JPCERT CC®

Japan Computer Emergency Response Team Coordination Center



JPCERT-TBM-2018-01

Issued: 2018-1-18

# JPCERT/CC Internet Threat Monitoring Report
# [October 1, 2017 - December 31, 2017]

## 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.

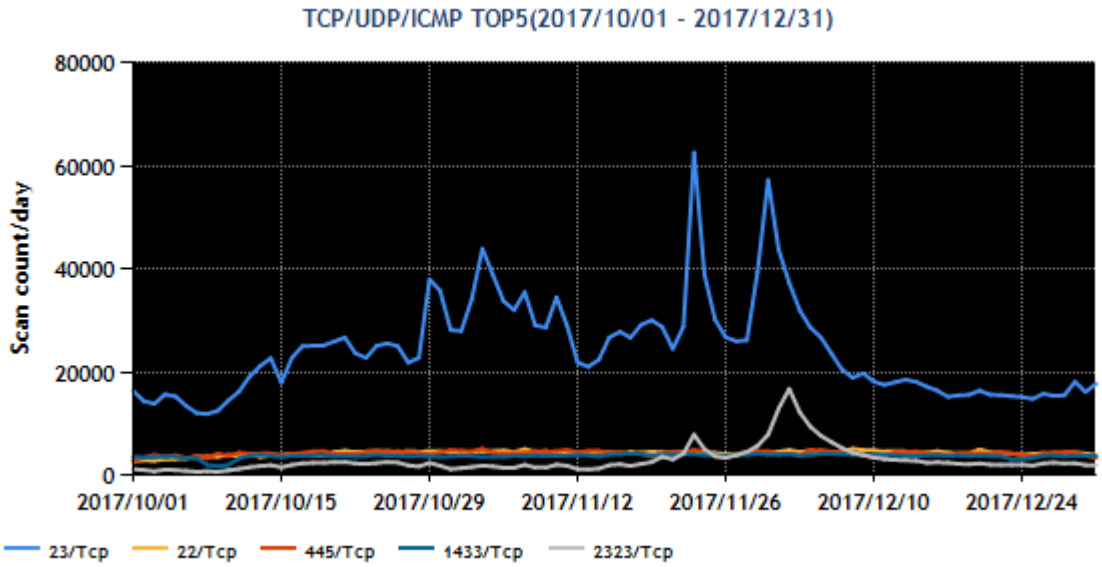
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

| Rank | Destination Port Numbers | Previous Quarter |
|---|---|---|
| 1 | 23/TCP (telnet) | 1 |
| 2 | 22/TCP (ssh) | 3 |
| 3 | 445/TCP (microsoft-ds) | 4 |
| 4 | 1433/TCP (ms-sql-s) | 2 |
| 5 | 2323/TCP | 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 relevant for that service / protocol.

[Figure 1] shows the number of packets received by the top 5 destination ports over the 3 month period.



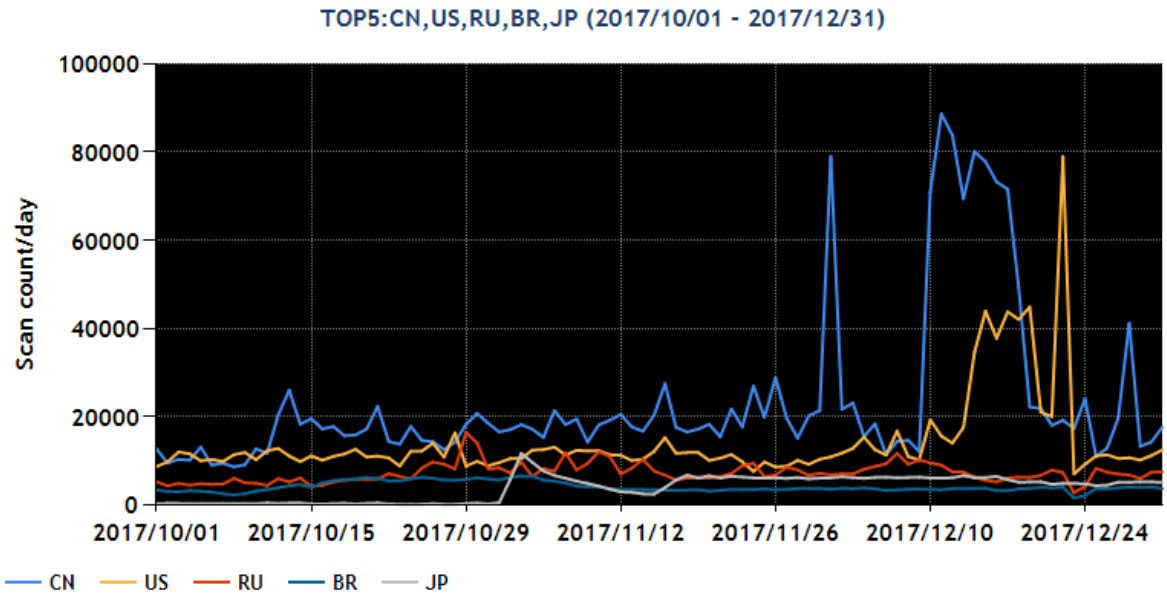

[Figure 1: Number of packets observed at top 5 destination ports from October through December 2017]

The top 5 source regions of packets observed are listed in [Chart 2].

