JPCERT CC®

JPCERT/CC Internet Threat Monitoring Report

January 1, 2019 ～ March 31 , 2019

JPCERT Coordination Center
April 11, 2019

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.

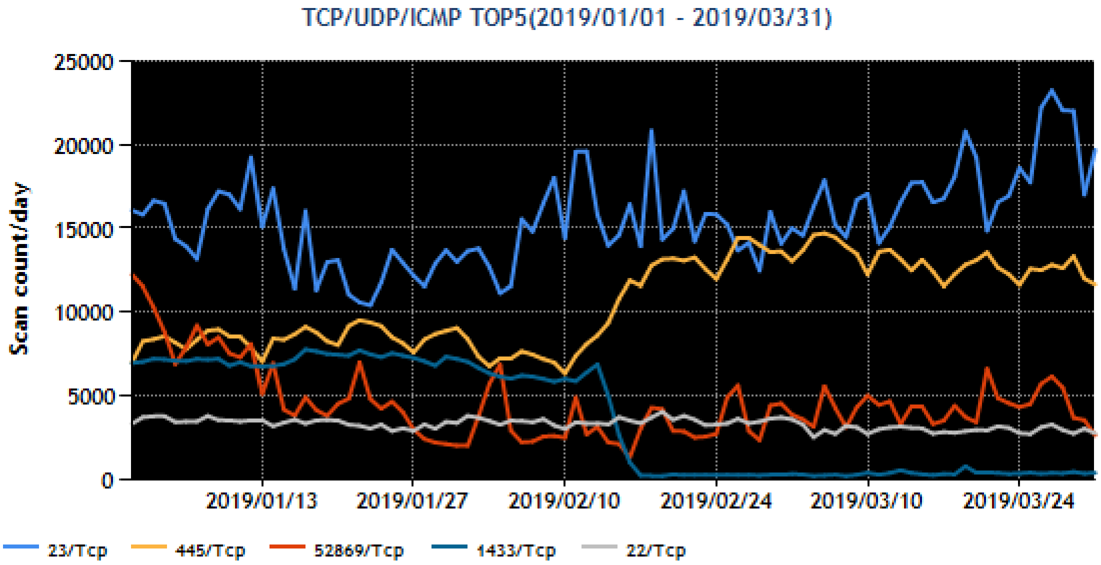
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[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	52869/TCP	6
4	1433/TCP(ms-sql)	3
5	22/TCP (ssh)	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 in [Figure 1].



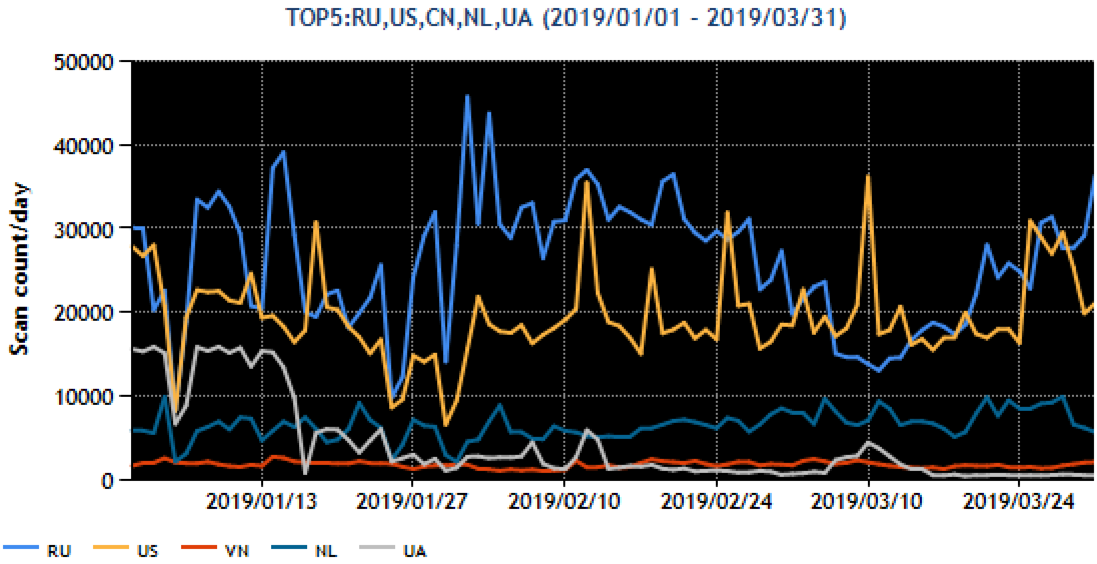
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2019]

The number of packets targeted to port 445/TCP has been increasing since around February 10. On the other hand, the number of packets targeted to port 1433/TCP has decreased sharply around February 15. The number of packets targeted to port 52869/TCP rose to third place in the ranking. 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	Ukraine	4

