JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2017.09.13 11:19:02 +09'00'

JPCERT-TBM-2017-03

Issued: 2017-08-03

JPCERT/CC Internet Threat Monitoring Report [April 1, 2017 – June 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.

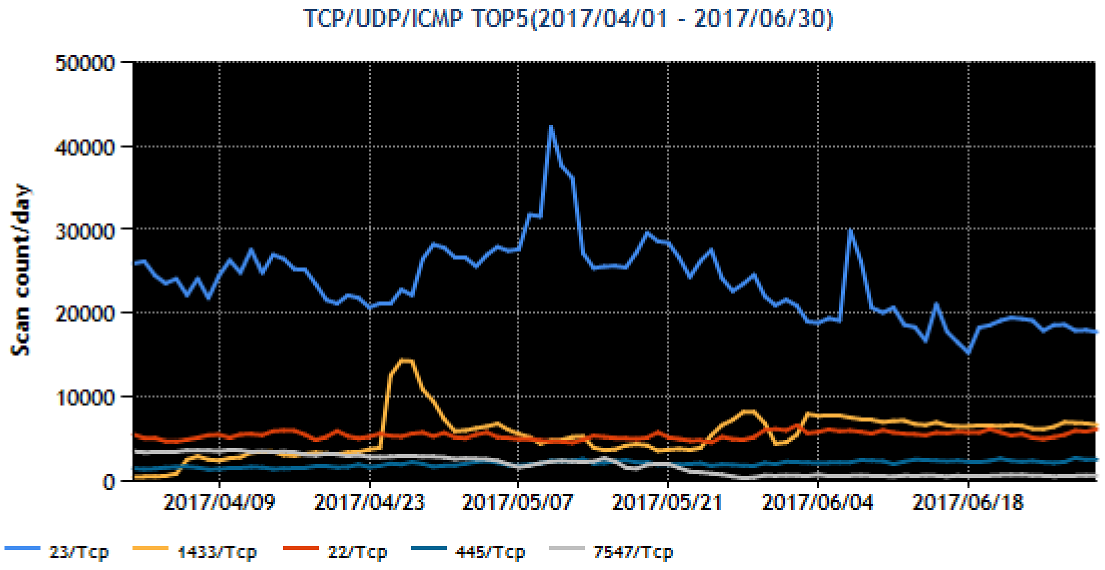
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	1433/TCP (ms-sql-s)	Not in top 10
3	22/TCP (ssh)	3
4	445/TCP (microsoft-ds)	Not in top 10
5	7547/TCP (cwmp)	4

*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.



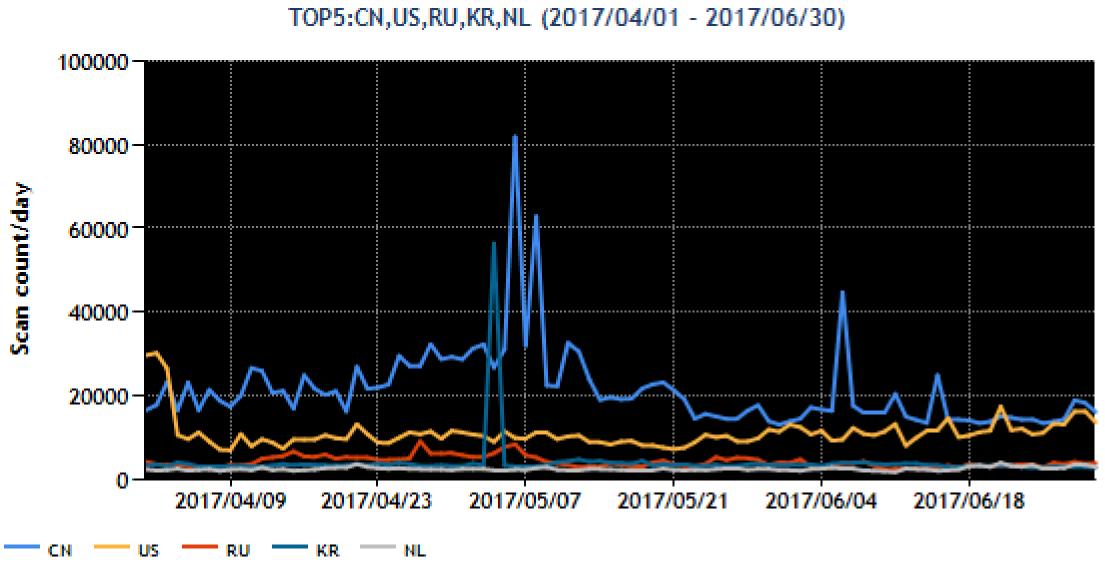
[Figure 1: Number of packets observed at top 5 destination ports from April through June 2017]

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	7
4	South Korea	4
5	Brazil	6

