JPCERT Coordination Center

JPCERT/CC Internet Threat Monitoring Report

October 1, 2019 - December 31, 2019

JPCERT Coordination Center
January 29, 2020

Tabele 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 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.

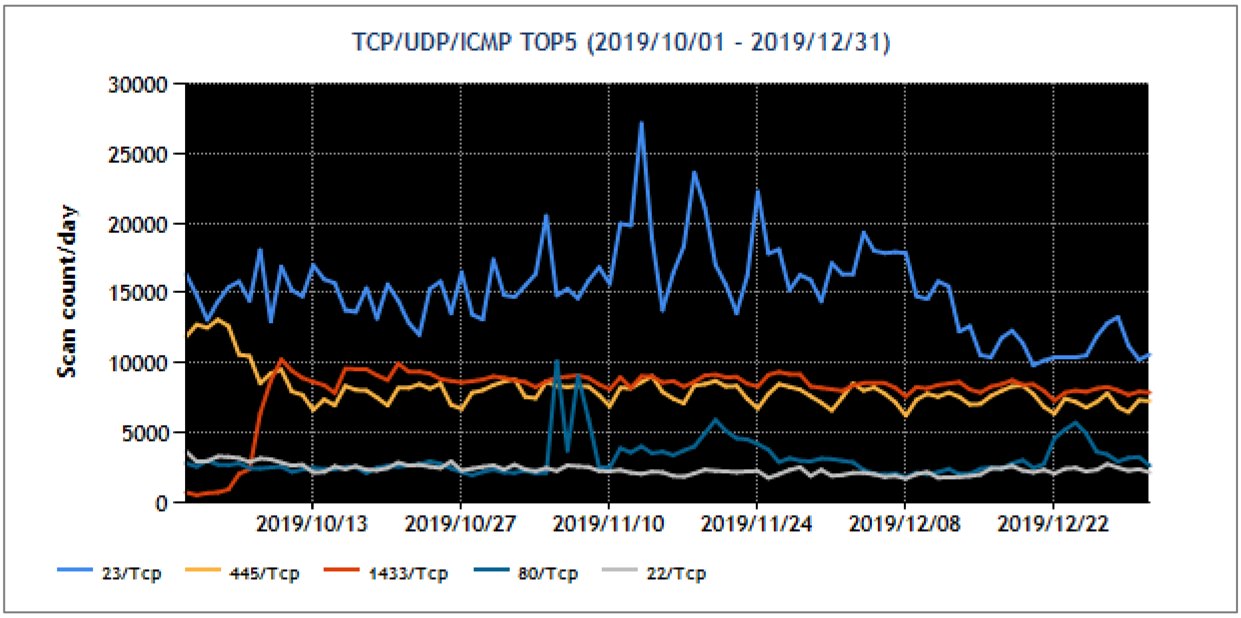
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1 : Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	2
3	1433/TCP (ms-sql)	Not in top 10
4	80/Tcp(http)	5
5	22/TCP	3

*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 2019]

