Japan Computer Emergency
Response Team Coordination
Center

JPCERT/CC®

JPCERT-IA-2017-01
Issued: 2017-02-09

JPCERT/CC Internet Threat Monitoring Report
[October 1, 2016 - December 31, 2016]

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.

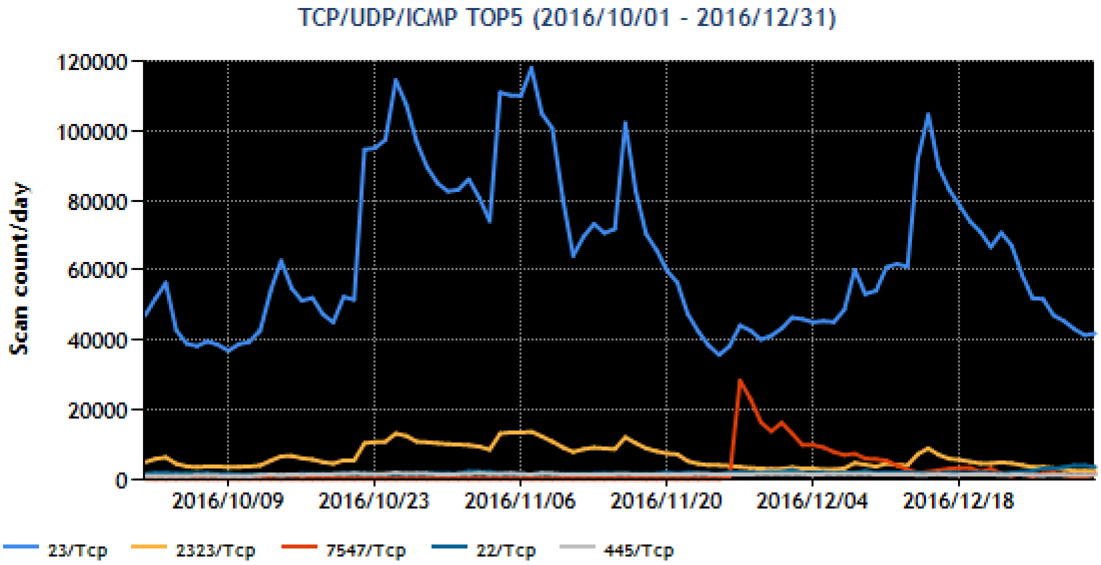
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	2323/TCP	Not in top 10
3	7547/TCP	Not in top 10
4	22/TCP	3
5	445/TCP (microsoft-ds)	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.



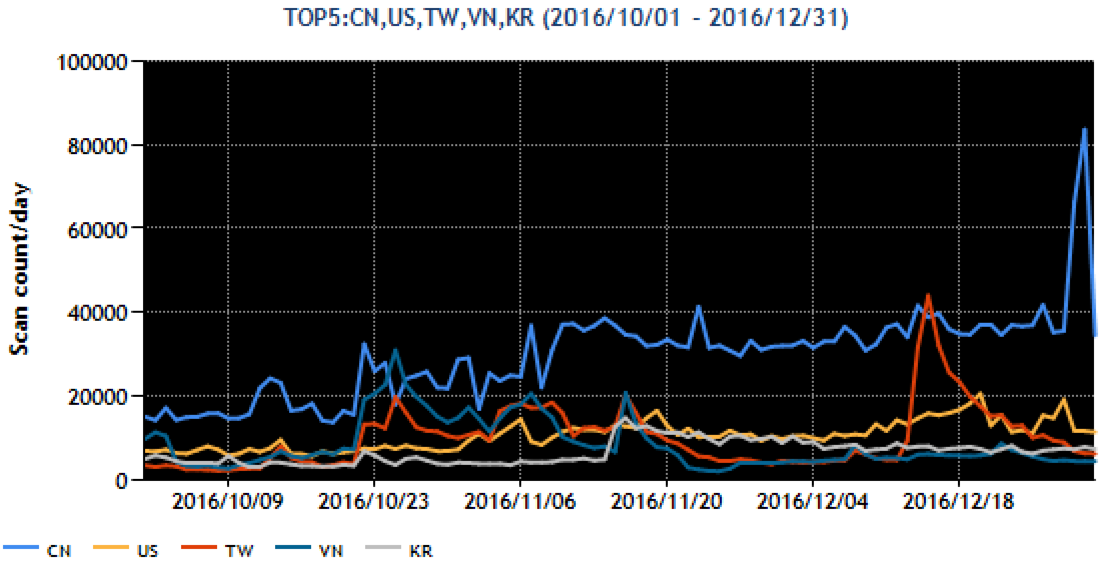
[Figure 1: Number of packets observed at top 5 destination ports from October through December 2016]

