JPCERT/CC Internet Threat Monitoring Report

July 1, 2020 ～ September 30, 2020

JPCERT Coordination Center
October 15, 2020

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.

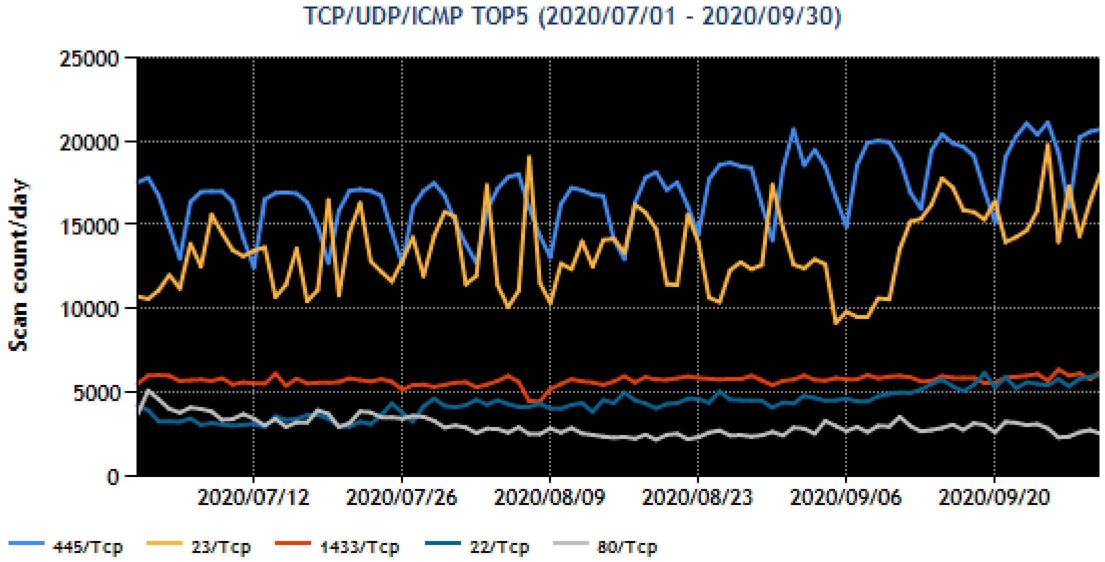
The top 5 destination port numbers for which packets were observed in Japan are listed in[Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	445/TCP (microsoft-ds)	2
2	23/TCP (telnet)	1
3	1433/TCP (ms-sql)	3
4	22/TCP (ssh)	5
5	80/TCP(http)	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 [Figure 1].



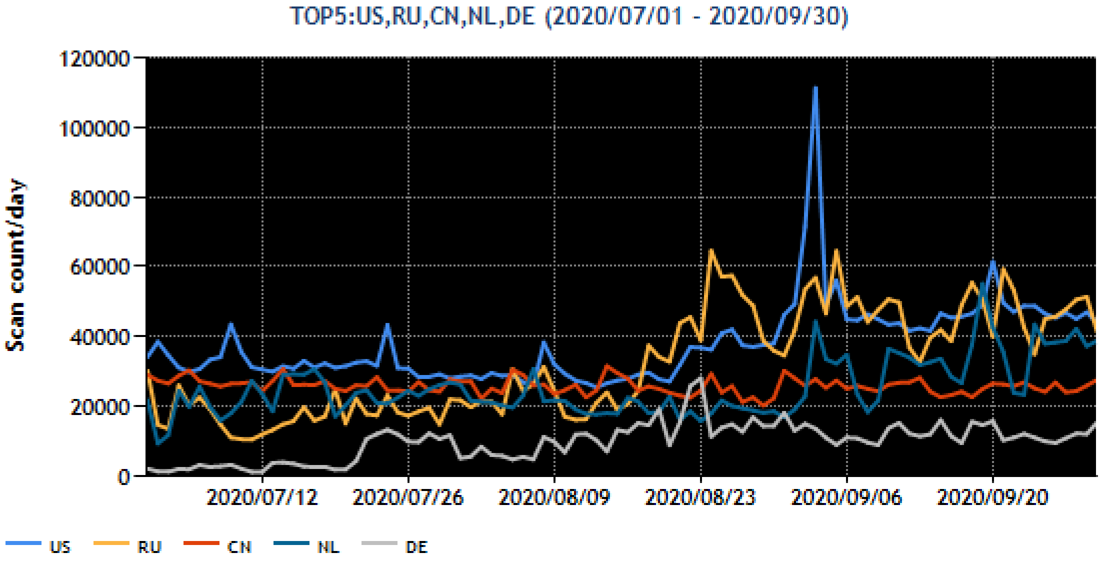
[Figure 1: Number of packets observed at top 5 destination ports from July through Septemer 2020]