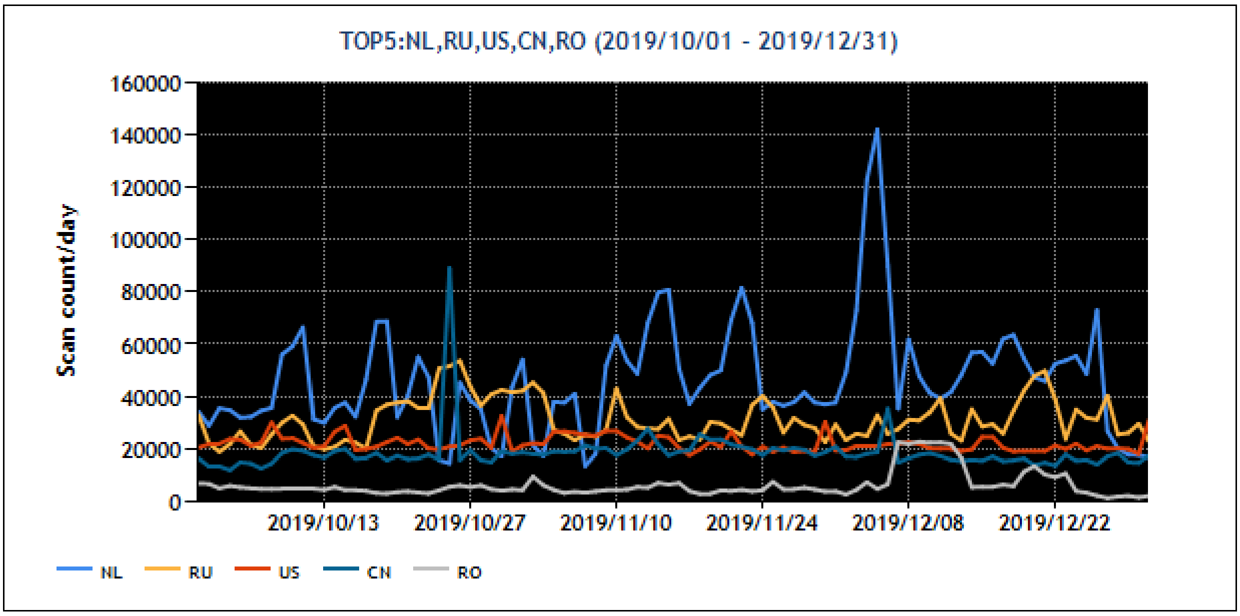
Throughout this quarter, the number of packets targeted to port 445/TCP and port 23/TCP remained fairly constant each week. The number of packets targeted to port 1433/TCP increased from October 4 and ended up ranking third. This event will be discussed in "2.1 Trends in the number of packets targeted to port 1433/TCP".

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	Netherlands	1
2	Russia	2
3	USA	3
4	China	4
5	Romania	6

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



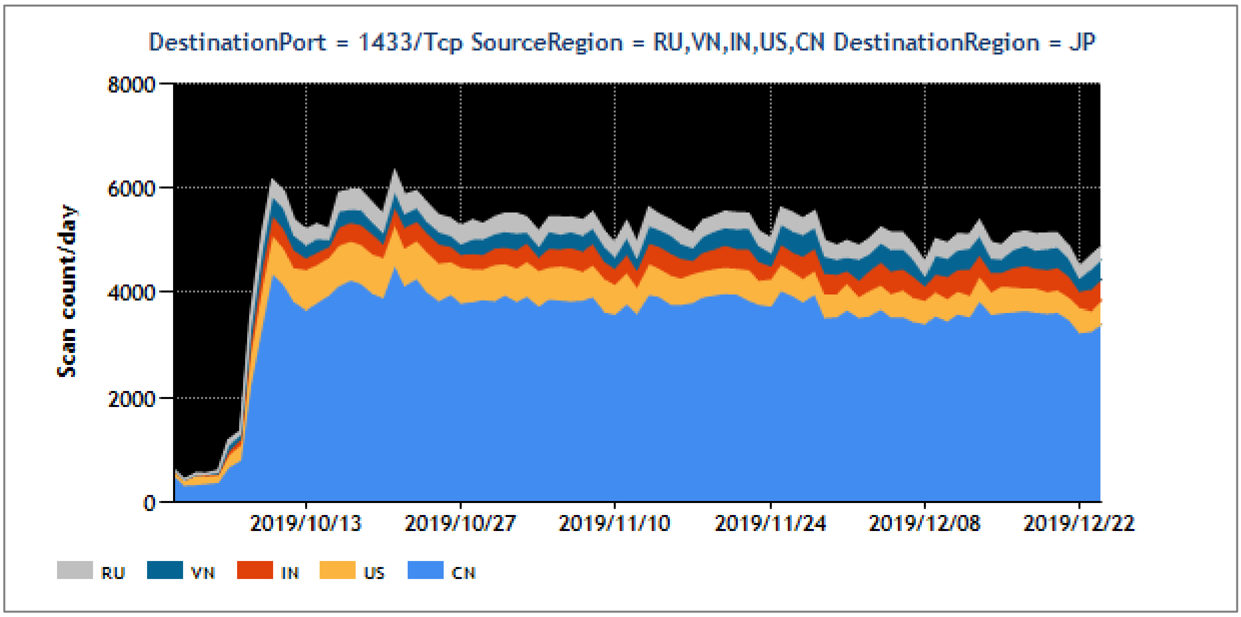
[Figure 2: Number of observed packets of the top 5 source regions from October through December 2019]