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



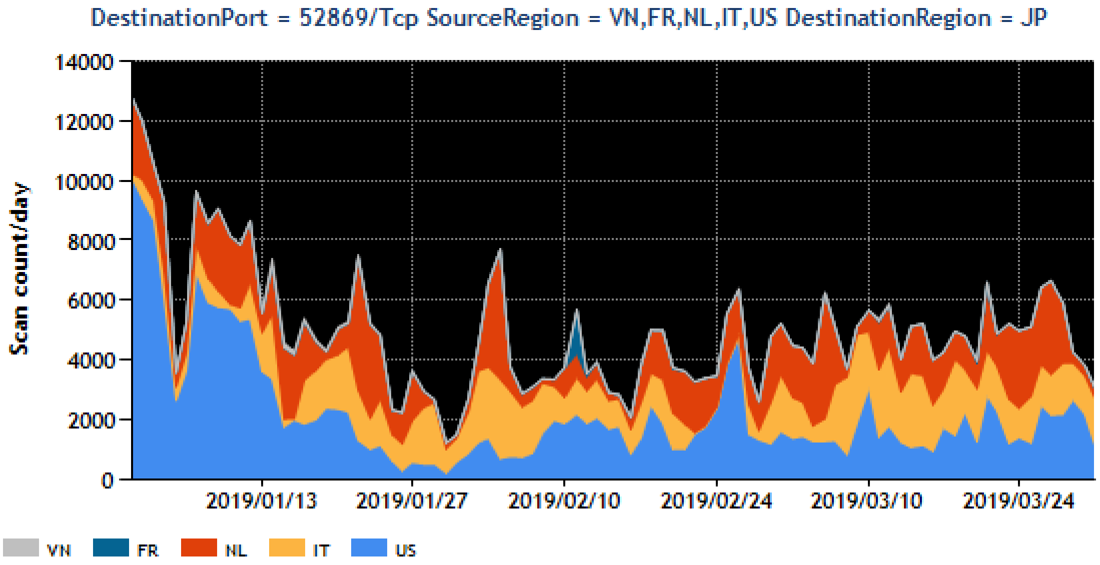
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2019]

In terms of source regions, the number of packets originating in Ukraine decreased around January 19, and the country fell below the Netherlands in the ranking. As for other regions, temporary fluctuations were seen, but there was no change in the ranking.

2. Events of Note

2.1. Trends in the number of packets targeted to port 52869/TCP

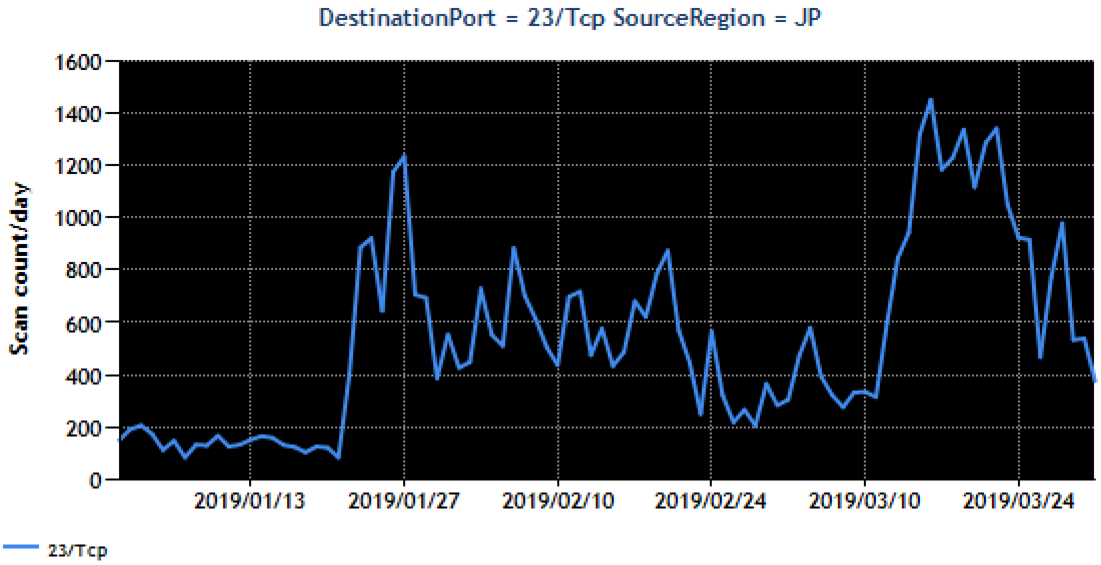
Packets targeted to port 52869/TCP have been observed(*2) since around January 2019. Major source regions are the United States, Italy and the Netherlands. A stacked area chart by region is shown in [Figure 3].



[Figure 3: Number of observed packets targeted to port 52869/TCP by major source region]

According to investigation, a known vulnerability in the miniigd service in Realtek SDK (CVE-2014-8361)(*3) has been found to be involved in these packets. Routers made using this SDK are affected by this vulnerability, which makes them susceptible to attacks carried out via the Internet. Many devices affected by this vulnerability still exist in Japan as well. The effect of the attack targeting this vulnerability is lost when the infected router is restarted, so it appears that attacks are carried out repeatedly to reinfect the devices, which explains the large number of attack packets that are observed.

Further, the number of packets targeted to port 23/TCP and sent from IP addresses in Japan has been increasing(*4) since late January. [Figure 4] These packets have the same characteristics seen in Mirai variants.



[Figure 4: Number of observed packets targeted to port 23/TCP and originating in Japan]

JPCERT/CC investigated some of the source IP addresses and found that the packets were sent from broadband routers manufactured by a Japanese vendor, and that the routers in question did not use firmware containing a fix for the SDK vulnerability mentioned above (CVE-2014-8361).

JPCERT/CC is contacting the users of vulnerable routers infected with malware through operators that manage the relevant IP addresses to request implementation of countermeasures.

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）
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 2018

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