JPCERT/CC Internet Threat Monitoring Report

January 1, 2020 ～ March 31 , 2020

JPCERT Coordination Center

May 12, 2020

JPCERT CC®

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.

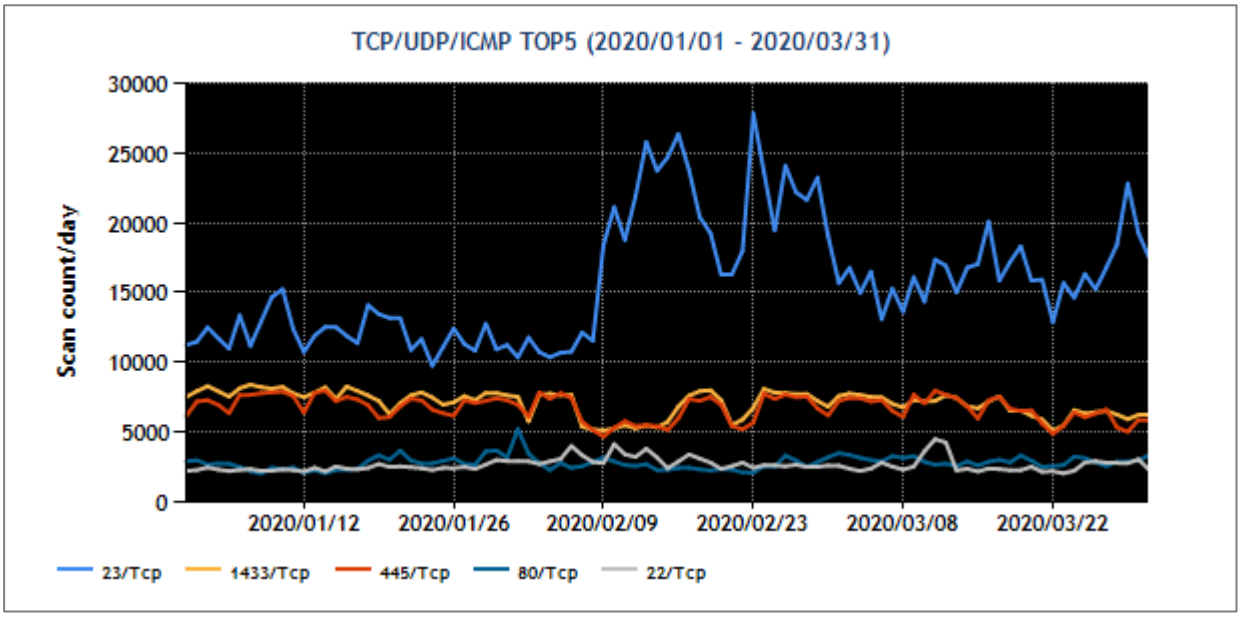
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1 : Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	1433/TCP (ms-sql)	3
3	445/TCP (microsoft-ds)	2
4	80/Tcp(http)	4
5	22/TCP	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 January through March 2020]

