Japan Computer
Emergency Response Team
Coordination Center

JPCERT CC®

JPCERT-TBM-2018-01
Issued: 2018-4-26

JPCERT/CC Internet Threat Monitoring Report

[January 1, 2018 - March 31, 2018]

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.

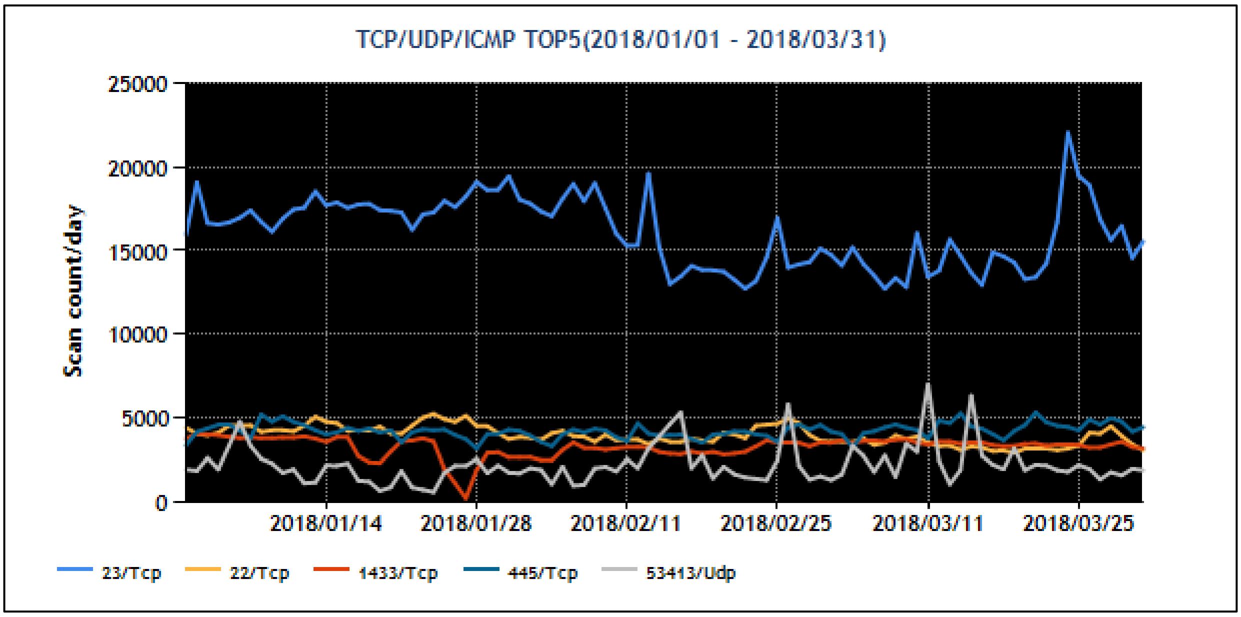
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	22/TCP (ssh)	2
3	1433/TCP (ms-sql-s)	4
4	445/TCP (microsoft-ds)	3
5	53413/UDP	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.