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	Taiwan	6
4	Vietnam	4
5	South Korea	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 October through December 2016]

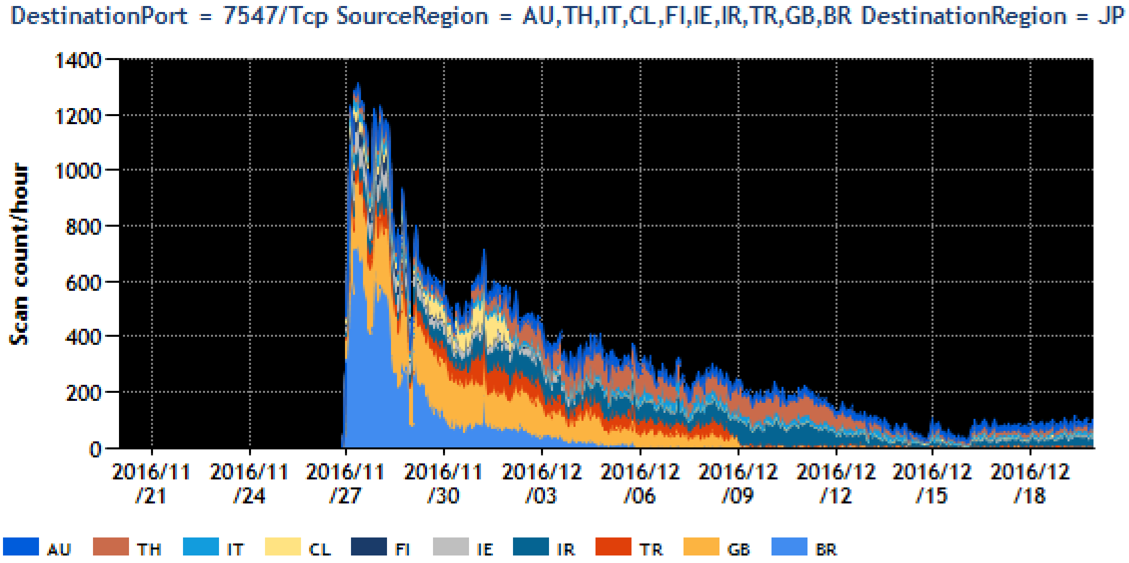
During this quarter, there was an increase in the number of packets targeted to ports including 23/TCP that are believed to be mainly used by devices, and these ports made up the top 3. Packets targeted to a number of other ports also increased. This increase will be discussed in detail in "2.1 Increase in the number of packets targeted to devices." Next, with regard to the top 5 source regions, Taiwan rose to third place from sixth in the previous quarter. Taiwan's rise to the top 5 is attributable to the fact that it was the source region for about 13% of the packets targeted to 23/TCP, which was the top destination port and accounted for nearly 55% of the total number of packets observed. While some minor fluctuations were seen in other regions, there were no changes meriting attention.

2 Events of Note

2.1 Increase in the number of packets targeted to devices

In "2.1 Increase in the number of packets targeted to port 23/TCP" of the previous issue of the Internet Threat Monitoring Report (July-September 2016), JPCERT/CC reported increased activities by the Mirai malware. Increased numbers of packets targeted to ports 23/TCP and 2323/TCP continued to be seen during this quarter as well. Packets targeted to a number of other ports were also observed, presumably a sign that the disclosure of Mirai's source code led to the creation of a variant.