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



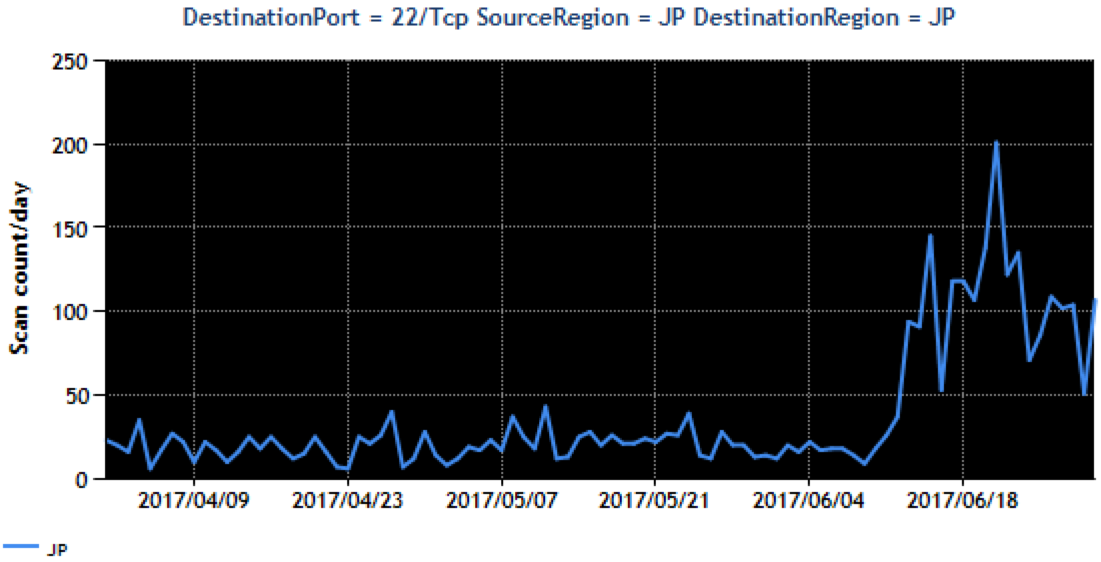
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2017]

During this quarter, a large number of packets targeted to ports for Windows SQL Server and SMB service requests were observed. Packets targeted to other ports such as 22/TCP and 23/TCP, which were in the top 5 list last quarter as well, also continued to be observed. These ports are used by webcams, routers, NAS and other devices made by certain vendors to listen for requests. Otherwise, there were no changes meriting attention.

2. Events of Note

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

Packets sent from domestic IP addresses and targeted to port 22/TCP used by SSH servers started increasing from around June 13, 2017 and continue to be observed despite some fluctuations(*2). (Figure 3)

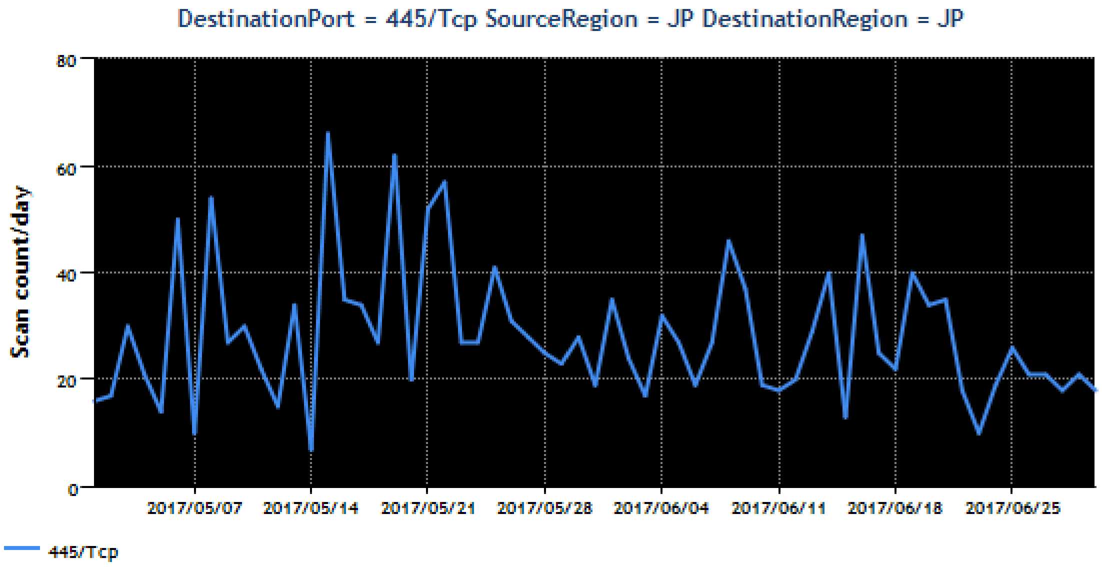


[Figure 3: Number of observed packets targeted to port 22/TCP]

Many of these packets are originating from networks that apparently belong to some mobile network operators and mobile virtual network operators in Japan. JPCERT/CC investigated some of the source IP addresses and observed behaviors that appeared to suggest operations of specialized devices equipped with built-in software. However, no specific product name or vendor has been identified so far. JPCERT/CC has provided the log data of observed packets to network operators and requested them to contact users of the devices that are identified as the sources of these packets.

2.2. Increase in the number of packets targeted to port 445/TCP from within Japan

The number of packets targeted to port 445/TCP has increased since early May. The ransomware WannaCry and its variants, which were infecting computers around the world around this time, perform reconnaissance activities when they are activated to search for other unprotected computers so that they may further spread the infection. JPCERT/CC believes the recent increase in the number of these packets was connected with the global spread of the malware WannaCry(*3,*4).



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

Suspecting the possibility that the sources of these packets may have been infected with malware, JPCERT/CC is working to provide information to the administrators of these IP addresses and request them to check for the existence of an infection. Some of the administrators have responded that malware has been detected.

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) Access to port 22/TCP from within Japan increases
https://www.jpcert.or.jp/newsflash/2017070701.html

(3) Observation of access to port 445/TCP, which appears to be attempts originating from computers infected with the ransomware WannaCry to infect other computers
https://www.npa.go.jp/cyberpolice/important/2017/201705191.html

(4) Observation of access to port 445/TCP, which appears to be attempts originating from computers infected with a variant of the ransomware WannaCry to infect other computers
https://www.npa.go.jp/cyberpolice/important/2017/201706221.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."

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