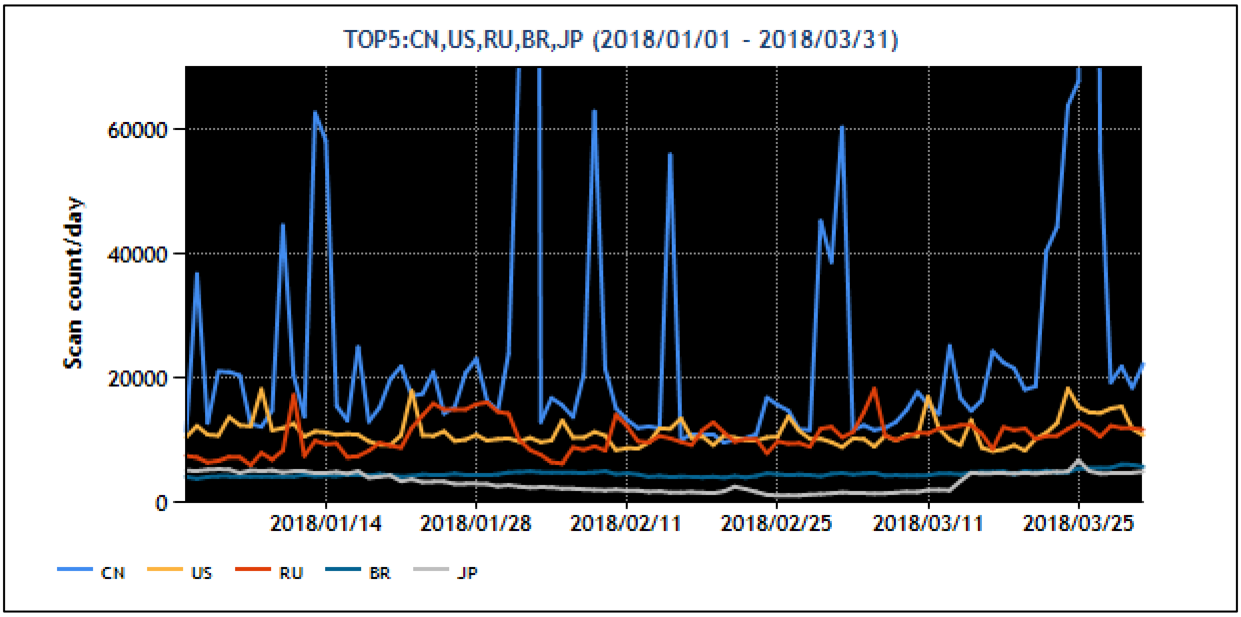
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2018]

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	4
5	Japan	5

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



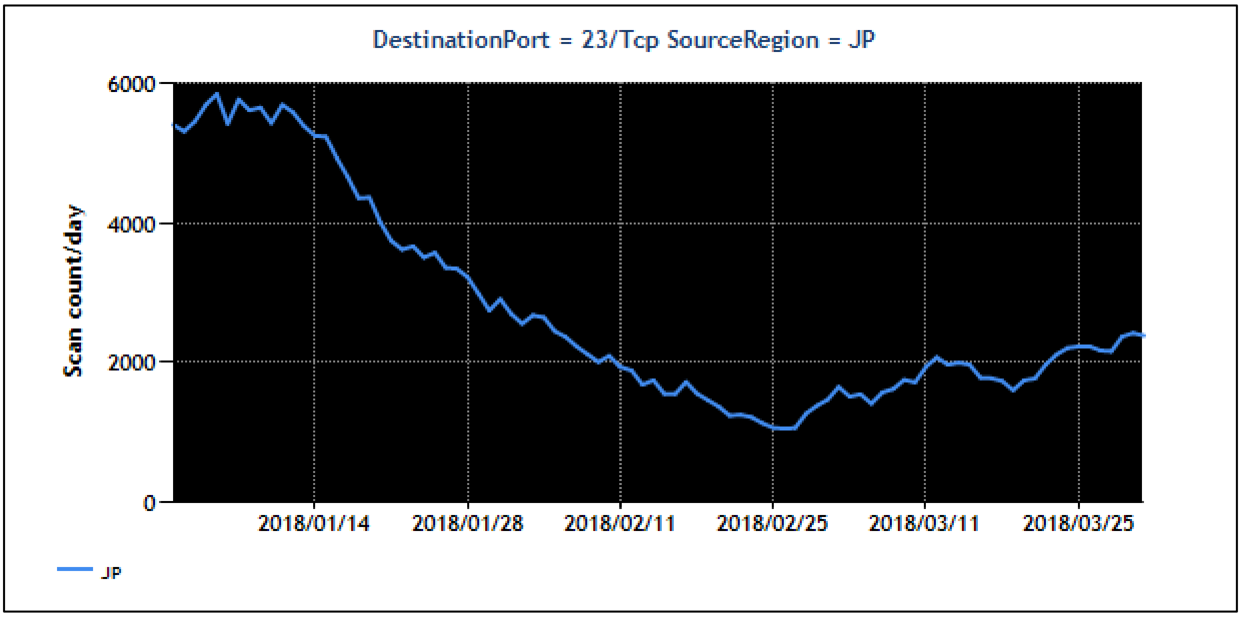
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2018]