[Chart 2: Top 5 source regions]

| Rank | Source Regions | Previous Quarter |
|---|---|---|
| 1 | China | 1 |
| 2 | USA | 2 |
| 3 | Russia | 3 |
| 4 | Brazil | 7 |
| 5 | Japan | Not in top 10 |

[Figure 2] shows the number of packets sent from the top 5 source regions over the 3 month period.



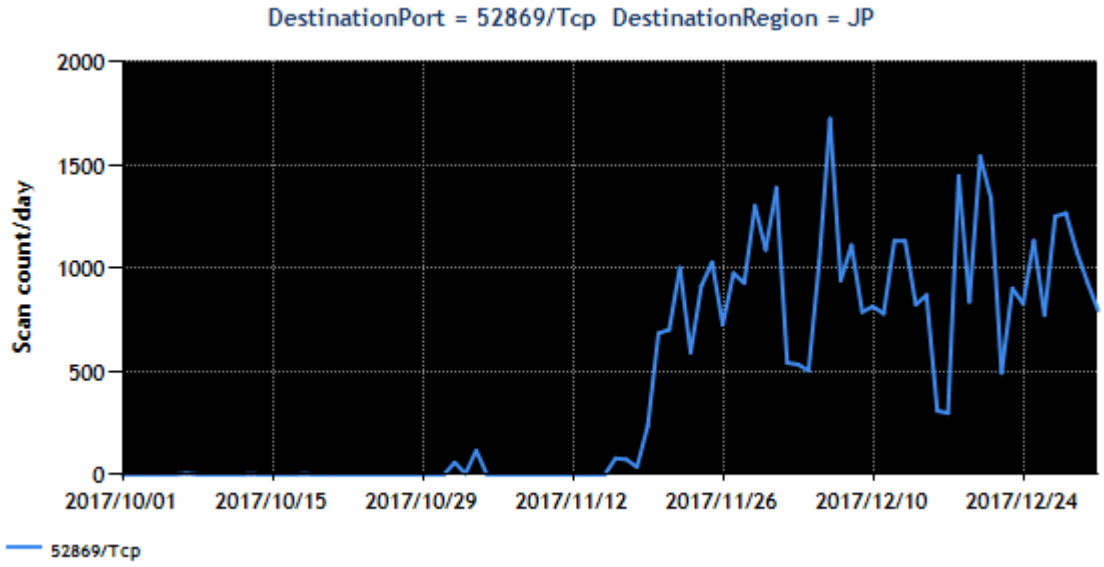

[Figure 2: Number of observed packets of the top 5 source regions from October through December 2017]

During this quarter, a large number of packets targeted to ports for Windows SQL Server and SMB service requests were observed, as in the previous quarter. Packets targeted to ports for SSH (22/TCP) and Telnet (23/TCP) requests, which were in the top 5 list last quarter as well, also continued to be observed, suggesting the presence of continued reconnaissance activities targeting vulnerable webcams, routers, NAS and other devices. In addition, Japan was ranked fifth in the list of top source regions. This is presumably because wireless LAN devices with many users in Japan were subjected to an attack exploiting their vulnerability and infected with a Mirai variant. Otherwise, there were no changes meriting attention.

## 2. Events of Note

### 2.1. Observation of packets targeted to port 52869/TCP

Packets targeted to port 52869/TCP have been observed since around October 30 and around November 15 (Figure 3).

