JPCERT CC®

JPCERT-TBM-2018-03
Issued: 2018-08-02

JPCERT/CC Internet Threat Monitoring Report

[April 1, 2018 - June 30, 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.

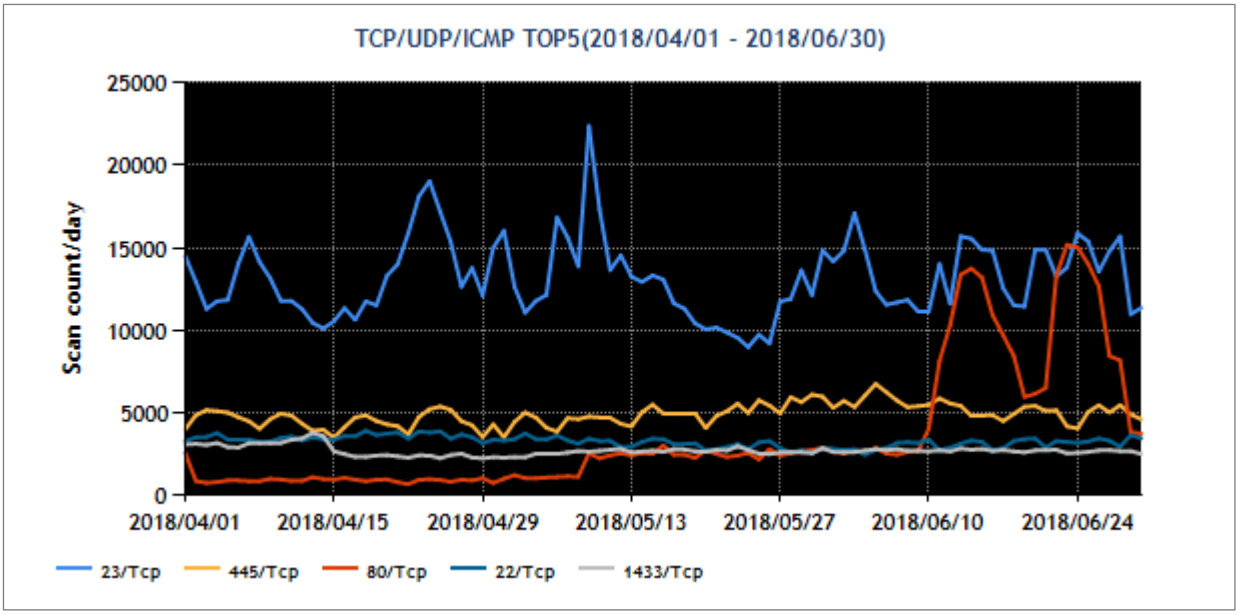
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	4
3	80/TCP (http)	Not in top 10
4	22/TCP (ssh)	3
5	1433/TCP (ms-sql-s)	2

*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.



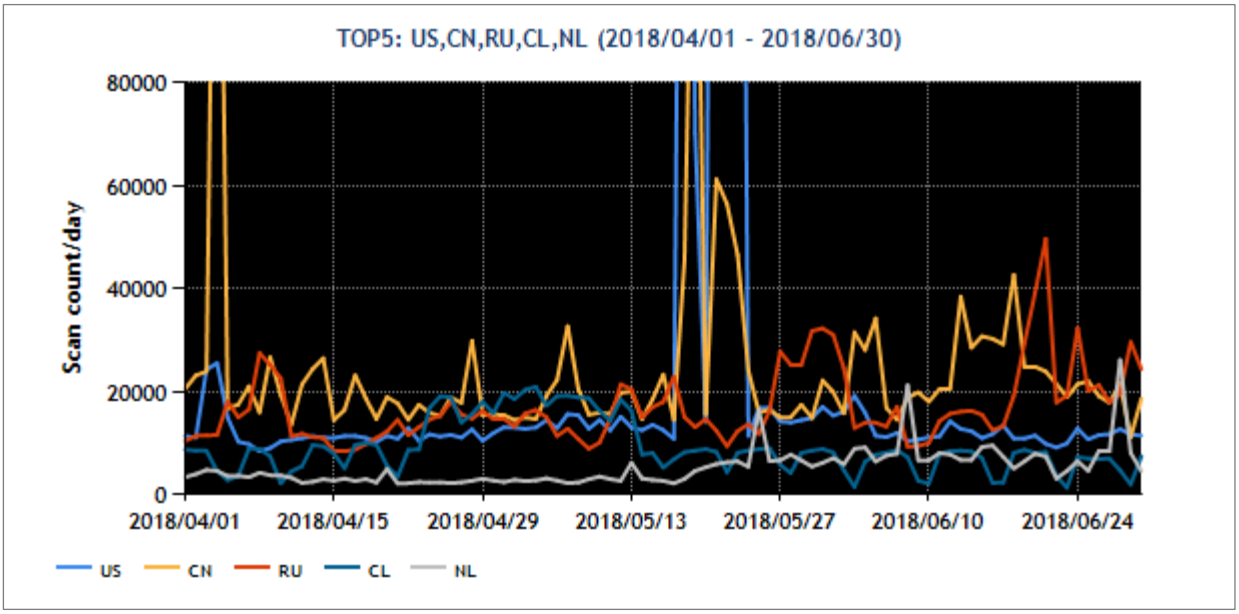
[Figure 1: Number of packets observed at top 5 destination ports from April through June 2018]