During this quarter, a large number of Windows SQL Server and SMB service request packets were observed, as in the previous quarter. The numbers of SSH (22/TCP) and Telnet (23/TCP) request packets observed remained in the top 5 list, suggesting the presence of continued reconnaissance activities targeting vulnerable webcams, routers, NAS and other devices. Moreover, JPCERT/CC continued to observe packets sent with the aim of exploiting a vulnerability in certain wireless LAN routers that used to be sold in Japan in order to infect these devices with a Mirai variant and further spread infection, as described in the previous quarter's report(*2). Otherwise, there were no changes meriting attention.

2. Events of Note

2.1. Observation of packets targeted to port 23/TCP and sent from IP addresses in Japan

[Figure 3] shows how the number of observed packets targeted to port 23/TCP with source IP addresses in Japan has transitioned between January and March. It is assumed that most of these packets originated from devices infected with a Mirai variant.



[Figure 3: Number of observed packets targeted to port 23/TCP]

The attackers behind the Mirai attacks appear to be changing the targets and method used from time to time, sending out different variants for each target and method. Devices infected with Mirai or its variant may be able to prevent infection with another variant by implementing a temporary countermeasure against the attack method used at the time of infection. However, in some cases devices without any drastic countermeasures taken will get out of the infected state when they are restarted by the malware or the users themselves, and then get reinfected with a new Mirai variant. For this reason, the breakdown of devices infected with a Mirai variant has been changing over time on the Internet as a whole.
Changes in the number of observed packets targeted to port 23/TCP can be broken down to indicate the transition in the number of infected devices targeted by each Mirai variant. Accordingly, the following assumptions can be made based on how the number of observed packets targeted to port 23/TCP and sent from within Japan shifted toward the end of February and how the number of packets subsequently increased, as shown in [Figure 3].

- For some time into February, the attackers were trying to infect certain wireless LAN routers previously sold in Japan with a Mirai variant; however, the number of infected devices gradually decreased after the users started implementing countermeasures in response to alerts issued by the device vendor[(*3)], ISPs, security organizations[(*4)] and others.

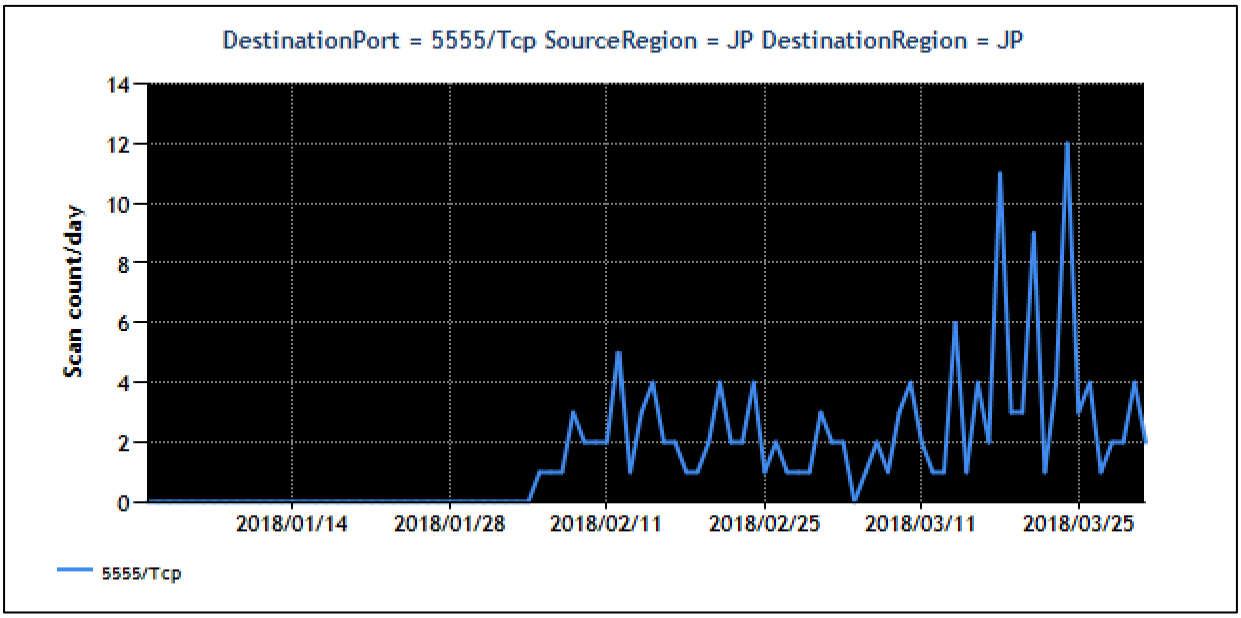
- Around the end of February, the attackers resumed attacks using Mirai variants targeting the same router models mentioned in the previous paragraph; as a result, devices that had gotten out of the infected state by being restarted became reinfected, and packets started being sent again from IP addresses that had temporarily stopped sending packets.

