JPCERT/CC Internet Threat Monitoring Report

October 1, 2020 ～ December 31, 2020

JPCERT Coordination Center

January 21, 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 mainly works with overseas National CSIRTs to deploy sensors and 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 during this quarter by sensors located in Japan.

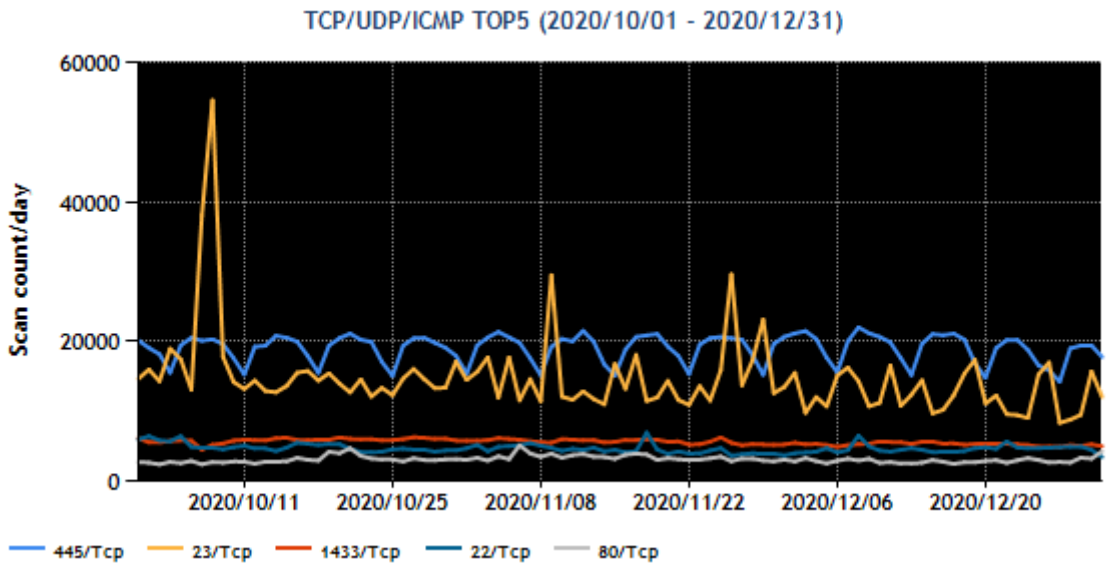
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[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	1433/TCP (ms-sql)	3
4	22/TCP (ssh)	4
5	80/TCP(http)	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 number of packets observed for each destination port number listed in [Chart 1] is shown [Figure 1].



[Figure 1: Number of packets observed at top 5 destination ports from October through December 2020]

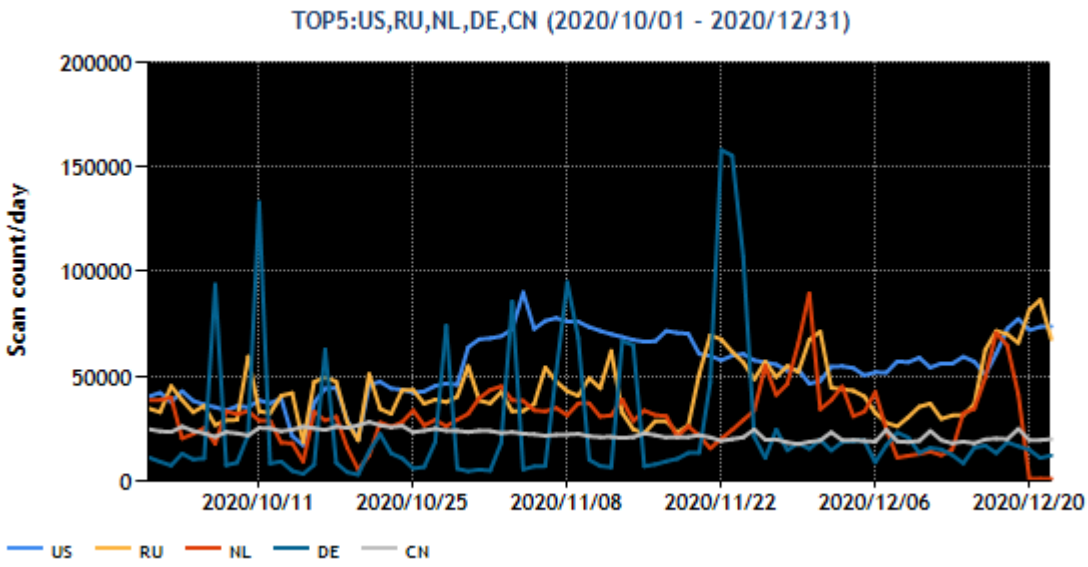
The ranking (top 5) in terms of the number of packets observed at each destination port remained unchanged from the previous quarter. Port 445/TCP (microsoft-ds) received the greatest number of packets. Periodic weekly fluctuations were seen throughout the quarter.