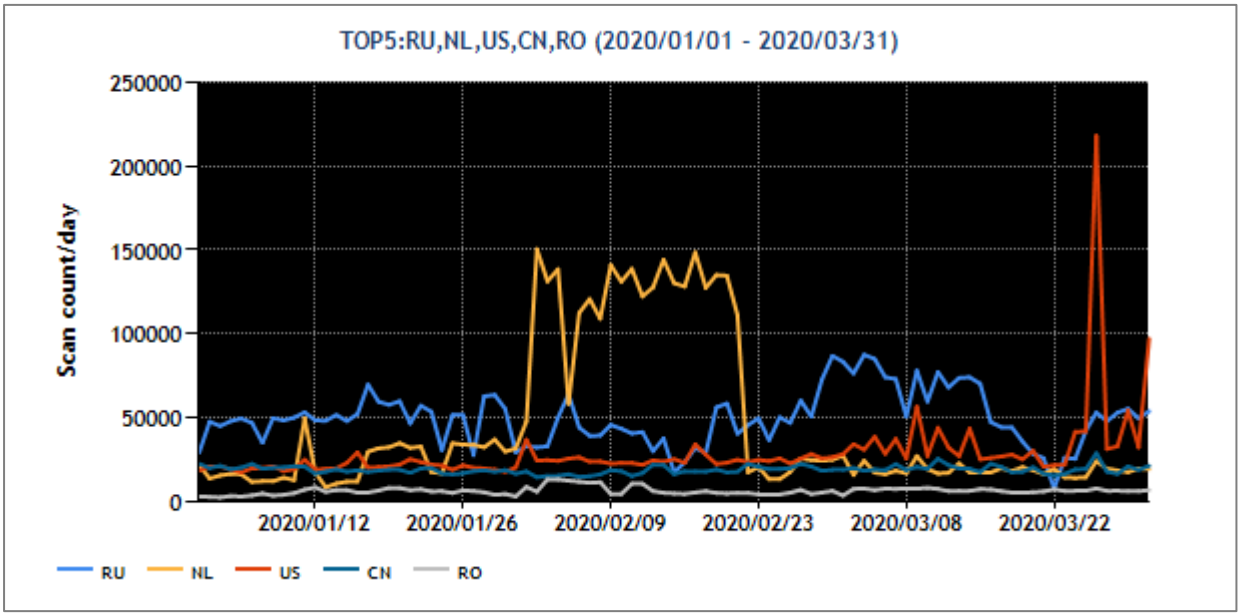
During this quarter, port 23/TCP received the greatest number of packets. From around February 9, the number of packets increased for about one month. This is assumed to be the result of increased activities of Mirai variants, etc.
Compared with the previous quarter, ports 445/TCP and 1433/TCP changed places. This is due to a larger decrease for port 445/TCP resulting in a greater number of packets for 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	Russia	2
2	Netherlands	1
3	USA	3
4	China	4
5	Romania	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 January through March 2020]

The top source region for the number of packets observed this quarter was Russia. The top 5 destination port numbers for packets originating in Russia are roughly the same as in other regions. However, its total number of packets for the top 5 destination port numbers is less than that of other source regions ranking below. The reason Russia still came out on top in total is the number of observed packets targeted to other ports. It is assumed that packets were sent to scan for a wide range of open ports(2) instead of a specific port. The Netherlands, which ranked second, showed similar trends as Russia. As for other regions, there were no changes in the rankings.

2. Events of Note

2.1. Reconnaissance activities targeting a vulnerability (CVE-2019-19781) in multiple Citrix products

On December 17, 2019, Citrix Systems published information about a vulnerability affecting multiple products(3). The proof-of-concept (PoC) exploit code for the vulnerability was also published around January 11(4). Part of the reconnaissance and attack activities against this vulnerability is observed with TSUBAME's sensors as packets targeted to ports 80/TCP and 443/TCP. However, the observation results do not indicate the type of attack intended after the scan.

JPCERT/CC is currently testing a honeypot that can be used to verify what kinds of requests are being sent. JPCERT/CC looked at the honeypot data captured on January 1, 2020 and later, and found that characteristics seen with PoC were contained within the requests (Chart 3). This suggests that reconnaissance activities scanning for said vulnerability started immediately after the PoC was published.

[Chart 3 : Honeypot observation trends]

Observation Date/Time	Source Regions	Request
3–4 pm January 11	DE	/vpn/%2e%2e/cpns/cfg/smb.conf
5–6 pm January 11	RU	/vpn/
1–2 am January 13	RU	/vpn/../vpns/cfg/smb.conf
8–9 pm January 14	KR	/vpn/
	KR	/vpn/
	KR	/vpn/
9–10 pm January 15	US	/vpn/../vpns/cfg/smb.conf

It is also possible to assume that the vulnerability scans listed in [Chart 3] were performed against focused targets based on information obtained from other sources. However, given that communications from the same source IP addresses were also detected by TSUBAME almost without exception, it appears likely that the scans are being performed widely in an exhaustive fashion, without narrowing down the targets in advance.

JPCERT/CC has received reports of attacks targeting this vulnerability(5). It is advised that users of the products affected by the vulnerability check their logs to make sure they have not been attacked(6).

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) NICTER Observation Report 2019
https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf

(3) CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance
https://support.citrix.com/article/CTX267027

(4) SRemote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway [CVE-2019-19781]
https://github.com/projectzeroindia/CVE-2019-19781

(5) JPCERT/CC Incident Handling Report [January 1, 2020 - March 31, 2020]
https://www.jpcert.or.jp/english/doc/IR_Report2019Q4_en.pdf

(6) Alert Regarding Vulnerability (CVE-2019-19781) in Citrix Products
https://www.jpcert.or.jp/english/at/2020/at200003.html

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.