JPCERT/CC provided relevant information to the administrators of the source IP addresses of the packets that were targeted to port 23/TCP and observed again on or after February 26. Some of the administrators responded that they were using the products stated in the alert announced on December 19, 2017, a fact that supports the above assumptions.

Apparently, there are still many devices that are being used without any countermeasures taken. Those who use the applicable routers listed in the alert(*5) to connect to the Internet are advised to take appropriate countermeasures.

2.2. Observation of packets targeted to port 5555/TCP

From around February 4, 2018, JPCERT/CC has been observing packets targeted to port 5555/TCP. These packets are being sent from source IP addresses both in Japan and abroad. The transition in the number of packets sent from IP addresses in Japan is shown in [Figure 4].



[Figure 4: Number of observed packets targeted to port 5555/TCP by major source region]

Since these packets have characteristics in common with packets sent from devices infected with Mirai, it is assumed that these packets originate from devices infected with a Mirai variant. These packets are targeted to port 5555/TCP, and very few packets targeted to other port numbers have been observed. JPCERT/CC accessed some of the sources in Japan to try to identify the models of the infected devices but was only able to confirm that port 5555/TCP was open. No information that identifies the model could be obtained.

In response to inquiries made by JPCERT/CC, some of the administrators of the source IP addresses responded that they were using Internet TV tuners ("TV boxes") manufactured overseas, connected to the Internet without using a router or a firewall.

JPCERT/CC checked the product specifications of the TV boxes in question and found that it used an Android Operating System. Port 5555/TCP, which the packets were targeted to, is a port number used by the daemon running on an Android device that accepts Android Debug Bridge (adb)(*6) commands. This port is not necessary once development is completed and therefore should be closed. It is highly likely that the attackers were scanning for and attacking devices available for remote debugging via a network.

There is a research indicating that malware designed to attempt to mine a cryptocurrency called Monero was using Mirai's code to try to communicate with port 5555/TCP overseas at around the same time(*7). It is conceivable that devices accepting adb commands were installed in Japan as well and were affected by this attack. Since there may be other devices with a similar problem, JPCERT/CC is continuing to gather information.

Any network-connected devices could be subject to attack, so it is recommended that access to these devices be appropriately controlled with a firewall, etc., and that they be monitored for any suspicious traffic.

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) Internet Threat Monitoring Report (Oct-Dec 2017)
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2017Q3_en.pdf

(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) 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/

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

(6) Android Debug Bridge
https://developer.android.com/studio/command-line/adb

(7) ADB.Miner: More Information
http://blog.netlab.360.com/adb-miner-more-information-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/english/tsubame/report/index.html