JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-TBM-2017-04

Issued: 2017-11-30

JPCERT/CC Internet Threat Monitoring Report [July 1, 2017 - September 30, 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.

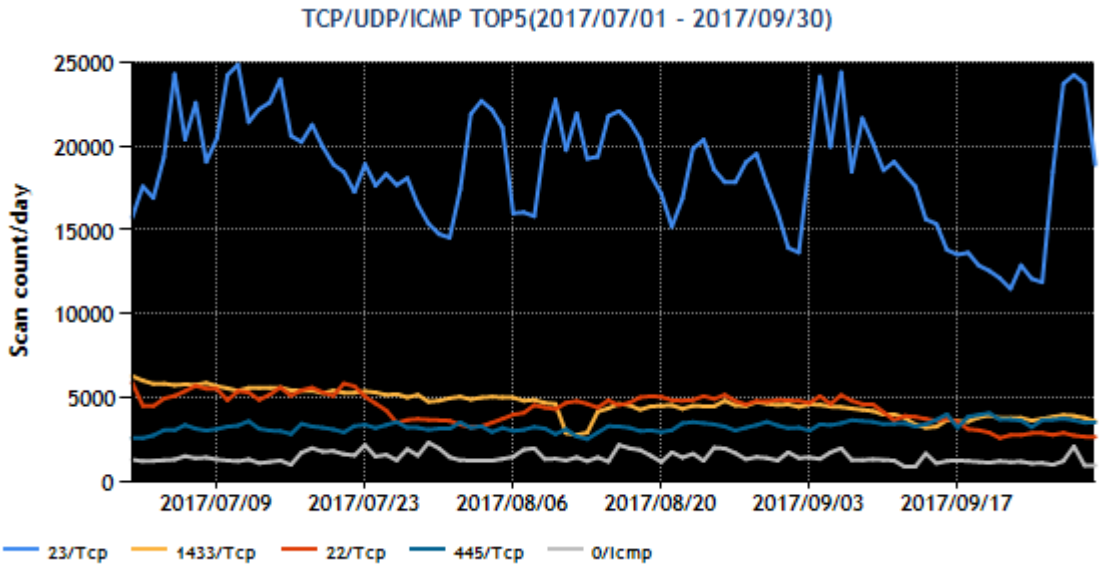
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

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



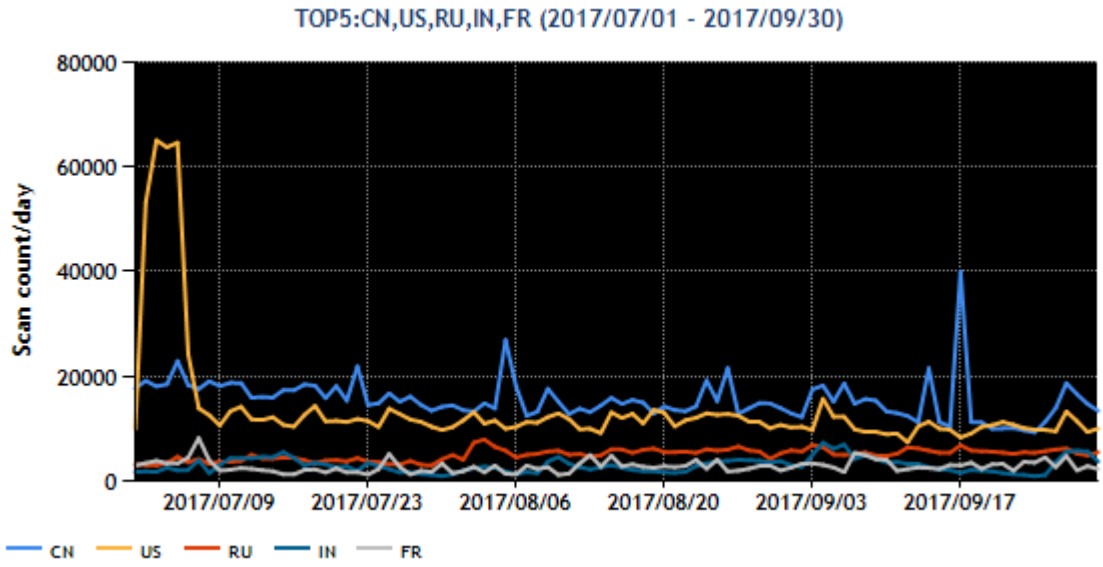
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2017]