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	Netherlands	4
4	China	3
5	Germany	5

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



[Figure 2: Number of observed packets of the top 5 source regions from October through December 2020]

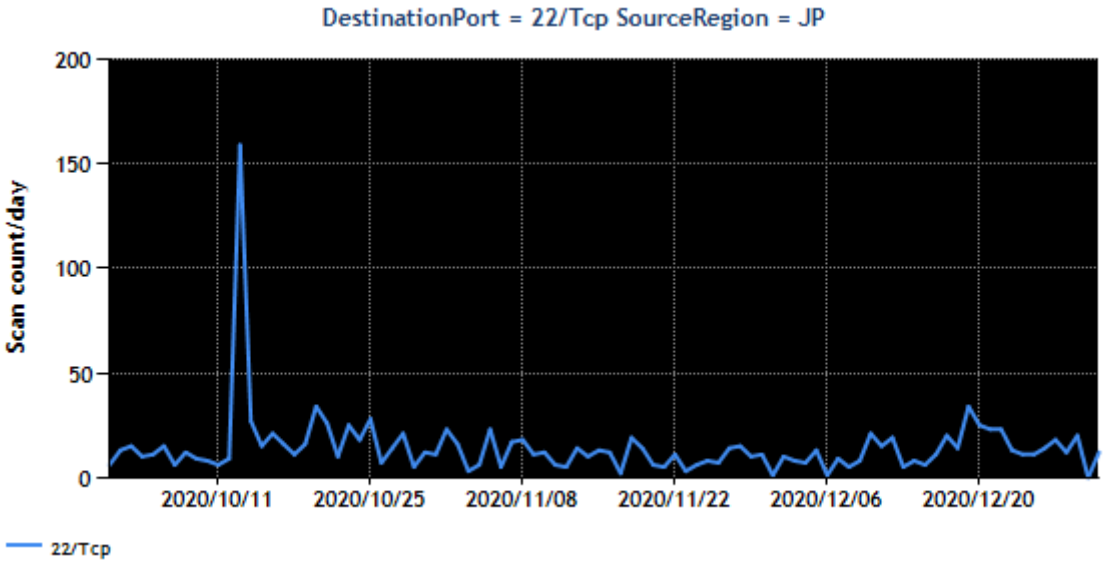
The top source region for the number of packets observed this quarter was the USA, where the number of packets increased from around October 30. The number of packets originating in China has been gradually decreasing, with Germany overtaking China in the ranking. In the Netherlands, the number of packets declined sharply on December 20.

It was found that most source IP addresses of packets that originated in the Netherlands before December 20 were assigned to other regions after this date. JPCERT/CC is currently investigating the legitimacy of such a phenomenon and possible reasons for it by sending queries to CSIRTs in the Netherlands and other means.

