JPCERT/CC Internet Threat Monitoring Report

April 1, 2019 ～ June 30 , 2019

JPCERT Coordination Center

July 11, 2019

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 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.

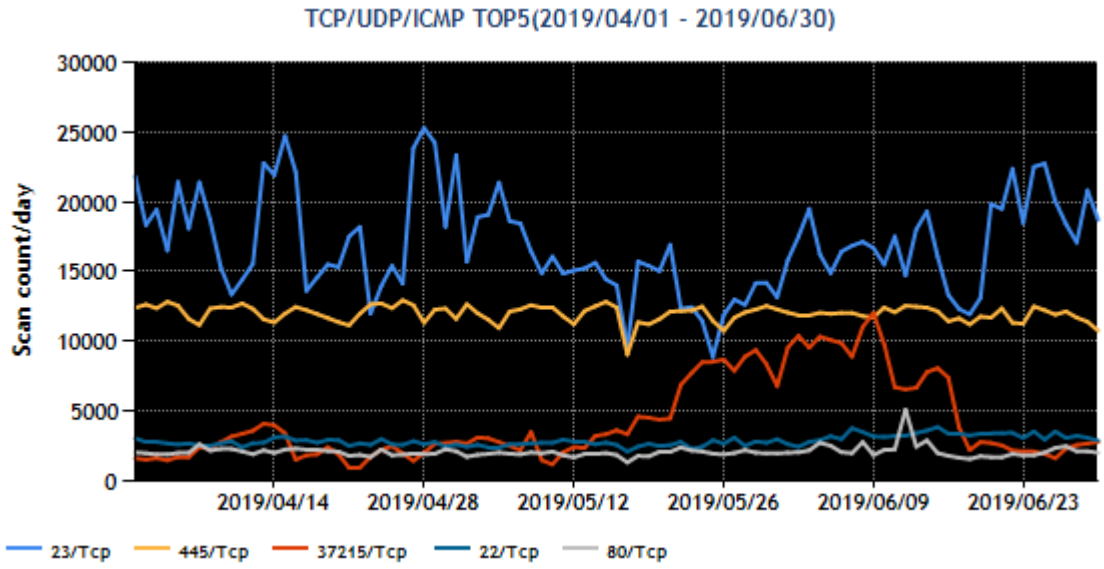
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[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	37215/TCP	Not in top 10
4	22/TCP (ssh)	5
5	80/Tcp(http)	6

*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 April through June 2019]

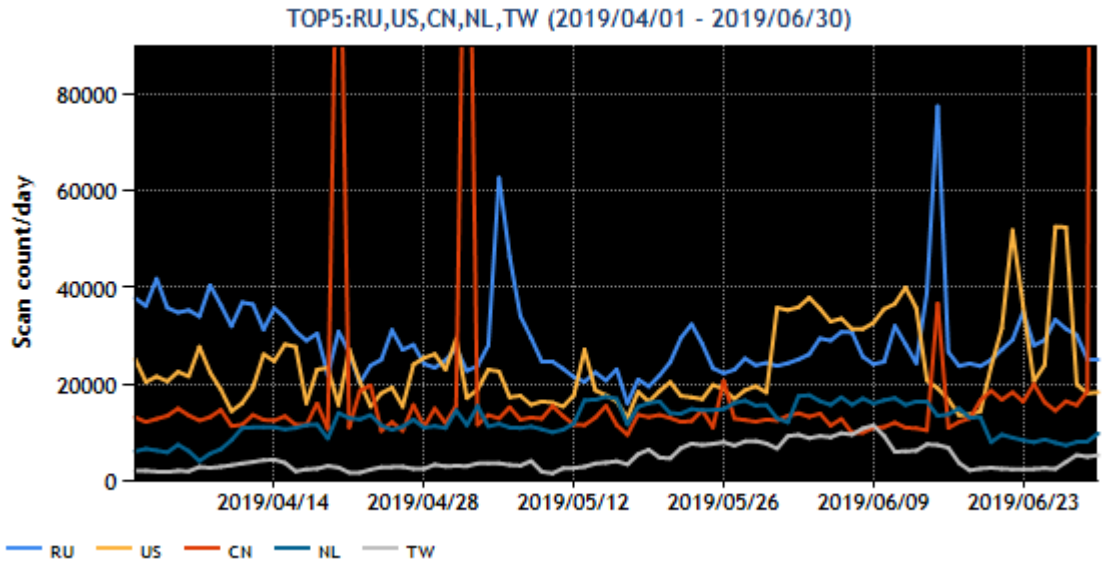
Throughout this quarter, the number of packets targeted to port 445/TCP remained fairly constant, and it even briefly surpassed the number of packets targeted to port 23/TCP. The number of packets targeted to port 37215/TCP increased for about a month from around May 14 and rose to third place in the ranking. Roughly 70% of the packets originated in Taiwan. During this period, information was published regarding activities of a Mirai variant that exploits vulnerabilities in a number of devices, and CVE-2017-17215 was listed as one of the targets. It is possible that packets targeted to port 37215/TCP increased due to activities of this malware.