Regarding the number of packets received this quarter, JPCERT/CC investigated the situation in the Netherlands, which continued to rank first as a source region. As a result, it was found that some of the sources where the packets originated were live web servers, and there were web pages stating that scans were being conducted to probe for open ports. When the packets were sorted based on whether they were related to this activity or not, it was found that nearly 80% of the packets were presumably sent for the scanning. Changes in the number of packets due to scanner activities were clearly shown in the graph. As for Romania, which ranked fifth, the number of packets spiked to approximately 3 to 4 times the normal volume for about a week from December 7, which affected its ranking in the total number for the quarter. As for other regions, there were no changes in the rankings.

2. Events of Note

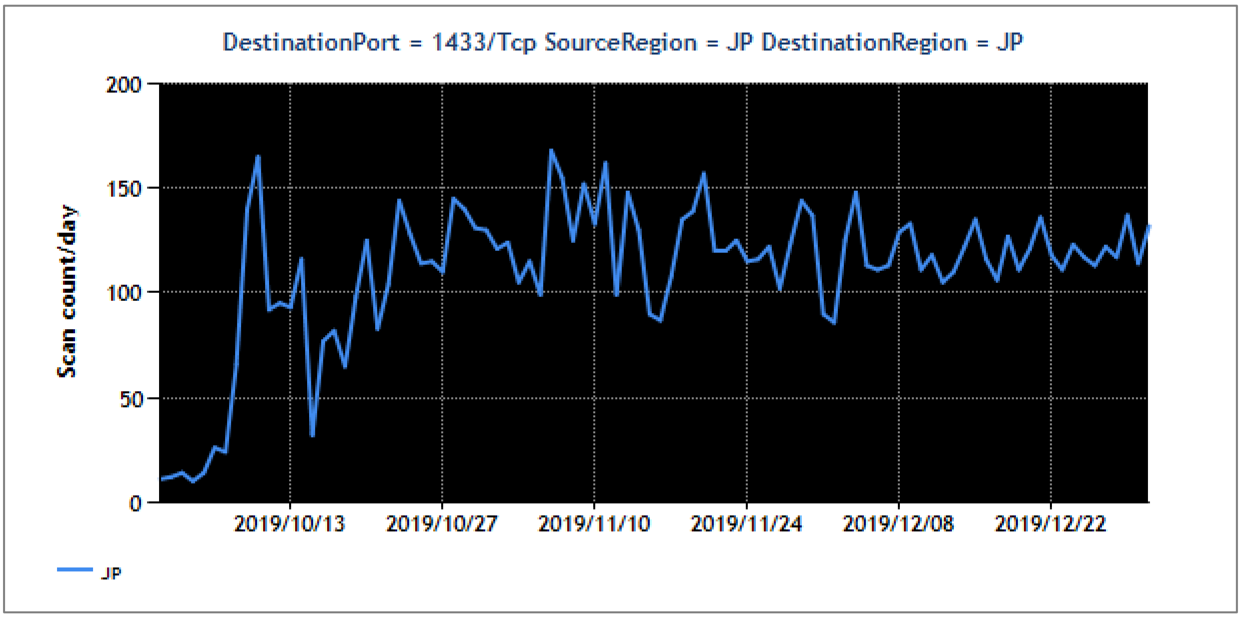
2.1. Trends in the number of packets targeted to port 1433/TCP

A large number of packets targeted to port 1433/TCP have been observed[2] since around October 4, 2019. As seen in the stacked graph by region shown in [Figure 3], China is a major source region, with others including the United States, India, Vietnam and Russia.



[Figure 3：Number of observed packets targeted to port 1433/TCP by major source region]

Japan is also a source region, and a large number of packets have been observed since around the same time. It ranks thirteenth in the rankings of source regions.