Port 445/TCP (microsoft-ds) received the greatest number of packets. The number has remained high since late April. In addition, the number of packets targeted to 22/TCP (ssh) has been increasing, as well as the number of source hosts. 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	2
2	Russia	1
3	China	4
4	Netherlands	3
5	Germany	9

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



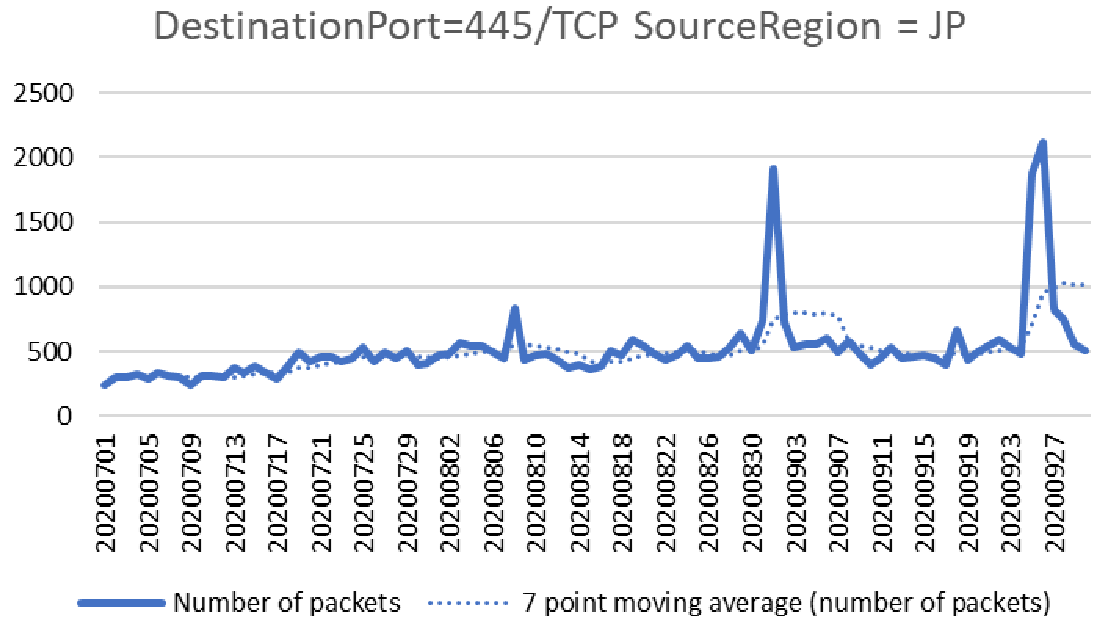
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2020]

The top source region for the number of packets observed this quarter was the USA. The top 5 destination port numbers for packets originating in the USA are roughly the same as in other regions. As for packets originating in Russia, which ranks second, port 22/TCP received the greatest number of packets, followed by port 3389/TCP. The numbers of packets targeted to these two ports were at least 10% greater compared to other regions, and the manner in which seasonal variations occur differs as well. As for other regions, there were no significant changes in the rankings.