An investigation of the breakdown by source region revealed a notable concentration in 3 specific regions. This phenomenon will be discussed in section 2.1 "Increase in the number of packets from sources that appear to be Windows environments." 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	Russia	1
2	USA	2
3	China	3
4	Netherlands	5
5	Taiwan	Not in top 10

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



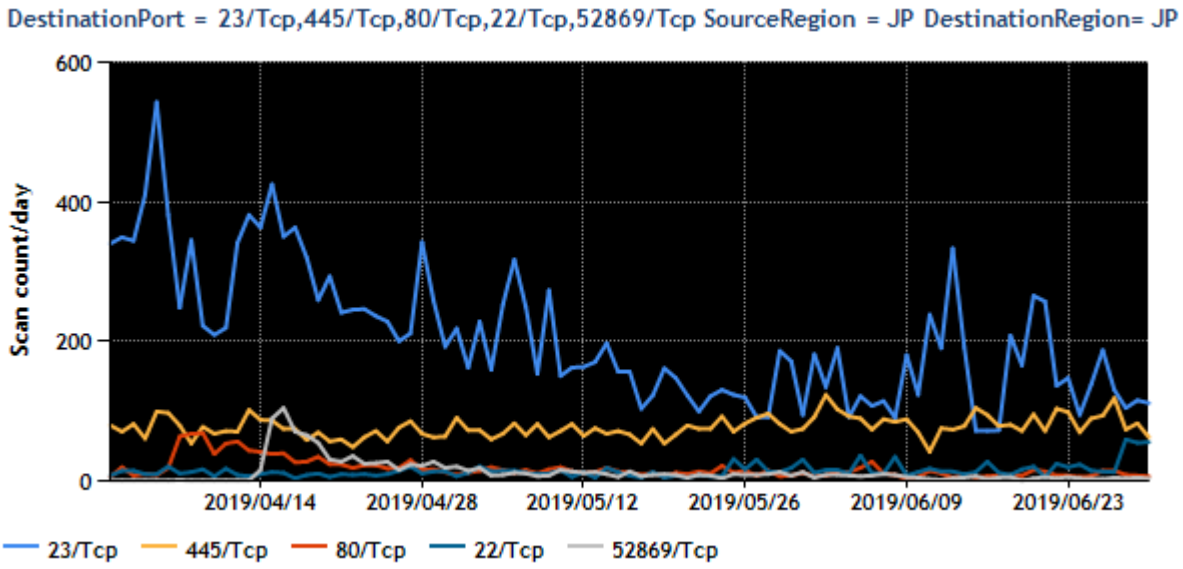
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2019]

In the breakdown of the number of observed packets by source region, packets originating in Taiwan increased from around May 12. This resulted in a change in the rankings. Packets targeted to port 37215/TCP were the greatest in number, accounting for about 70% of the packets originating in Taiwan. Temporary fluctuations were seen in other regions, but none to an extent affecting full-year rankings.

2. Events of Note

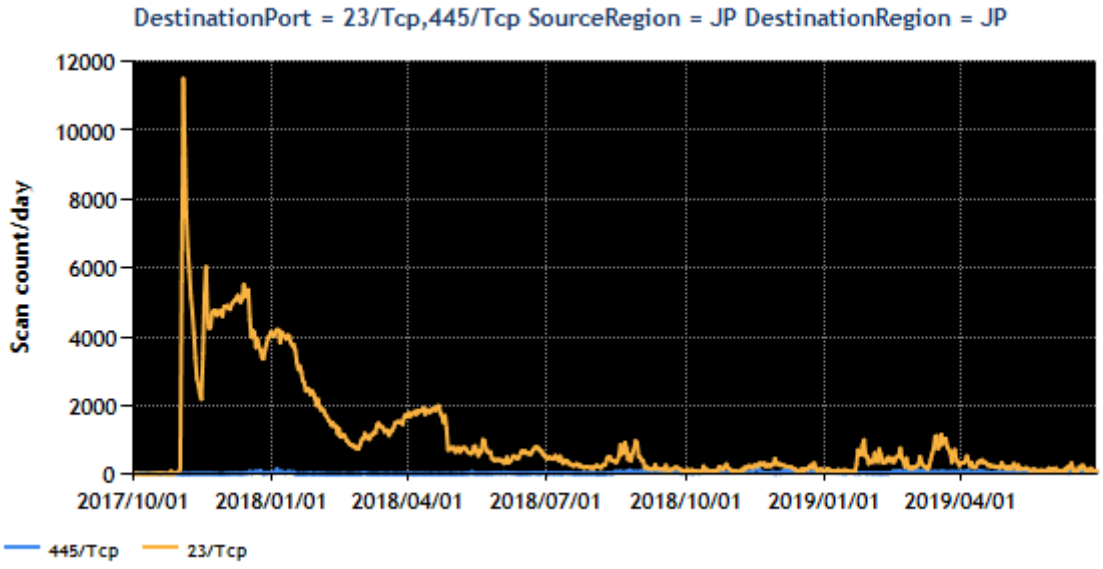
2.1. Trends in packets sent from Japan

The trends in the numbers of packets originating in Japan observed at each destination port since April 2019 are shown in [Figure 3].