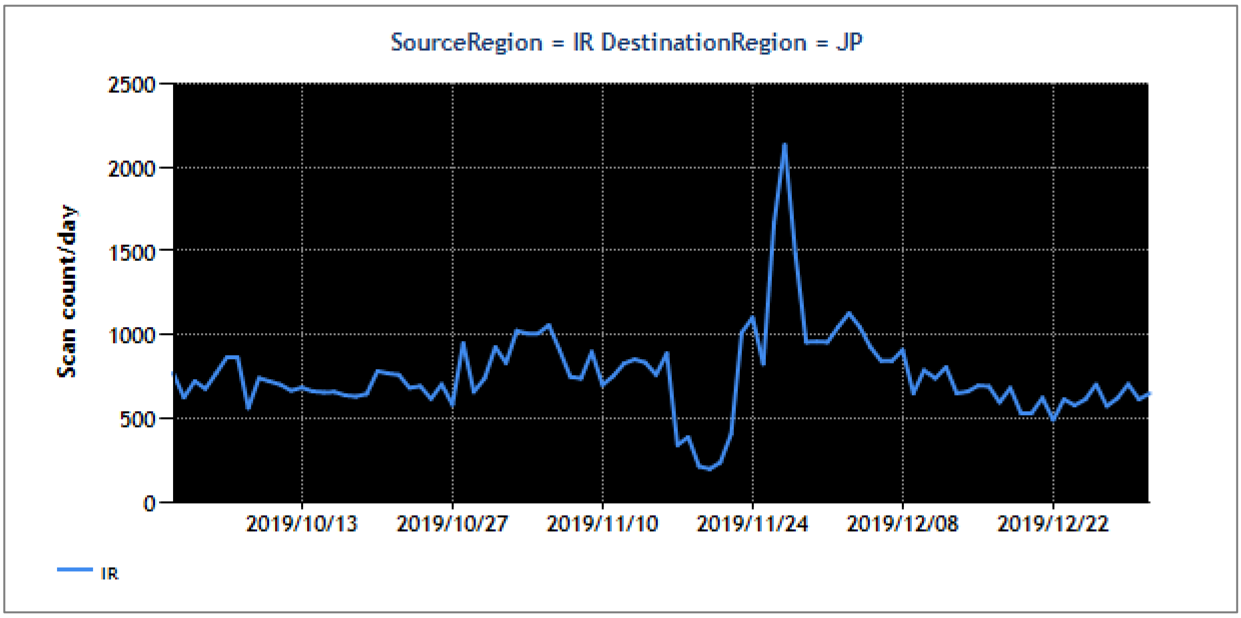


[Figure 4：Number of observed packets targeted to port 1433/TCP and originating in Japan]

It is not possible to tell what kind of attack is intended after the scans based on observation with TSUBAME's sensors. Therefore, JPCERT/CC set up a honeypot to see what kind of requests were being sent to port 1433/TCP, and it found that authentication attempts were being made targeting SQL Server.
Next, JPCERT/CC investigated the sources and found that IIS and SMB were running on many of the hosts that were sending packets to ports 1433/TCP and 445/TCP, which suggests that these were Windows environments. The findings did not point to any particular Windows versions as a predominant source, and SMB and RDP ports were open in some cases while closed in others. As such, no common characteristics were found. JPCERT/CC still has not been able to identify the malware that has infected these hosts and is sending the packets.
Authentication attacks targeting servers running SQL Server may continue to be seen for some time. It is advised that appropriate steps be taken to protect relevant servers, such as performing proper access control and using a strong password.