2. Events of Note

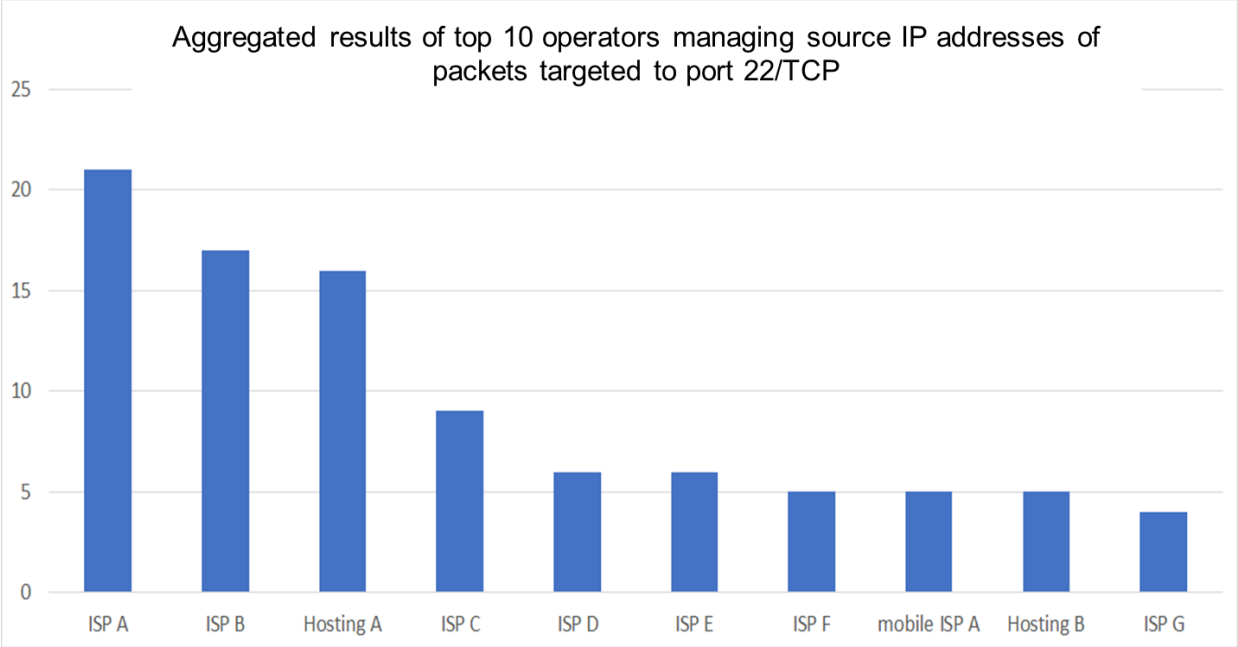
2.1. Increase in the number of packets targeted to port 22/TCP from Japan

Throughout this quarter, JPCERT/CC observed packets targeted to port 22/TCP (ssh) from Japan [Figure 3].



[Figure 3 : Number of observed packets targeted to port 22/TCP (originating in Japan)]

JPCERT/CC previously requested operators managing the source IP addresses of packets targeted to port 22/TCP to conduct an investigation, and a number of them have responded to date that their host had been breached and infected with malware. It is possible that sources that sent the packets in question had been similarly breached. In an attempt to find commonalities among the sources of packets targeted to port 22/TCP observed this quarter, JPCERT/CC aggregated the WHOIS lookup results according to operators (the names of operators are kept anonymous). The results are shown in [Figure 4].



[Figure 4 : Aggregated results of top 10 operators managing source IP addresses of packets targeted to port 22/TCP (originating in Japan)]

Among the top 3 organizations, ISP A and ISP B provide services by distributing dynamic IP addresses. Hosting A is a business operator that provides services by distributing fixed IP addresses that are often used when setting up servers.