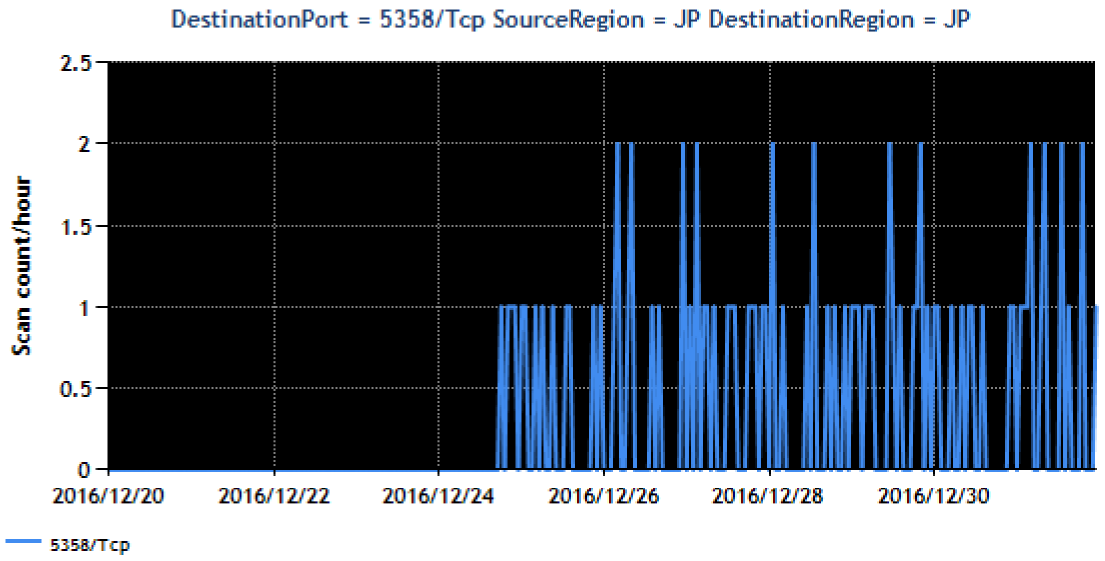
As shown in Figure 1, packets targeted to 7547/TCP were the third most observed packets. To see how the number of packets varies by region, the observation results for the top 10 regions are shown graphically in Figure 3.



[Figure 3: Number of observed packets targeted to port 7547/TCP in the top 10 regions]

Packets originating in a number of regions including Brazil, the UK and Turkey increased at around the same time, and then they gradually decreased. The speed at which they decreased varied by region. In many of the regions, it was reported that the transmission of packets was due to vulnerabilities in network devices used to connect to ISPs[*2,3,4]. Based on the reported information, JPCERT/CC investigated product information and found a number of products that applied. In many cases, however, ISPs assign new model numbers to devices when distributing them to the users, instead of using the numbers given by the manufacturers, making it difficult to identify products with their model numbers. For this reason, ISPs in the regions where a large number of packets were transmitted had to call on manufacturers to provide modified firmware, announce information on how to restore suspended routers, and handle other relevant tasks. As such, JPCERT/CC decided that it would be difficult to search for vulnerable devices used in Japan based on model numbers issued overseas, and gathered information about cases of failure that occurred in Japan and other data to see if there is any occurrence of events in which devices infected with malware act as a springboard. Since only one packet was transmitted during the period in question, and no related announcements or reports of failures or emergency responses are known to have been made, it is presumed that the impact was small in Japan.

Next, changes in the number of packets sent from IP addresses in Japan and targeted to port 5358/TCP, observed from around December 24, 2016, are shown in Figure 4.



-

[Figure 4: Number of observed packets targeted to port 5358/TCP in Japan]

JPCERT/CC checked the status of packet transmission up to December 24 and found that packets exhibiting the characteristics of Mirai were sent from these source IP addresses to ports 23/TCP and 2323/TCP. Accordingly, it is presumed that the devices installed at the source of these packets were already infected with Mirai.

In an effort to reduce suspicious packets, JPCERT/CC has been carrying out investigations to infer the models of devices installed at the source of the packets. Considering the possibility that the behavior of the Mirai malware or its variant may have changed, JPCERT/CC investigated these hosts this time again. As a result, while no particular models were identified, some common characteristics were found among the packet sources, providing insights about the devices. JPCERT/CC provided TSUBAME's observation data and information about the inferred devices to the supposedly relevant vendor, and packet logs to the administrators (mostly ISPs) of IP addresses from which packets were sent to 5358/TCP.