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	India	7
5	France	9

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



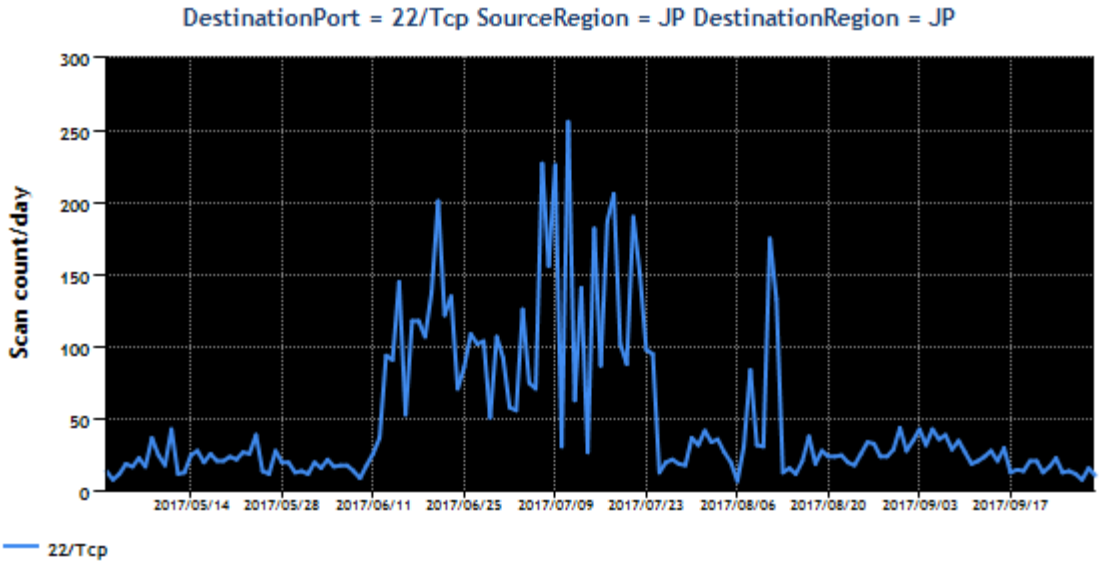
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2017]

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. A large volume of 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. Otherwise, there were no changes meriting attention.

2. Events of Note

2.1. Increase in the number of packets targeted to port 22/TCP

Section 2.1 "Increase in the number of packets targeted to port 22/TCP" of the previous Internet Threat Monitoring Report(*2) noted that packets targeted to port 22/TCP temporarily increased from around June 13, 2017, suggesting attacks against SSH servers, and that some sharp fluctuations were seen before the number of packets fell. These packets are still observed although they have remained at the level after the fall. (Figure 3)



[Figure 3: Number of observed packets targeted to port 22/TCP]