[Figure 3: Numbers of packets originating in Japan observed at top 5 destination ports]

Since November 2017 [Figure 4], packets targeted to port 23/TCP have continued to account for the biggest share of packets originating in Japan, and most of those packets were sent by devices infected with Mirai or a Mirai variant. However, product vendors and Internet service providers have subsequently called for actions to be taken, and users have updated or replaced their devices. As a result, the number of packets targeted to port 23/TCP has been declining. This quarter, the number of packets targeted to port 445/TCP gradually increased, temporarily surpassing the number of packets targeted to port 23/TCP.

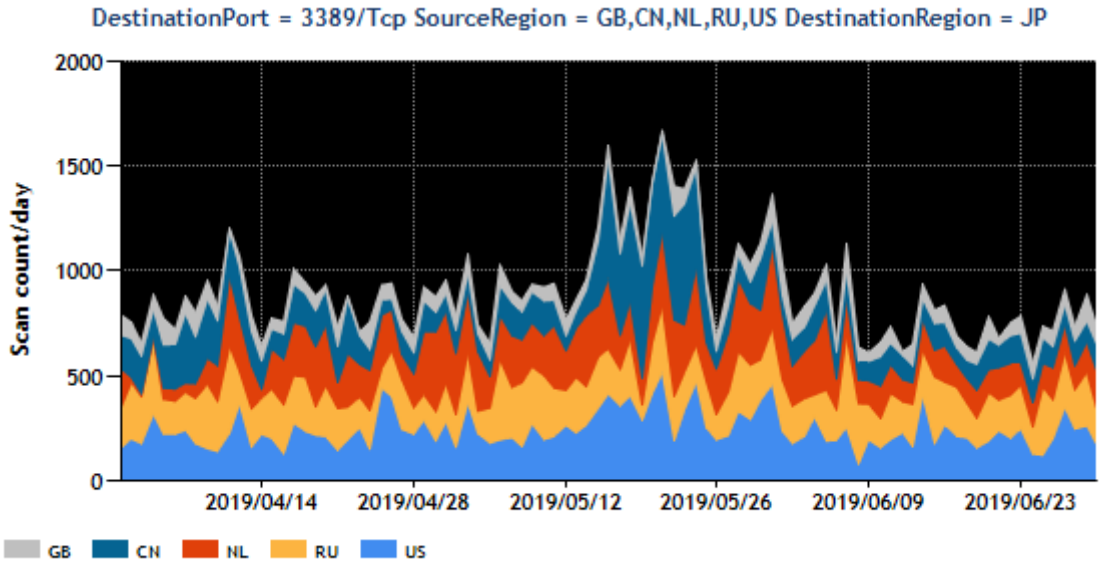


[Figure 4: Long-term trend in numbers of packets targeted to port 23/TCP and port 445/TCP]

There is a certain 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, including old versions, but there was no disproportionate concentration on a particular version or machine use. Windows uses port 445/TCP for various purposes. Past cases of attack widely performed through this port include methods such as hacking an account with a weak password to break into a server and executing malware to infect the system, and exploiting a known vulnerability in Windows to infect a server with malware. One type of the malware used in these attacks was Wannacry, and the window size for TCP packets sent by Wannacry has the same characteristics as the packets observed in this quarter. These circumstances suggest that the packets observed in this quarter were sent by Windows servers infected with malware to spread infection. JPCERT/CC has been contacting operators that manage the relevant IP addresses, but so far no notable decrease in the number of packets has been seen.

2.2. Trends in the number of packets targeted to port 3389/TCP

While not among the top 5 destination port numbers of this quarter, JPCERT/CC observed an increase in the number of packets targeted to port 3389/TCP for about 10 days from around May 14, 2019. As seen in the stacked graph by region shown in [Figure 5], China, the United States, and the Netherlands are the major source regions.



[Figure 5: Number of observed packets targeted to port 3389/TCP by major source region]

The increase in these packets is probably related to the publication of information(*2) regarding a vulnerability in Microsoft's Remote Desktop Service (CVE-2019-0708). Immediately after this vulnerability information was published, the number of packets observed increased for about two weeks. This vulnerability also affects Windows XP and Windows Server 2003, which are no longer supported, and as an exceptional measure Microsoft has released a security update for these operating systems as well.

Other organizations have also issued an alert, pointing out that the vulnerability is likely to be exploited to create malware.

Official support for Windows Server 2008 and Windows Server 2008 R2 will end on January 14, 2020.

Since there is also the case described in 2.1, users of relevant devices are advised to make sure the Windows version they use are supported, security updates are properly performed, unnecessary ports are not kept open, and passwords with an appropriate strength are used.

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 Report for January 2019 (Japanese)
https://www.npa.go.jp/cyberpolice/important/2019/201903282.html

(3) JPCERT/CC Internet Threat Monitoring Report[October 1, 2017 - December 31, 2017]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2017Q3_en.pdf

(4) NICTER Analysis Team(test operation) (Japanese)
https://twitter.com/nicter_jp/status/1102834623405416448

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