JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-IA-2017-02

Issued: 2017-05-11

JPCERT/CC Internet Threat Monitoring Report [January 1, 2017 - March 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. This report will mainly show the analysis results of packets targeted to Japan during this quarter.

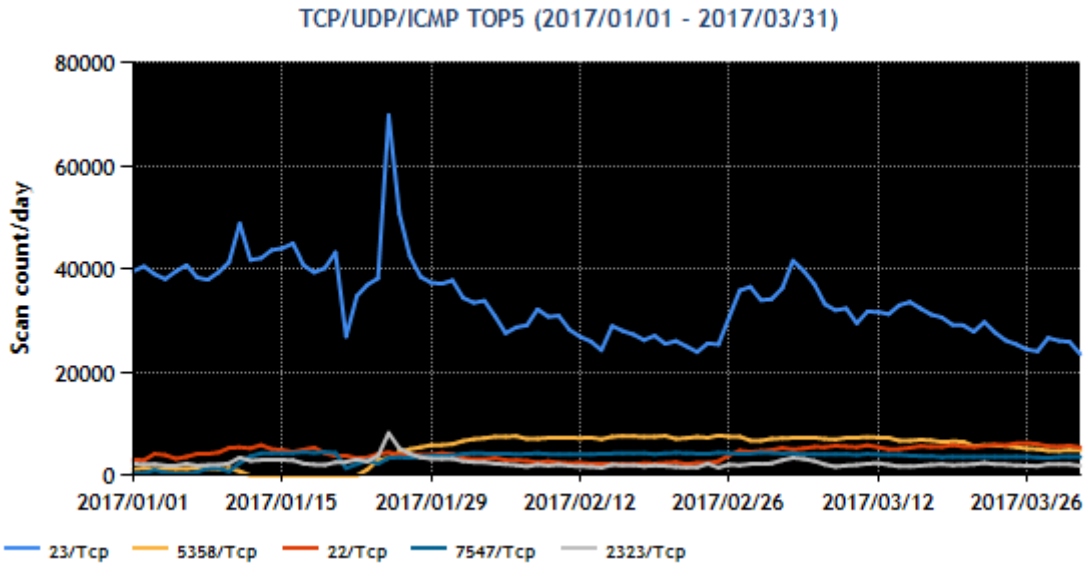
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	5358/TCP	Not in top 10
3	22/TCP (ssh)	4
4	7547/TCP	3
5	2323/TCP	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.



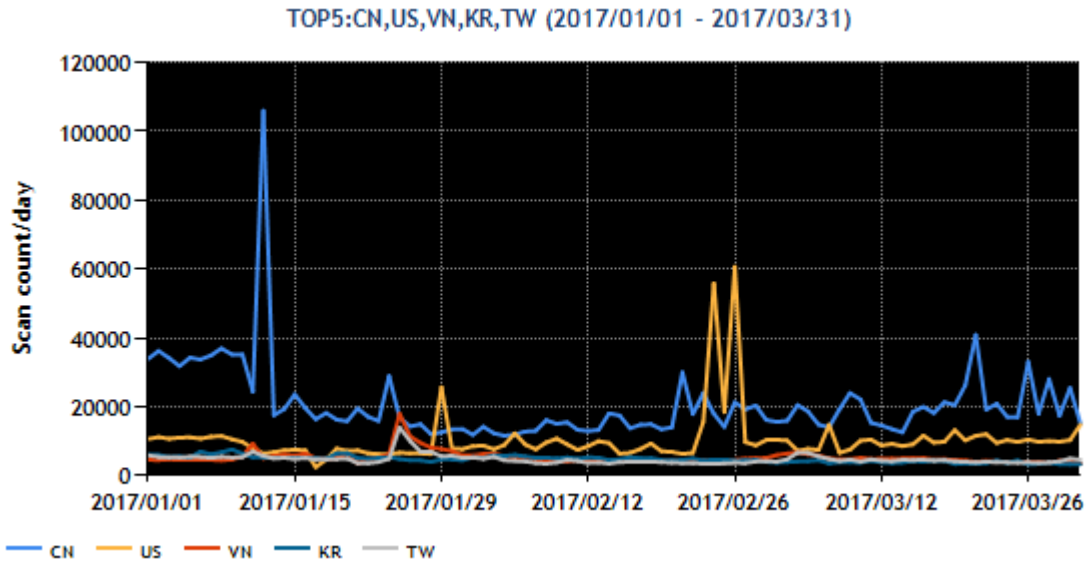
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2017]

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	Vietnam	4
4	South Korea	5
5	Taiwan	3