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	USA	2
2	China	1
3	Russia	3
4	Chile	Not in top 10
5	Netherlands	7

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



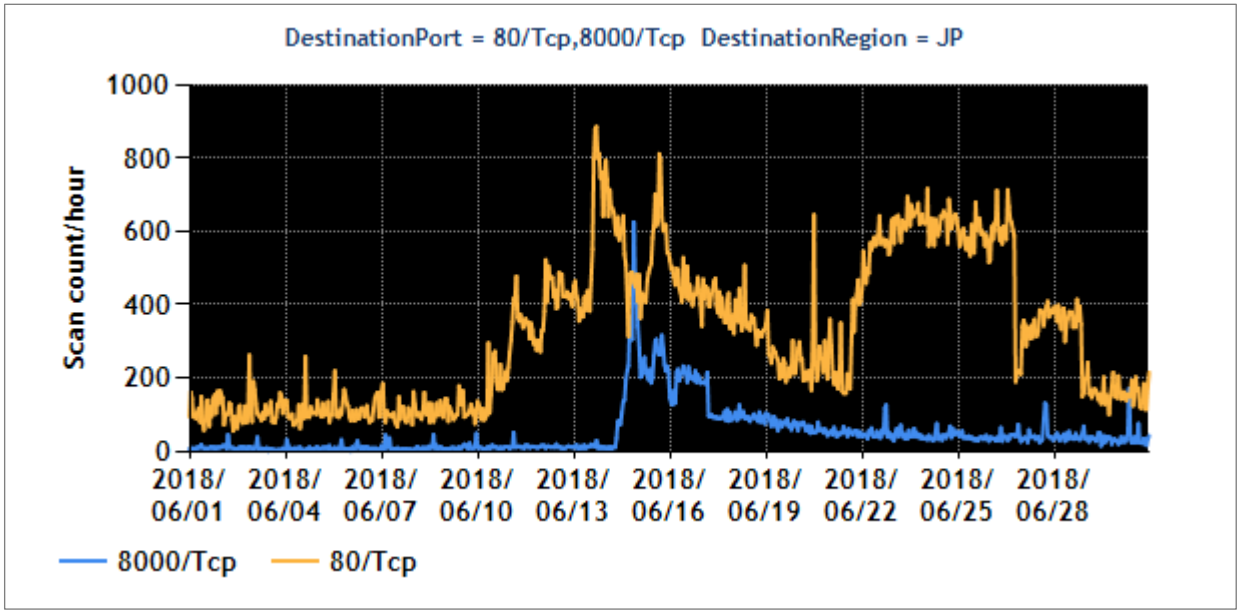
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2018]

The number of packets targeted to 80/TCP has been increasing since mid-June. This will be discussed later in 2.1 Events of Note. Furthermore, packets targeted to ports for Windows SQL Server and SMB service requests were observed, as in the previous quarter. Packets targeted to other destination ports such as 22/TCP and 23/TCP, which were in the top 5 list last quarter as well, also continued to be observed, suggesting the presence of attempts to exploit vulnerabilities in webcams, routers, NAS and other devices. The change in the ranking of source regions is due to continued observation of packets from the Netherlands scanning springboards for UDP reflection attacks, and packets from Chile scanning ports used by platforms for distributed applications.