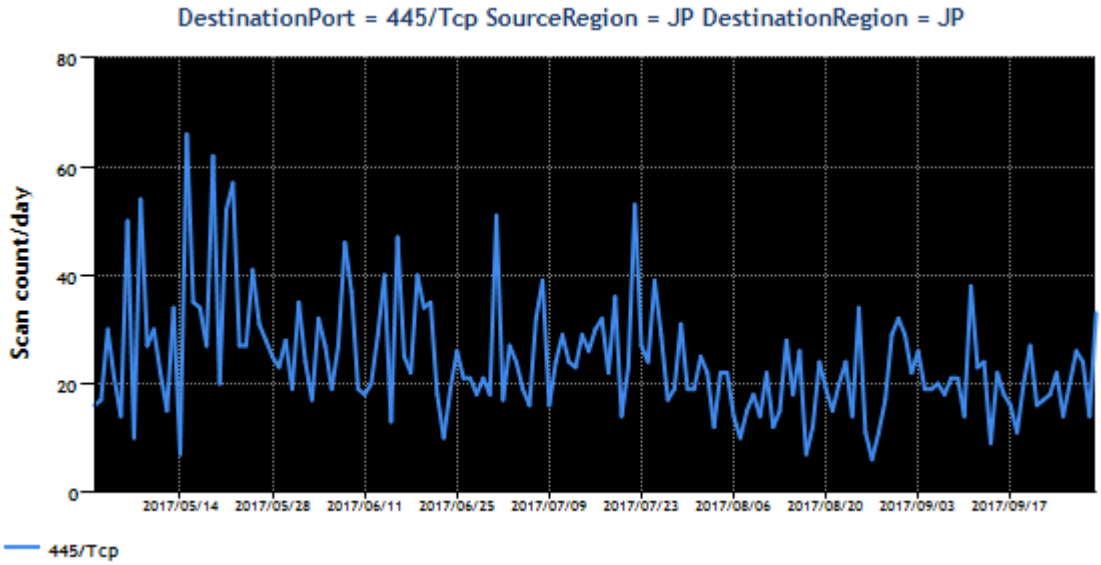
Many of these packets originated from networks that apparently belonged to NTT DOCOMO, which provides mobile communication services in Japan, as well as OCN and NTT Plala, which provide virtual mobile communication services. The presence of distinctive characteristics(*3) in some of the parameters of TCP packets that were continually observed from June suggested that the devices sending the packets were infected with a particular type of malware. JPCERT/CC notified the network operators that manage the source IP addresses and took other necessary steps, while conducting detailed investigations. Specifically, JPCERT/CC obtained honeypot data from other research institutions, listed up a number of login credentials used by the attackers, and attempted to log in to network devices that have a large share in Japan. Through this test, JPCERT/CC confirmed that it was possible to log in to these devices and execute arbitrary code. JPCERT/CC reported the results of this investigation as a vulnerability that allows third parties to remotely execute arbitrary command. Following coordination by relevant institutions, vital information including countermeasure information provided by the product developers was made available through JVN(*4) and other channels on September 12.

After the increase in June, the number of packets fell in late July, but a temporary rise was seen again in early August. Moderate fluctuations were subsequently observed, but the number of packets has been steadily declining following the release of information on JVN. JPCERT/CC has provided information

about observed packets to network operators that manage source IP addresses, and requested them to call on users identified as the sources of these packets to take necessary action.

2.2. Observation of packets targeted to port 445/TCP from within Japan

Packets targeted to port 445/TCP have been continually observed since early May.



[Figure 4: Number of observed packets targeted to port 445/TCP]

JPCERT/CC concluded that these packets were likely originating from devices infected with malware such as WannaCrypt (also known as WannaCry), provided relevant information to operators that manage affected IP addresses, and requested them to look for the presence of infection. As a result, some operators replied that they detected WannaCrypt.

The ransomware WannaCrypt, which spread around the world in early May, and its variants perform reconnaissance activities using port 445/TCP when they are activated in order to search for other unprotected computers so that they may further spread the infection. The packets observed by TSUBAME are related to these reconnaissance activities. In the case of WannaCrypt, if an infected device succeeds in accessing the kill switch, the malware becomes deactivated and stops sending packets to scan for other computers. However, it has been confirmed that some variants of WannaCrypt continue activities to infect other computers even after successfully accessing the kill switch(*5). Since these variants do not encrypt files or display any ransom note, users often do not notice that their computers are infected.

Packets targeted to port 445/TCP continue to be observed, so vulnerable computers that have not applied security updates may be subjected to attacks. JPCERT/CC has also identified new computers located in Japan that are sending scanning packets. Users are advised that they ensure security countermeasures

are taken and check the logs of firewalls, routers, etc. to make sure their devices are not sending out suspicious packets targeted to port 445/TCP.

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 (Apr-Jun 2017)
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2017Q1_en.pdf

(3) Traffic attributed to Hajime and Mirai (Japanese)
https://sect.iij.ad.jp/d/2017/09/072602.html

(4) JVN#68922465 Backdoor found in Wi-Fi STATION L-02F
https://jvn.jp/en/jp/JVN68922465/index.html

(5) WannaCry scare isn't over yet (Japanese)
https://sect.iij.ad.jp/d/2017/09/192258.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 2017 Fiscal Year."