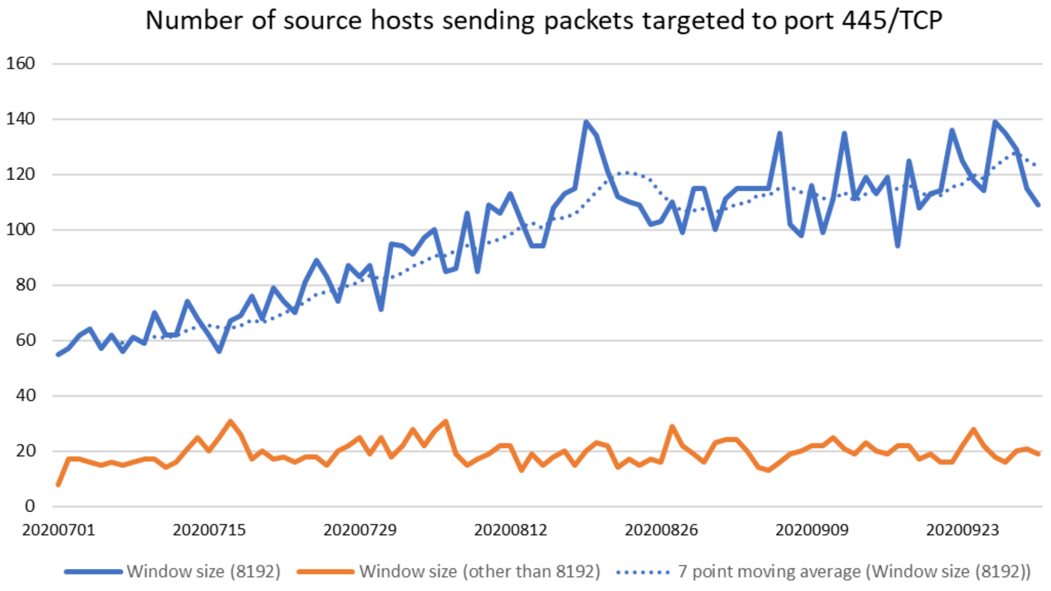
2. Events of Note

2.1. Increase in the number of packets targeted to port 445/TCP from Japan

Throughout this quarter, the number of packets targeted to port 445/TCP from Japan as well as the number of hosts sending these packets has been increasing, accompanied by temporary surges. (Figure 3,Figure 4)



[Figure 3: Number of observed packets targeted to port 445/TCP (originating in Japan)]



[Figure 4：Number of source hosts sending packets targeted to port 445/TCP (originating in Japan)]

There is a characteristic in the TCP window size of the observed packets targeted to port 445/TCP. JPCERT/CC investigated some of the sources and found several Windows operating systems, but there was no disproportionate concentration on a particular version or machine use. JPCERT/CC contacted operators managing the source IP addresses, and some of them replied that a version of Windows server no longer supported was being used. These operators have observed mining malware activity on compromised servers, as well as attacks against other hosts exploiting the MS17-010 vulnerability. Many of the observed packets targeted to port 445/TCP had a particular window size.

As shown in Figure 4, the number of hosts sending packets with a window size of 8192 is on the rise. On the other hand, not much change is seen in the number of hosts sending packets with a value other than 8192. The 8192 window size corresponds to the characteristics of packets generated by malware known to exploit the MS17-010 vulnerability.

Since the end of September 2020 as well, JPCERT/CC has been continuing to contact operators managing source IP addresses and observe packets targeted to port 445/TCP. JPCERT/CC advises administrators of machines running Windows to check for any versions that are no longer supported or open network ports that are not needed, check whether updates and other measures are conducted appropriately, and review passwords to make sure they are of appropriate strength.