2. Events of Note

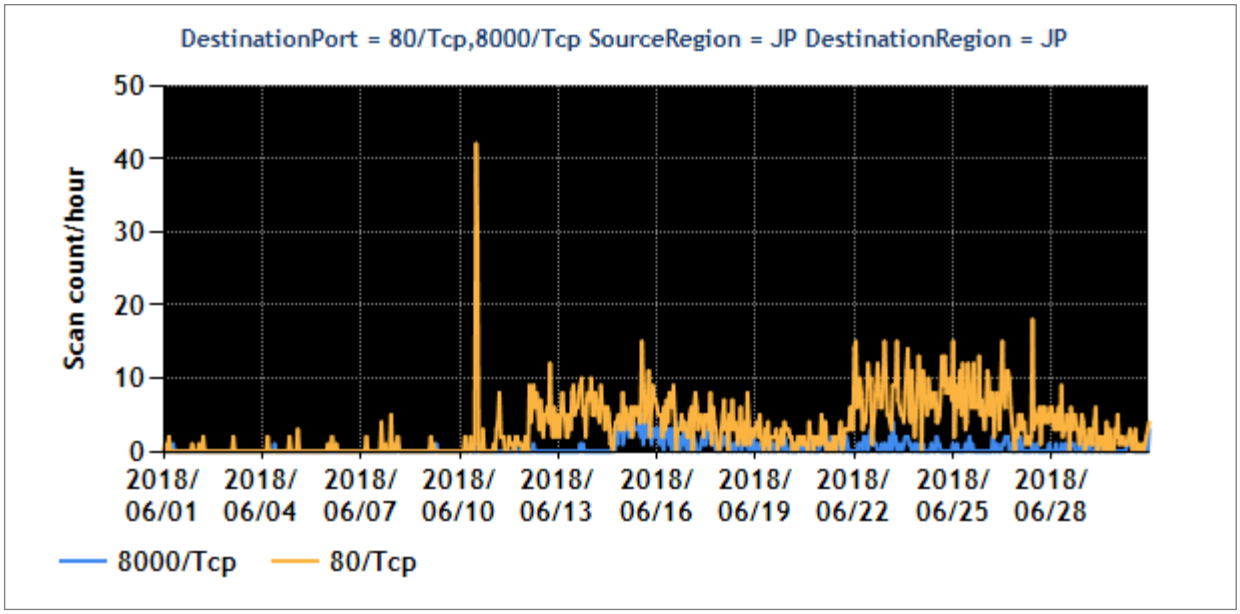
2.1. Increase in the number of packets targeted to ports 80/TCP and 8000/TCP

Packets targeted to port 80/TCP[*2*3*4*5] were continually observed from June 10. Starting on June 14[*6], packets targeted to port 8000/TCP were observed. [Figure 3]



[Figure 3: Number of observed packets targeted to ports 80/TCP and 8000/TCP]

The destination IP addresses and the sequence numbers of TCP headers match, which is a characteristic of packets sent by the Mirai malware. Although source regions vary, packets sent from within Japan were also identified. [Figure 4]



[Figure 4: Number of observed packets sent from Japan and targeted to ports 80/TCP and 8000/TCP]

When some of the source IP addresses for these packets in Japan were accessed, the banner of a "Server: uc-httpd/1.0.0" web server and a login screen that appeared to be of a webcam or recorder were displayed. Published information is available on a number of relevant vulnerabilities in uc-httpd/1.0.0, some of which have exploit code published on the Internet. It is unclear whether the increase in the number of packets observed from June 10 had to do with attacks using the exploit code. JPCERT/CC later obtained access logs confirming attacks by some devices that appear to have used the exploit code against web servers accessible on the Internet.

JPCERT/CC provides packet information observed with TSUBAME to telecommunications carriers and asks them to contact users identified as packet sources.

As for users who use devices such as webcams and recorders directly connected to the Internet, consider prohibiting access to the devices from the Internet. If this is not possible, restrict access to the required minimum using firewall or other means, and change the password from the default password.

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) Destination port 80/TCP seeing increased access with Mirai bot characteristics (Japanese)
https://www.npa.go.jp/cyberpolice/detect/pdf/20180613.pdf

(3) Observation Report for June 2018 (Japanese)
https://www.npa.go.jp/cyberpolice/detect/pdf/20180723_toukei.pdf

(4) Communication targeting 80/TCP increasing
http://blog.nicter.jp/reports/2018-04/mirai-80/

(5) Botnets never Die, Satori REFUSES to Fade Away
https://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/

(6) Satori IoT Botnet Variant
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/

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