JPCERT/CC used Shodan to scan and analyze the range of source IP addresses of observed packets held by Hosting A, and it found that about 30% of them were the IP addresses of servers with common characteristics. On the other hand, the sources of packets from ISP A and ISP B did not have such characteristics. JPCERT/CC conducted further analysis as it was possible that attackers may be exploiting servers with those characteristics in some way. As a result, it was found that these servers were used to play multiplayer world-building games, and upon further investigation of the characteristics, the following information was obtained.

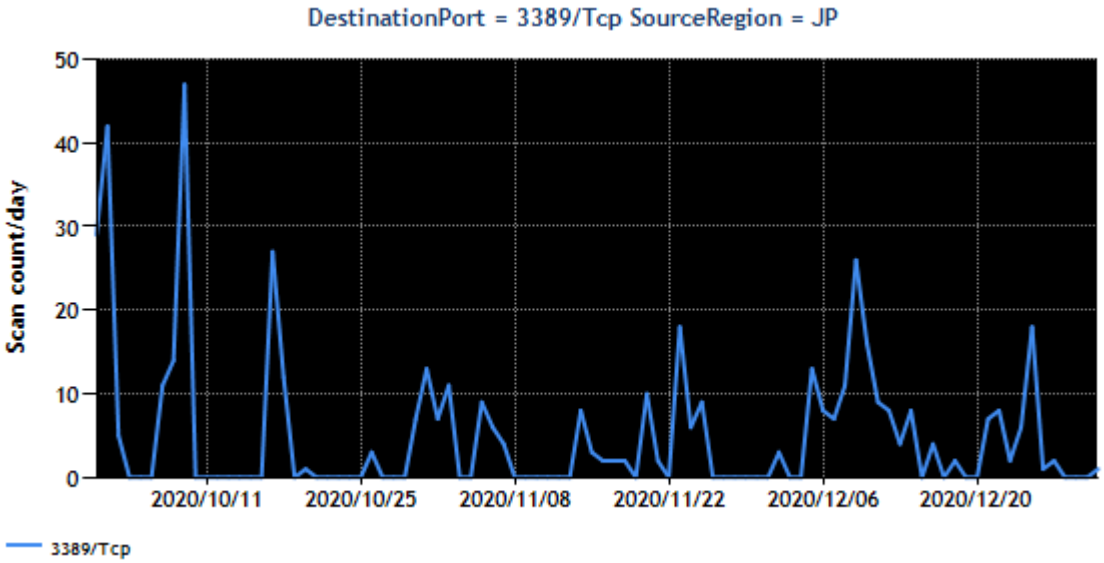
- SSH can be connected by password authentication, and if users have set a simple password, it might allow intrusion. The only user initially registered is root.
- While most services other than multiplayer game services are inactive, a service subject to UDP-based amplification attacks is active, and no external access restrictions are in place, such as a firewall.

As a result of investigations, it was found that while this service was offered by the provider with consideration given to various security issues, the lack of sufficient measures by the service users was allowing third parties to exploit the service. Since these servers are intended for game use, some users may think that it would be fine to give priority to convenience and change settings, but given that these

may be used as a springboard for attacks against other important servers, it is necessary to conduct proper maintenance of servers even if they are used for games. Maintaining a secure environment is essential to server management, such as stopping unnecessary services, permitting only necessary communications with the firewall, avoiding the use of simple passwords for the administrator account, and applying operating system updates.

2.2. Observation of packets targeted to port 3389/TCP originating in Japan

During this quarter, fluctuations in the number of packets targeted to port 3389/TCP (ms-wbt-server) have been observed [Figure 5].



[Figure 5 : Number of observed packets targeted to port 3389/TCP (originating in Japan)]

Search results on Shodan, etc. confirmed that almost all the sources were waiting for packets targeted to port 3389/TCP. When JPCERT/CC contacted an operator managing the source IP addresses, it responded that a version of Windows server no longer supported had been breached, and an unknown tool had been installed.

Users of Windows servers should check once again to make sure they are not running on a version of operating system no longer supported and security update programs are applied properly.

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 2020.