2.2. Observation of packets assumed to be part of DDoS attacks

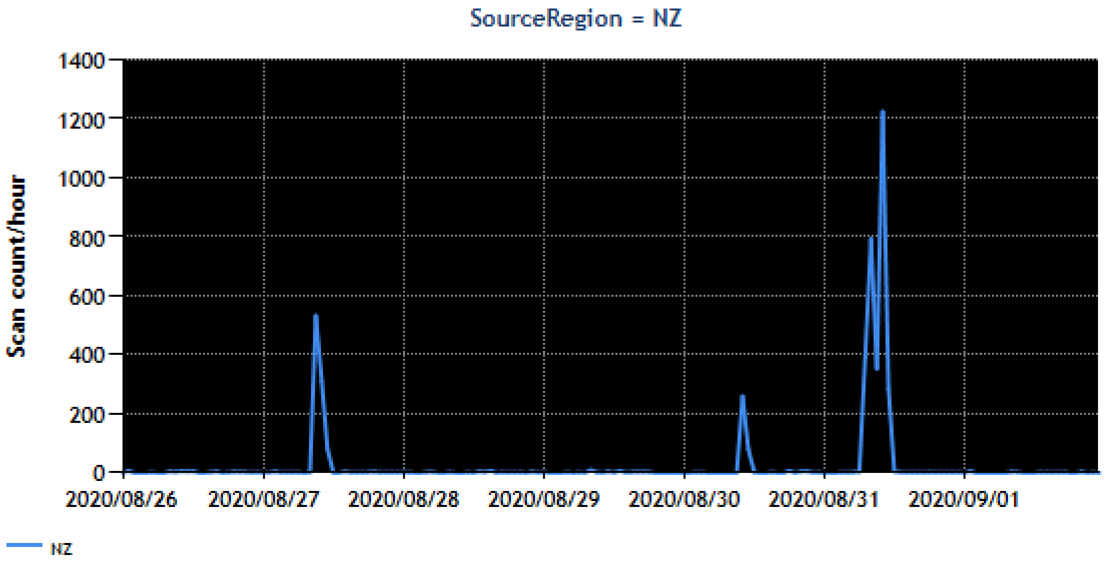
On August 27, 30 and 31, JPCERT/CC observed temporary increases in the number of packets originating in New Zealand. Around this time, there were news reports of DDoS attacks targeting the New Zealand Stock Exchange and the Bank of New Zealand.[(2)] The packets observed had characteristics that are commonly seen in packets related to DDoS attacks, suggesting that they were the result of attempted and successful attacks. The observation results are shown in [Chart 3] and [Figure 5].

[Chart 3: Number of source IP addresses of packets observed by TSUBAME]

Date	Number of Source IP Addresses (*1)	Organization Owning the IP Addresses (*2)
August 27, 2020	4	New Zealand Stock Exchange
August 30, 2020	1	New Zealand Stock Exchange
August 31, 2020	7	Bank of New Zealand

(*1) Number of source IP addresses seen with more than a certain number of packets captured by TSUBAME

(*2) Organizations owning IP addresses identified with WHOIS lookup



[Figure 5: Number of packets sent from New Zealand between August 26 and September 2]

The packets sent from these IP addresses had either one of the following two sets of characteristics.

- Characteristics 1
  - Source port number is 443/TCP
  - Window size is fixed
  - Sequence number is fixed

- Characteristics 2
  - Destination port number is 23/TCP
  - Window size is fixed

JPCERT/CC reported these observed events and characteristics to the national CSIRT of New Zealand (CERT NZ).

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) Unprecedented: DDoS Attacks Take Down NZ Stock Market, Banks, Online News & Weather Service
https://secalerts.co/article/unprecedented-ddos-attacks-take-down-nz-stock-market-banks-online-news--weather-service/444f8e80
DDoS Attacks on New Zealand Stock Exchange Highlight Global Spike in ISP Assaults
https://www.msspalert.com/cybersecurity-markets/asia-pacific/ddos-attacks-on-new-zealand-stock-exchange-highlight-global-spike-in-isp-assaults/

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.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/english/tsubame/