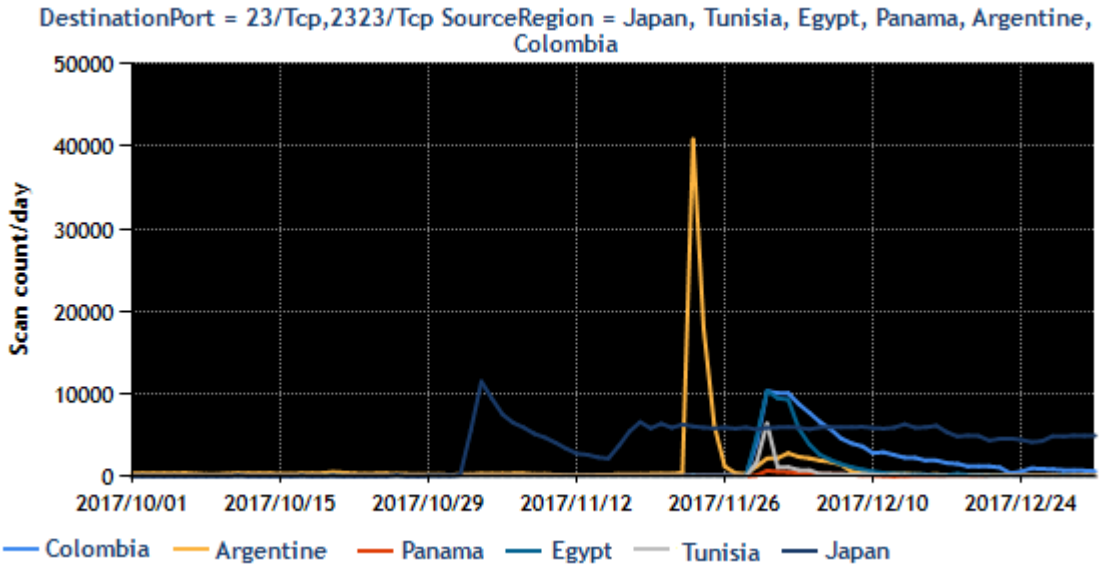



[Figure 3: Number of observed packets targeted to port 52869/TCP]

TSUBAME's sensors are deployed in 21 economic regions including Japan, but the sensors that observed these packets were almost entirely in Japan. This trend continued until November, and since December sensors deployed overseas have also been observing these packets. It is presumed that the packets scanning this port are sent in order to find hosts with the vulnerability in Realtek SDK's miniigd service that was disclosed in April 2015(*2). Since the attack code for this vulnerability is already disclosed on the Internet, attacks can be performed easily. Moreover, upon finding that some of the routers widely used in Japan are affected by this vulnerability if old firmware is used(*3), JPCERT/CC issued an alert on December 19, 2017(*4) to call for early measures . Other organizations have also issued alerts(*5) regarding this matter.

### 2.2. Observation of packets targeted to ports 23/TCP and 2323/TCP

Figure 4 shows the numbers of observed packets targeted to ports 23/TCP and 2323/TCP by major source region. From around the end of October, previously unseen numbers of packets started to be observed.




[Figure 4: Number of observed packets targeted to ports 23/TCP and 2323/TCP by major source region]

The fact that these packets share common characteristics with packets originating from devices infected with Mirai suggests that they originate from devices infected with a Mirai variant. In addition, JPCERT/CC accessed and investigated some of the sources to try to identify the models of infected devices that were sending packets targeted to port 23/TCP from within Japan, but no identifying information other than the fact that port 52869/TCP is open could be obtained.

As shown in Figure 4, packets targeted to port 23/TCP started being observed from around October 30, and this roughly corresponds to the time when packets targeted to port 52869/TCP were temporarily observed, as stated in 2.1. Packets targeted to port 23/TCP subsequently decreased toward November 14, and this also corresponds to the time when packets targeted to port 52869/TCP were not observed, as stated in 2.1. Then from November 15, packets targeted to port 52869/TCP started being observed again, and the number of packets targeted to port 23/TCP from within Japan also increased. Subsequently, the numbers of packets have remained roughly constant. Based on this observation of changes in the numbers of packets, it is possible to envision a scenario, as one possibility, in which packets were sent to port 52869/TCP to scan for vulnerable devices and infect such devices with a Mirai variant, and the infected devices in turn started sending packets targeted to port 23/TCP.

From November 15, packets targeted to port 2323/TCP also started being observed in addition to those targeted to port 23/TCP.

Source regions were no longer confined only to Japan as well: they expanded to include Argentina from around November 23, and Colombia, Panama, Egypt, Tunisia and so on from around November 29(*6). It is presumed that, in all of these regions, vulnerable Internet connection devices(*7) were attacked and infected with a Mirai variant.

## 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) (0Day) Realtek SDK miniigd AddPortMapping SOAP Action Command Injection Remote Code Execution
http://www.zerodayinitiative.com/advisories/ZDI-15-155/

(3) Important notice and request regarding Logitec 300 Mbps wireless LAN broadband routers and set models (11 models) (Japanese)
http://www.logitec.co.jp/info/2017/1219.html

(4) Alert Regarding Mirai Variant Infections
https://www.jpcert.or.jp/english/at/2017/at170049.html

(5) Activities regarding a Mirai variant that is spreading infection by exploiting a vulnerability in router products (December 19, 2017) (Japanese)
http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf
Observation of accesses to destination port 52869/TCP targeting vulnerable routers, and accesses that conduct scans using telnet from within Japan (Japanese)
https://www.npa.go.jp/cyberpolice/important/2017/201712191.html
Alert Regarding the Spread of Mirai Variant Infections (Japanese)
https://wizsafe.iij.ad.jp/2017/12/175/

(6) Mirai Variant Infections Rapidly Increasing in Japan (As of November 2017) (Japanese)
https://sect.iij.ad.jp/d/2017/12/074702.html

(7) Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product
http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

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 2017



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