties as a springboard.

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 [July 1, 2021 - September 30, 2021]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q2_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.