2.2. Impact of Internet shutdown in Iran

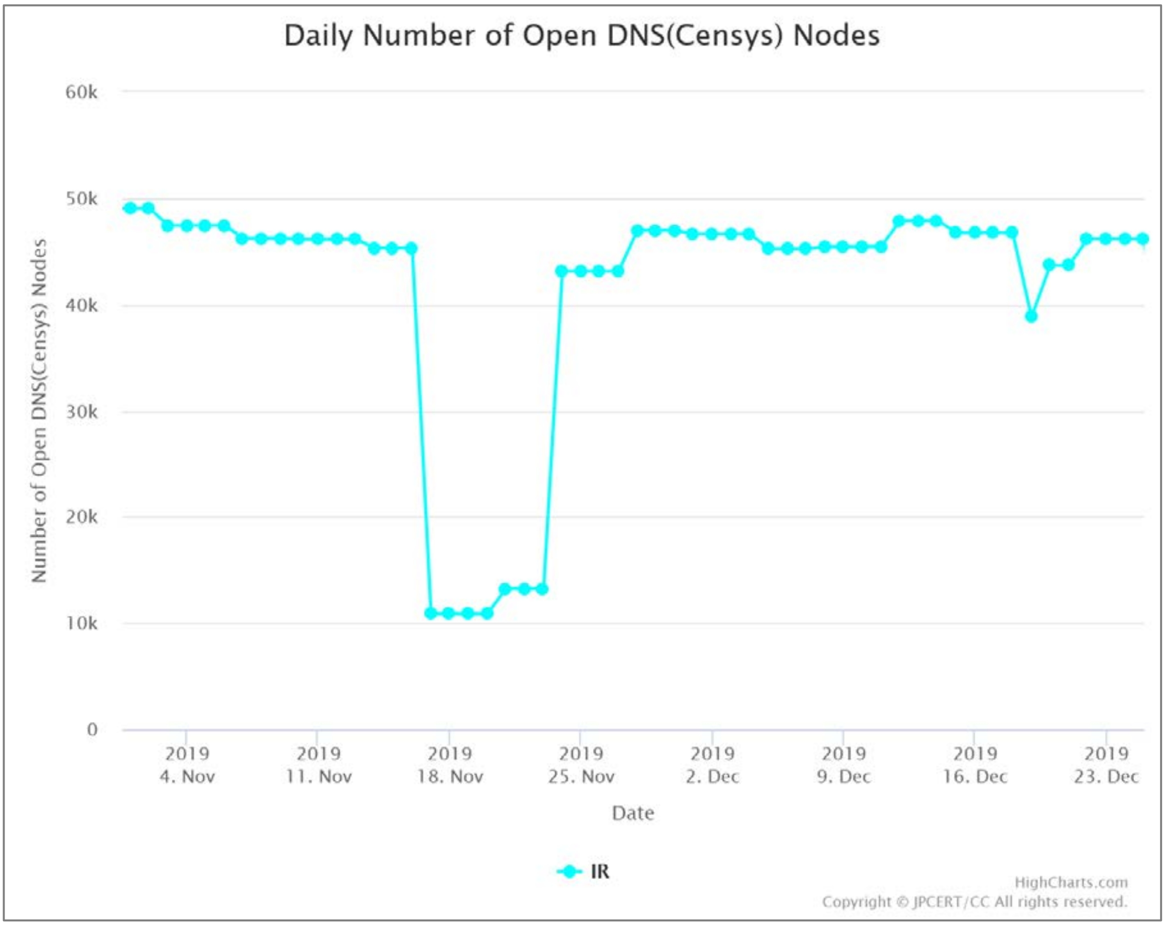
Packets captured by TSUBAME's sensors are affected not only by the status of the source but also by changes in the status of the paths that the packets are sent through. In other words, even when there is no significant change in the status of the source, if the transmission path of packets is shut down or becomes unstable, for instance, the number of packets observed will decrease.
From November 17 to 23, 2019, the number of packets observed originating in Iran (IR) decreased.



[Figure 5：Number of packets sent from Iran]

In Iran, demonstrators rallied in Tehran and elsewhere to protest the decision to raise gasoline prices from November 15[3]. NetBlocks, an NGO that monitors cyber security and Internet governance, presumes that the Internet shutdown was carried out during this period[4].

JPCERT/CC is conducting a demonstration project called Mejiro[5] with the aim of visualizing Internet risks, in which it provides information about Internet nodes with an open port. According to Mejiro, the number of open resolvers decreased from November 17 to 23.



[Figure 6：Number of open resolver nodes in Iran (from Mejiro)]

JPCERT/CC believes that it makes more sense to assume that the temporary changes in the observation data of TSUBAME and Mejiro were due not to any botnet activities or changes in the status of open resolvers in Iran, but to communication restrictions.

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) Observation of accesses targeting a vulnerability in PHP-FPM (CVE-2019-11043) (Japanese Only)
https://www.npa.go.jp/cyberpolice/important/2019/201911281.html

(3) Iran Reimposes Internet Blackout in Various Provinces, ILNA Says
https://www.bloomberg.com/news/articles/2019-12-25/iran-reimposes-internet-blackout-in-various-provinces-ilna-says

(4) NetBlocks.org (@netblocks)
https://twitter.com/netblocks/status/1196116024359366656

(5) Internet Risk Visualization Service -Mejiro- (Demonstration Test)
https://www.jpcert.or.jp/english/mejiro/

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 2019.