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



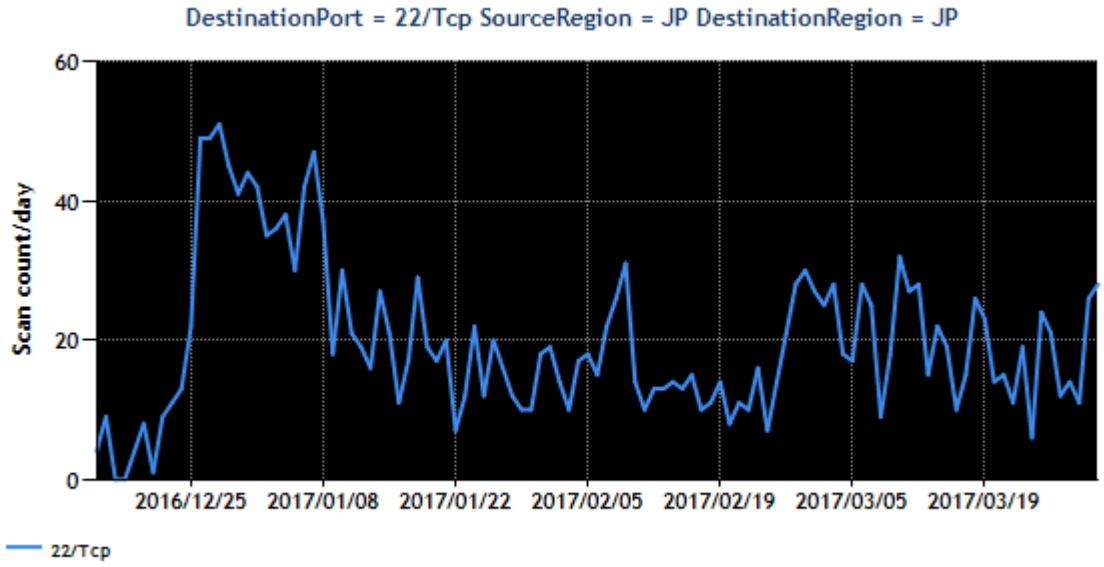
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2017]

During this quarter, a more than usual number of packets targeted to 22/TCP, 23/TCP and certain other ports (which fairly common devices are believed to use to listen for requests) were observed in major regions. This trend was particularly notable in Vietnam and South Korea, pushing both regions up one notch in the ranking of top 5 source regions. The ratio of packets among destination ports where an increase was seen was largely the same in all source regions. 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 ports used by SSH servers started increasing from around December 25, 2016 and continue to be observed despite some fluctuations. (Figure 3)



[Figure 3: Number of observed packets targeted to port 22/TCP in the top 10 regions]

JPCERT/CC randomly extracted a number of these packets and investigated their sources. The results showed that about half originated from foreign-made NAS devices.

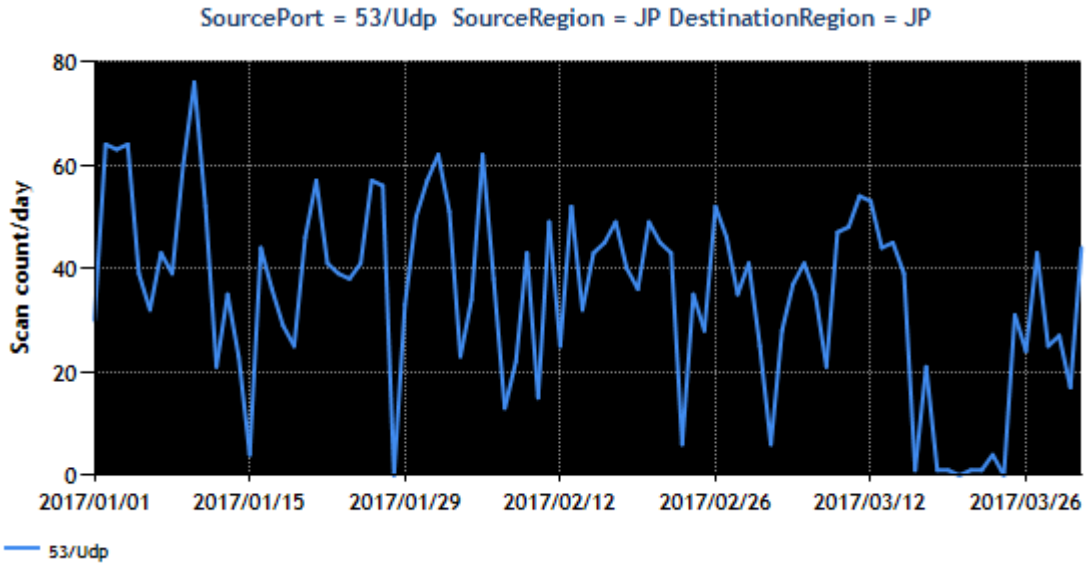
These NAS products allow users to configure web server, telnet, SSH and other services as additional functions. While the existence of any causality is yet unclear, JPCERT/CC has confirmed cases where it is suspected that the NAS may be sending packets due to an infection with malware as a result of an attack on a function that the user had added.

There were also cases where an HTML content intended to redirect users to a phishing site was placed on a server with an active web server function.

Users and administrators of these products are advised to check access logs, etc., to make sure telnet, SSH and other services that can be used by a third party to remotely gain access are not activated unintentionally.

2.2. DNS Water Torture attacks using open resolvers, etc., in Japan

During this quarter, TSUBAME has continued to receive reply packets sent from numerous IP addresses around the world in response to DNS queries. JPCERT/CC analyzed these packets and found that they were answer packets sent in response to name resolution request packets that contain nonexistent random host names. These answer packets are believed to be responses to name resolution request packets sent by a third party to open resolvers using spoofed IP addresses of TSUBAME's sensors, as part of a DNS Water Torture attack. See Figure 4 for trends in the number of packets sent from source port 53/UDP.



[Figure 4: Number of observed packets sent from port 53/UDP]

Open resolvers are believed to be a breeding ground supporting DNS Water Torture attacks, which is an attack method with a severe impact. As such, JPCERT/CC has been conducting activities to provide information to administrators of organizations that have open resolvers and request that they take appropriate steps. Some of the administrators have responded that, after investigating their routers to determine whether they are open resolvers, they implemented countermeasures such as updating the firmware and setting filter rules.
JPCERT/CC will continue to work to reduce open resolvers.

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

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 2016