As a result, it appears that users who received information from the ISPs contacted the product vendor, leading to investigation of the phenomena observed. The investigation findings shed light on how the devices get infected with malware.

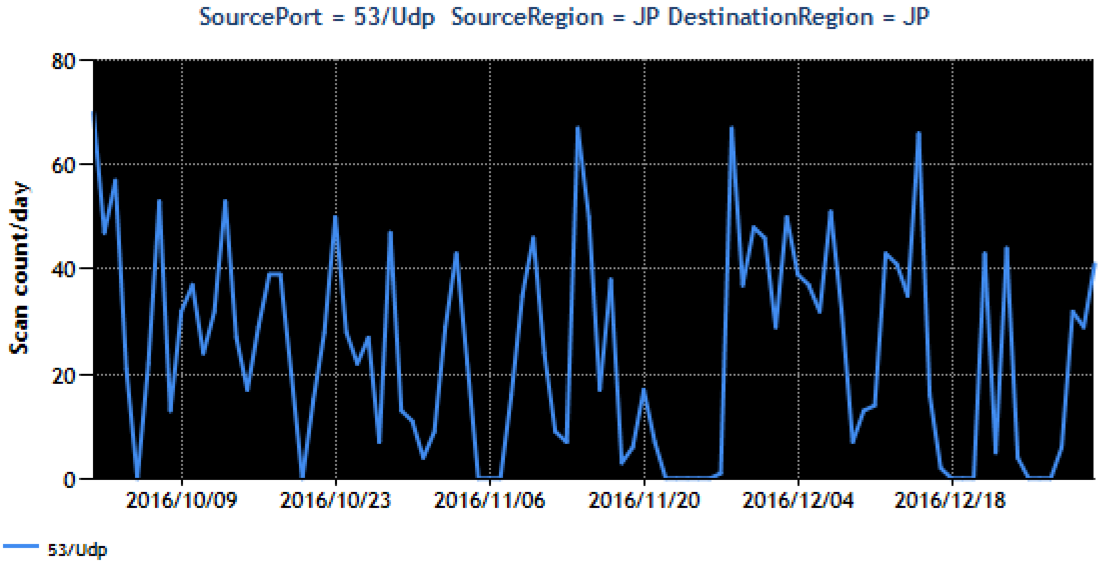
The products in question get infected with malware only when a certain condition is met. JPCERT/CC continues to provide information about malware behavior to vendors to help them devise countermeasures, as well as redoubling efforts to contact administrators of source IP addresses.

Additional events were seen later, including cases in which devices that are apparently infected with

Mirai send packets to the port of a surveillance camera product with a known vulnerability(*5,6). It is presumed that attackers use Mirai and its variant to scan for devices that can be accessed via the Internet, and carry out attacks on those with security issues, including unaddressed vulnerabilities and use of the default password and other settings.

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

TSUBAME has been receiving 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 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 5 for trends in the number of packets sent from source port 53/UDP.



[Figure 5: Number of observed packets sent from port 53/UDP]

A DNS Water Torture attack using open resolvers, etc., is believed to be an attack method with a severe impact. As such, JPCERT/CC has resumed activities to provide information to administrators of organizations that have open resolvers and request that they take appropriate steps. Some of the administrators have already replied with investigation results, including improper filtering rules of routers. JPCERT/CC will continue to work to reduce open resolvers in an effort to help keep DNS Water Torture attacks in check.

3 References

(1) Service Name and Transport Protocol Port Number Registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) New Variant of Mirai Embeds Itself in TalkTalk Home Routers
https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html

(3) New Mirai Worm Knocks 900K Germans Offline ?
https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

(4) TR-069 NewNTPServer Exploits: What we know so far
https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/

(5) Surge in Access Believed to be Caused by Variant of Mirai Bot Attempting to Infect <Japanese only>
https://www.npa.go.jp/cyberpolice/detect/pdf/20170120.pdf

(6) Alert Regarding Management of Devices Connected to the Internet <Japanese only>
https://www.jpcert.or.jp/at/2016/at160050.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 2016

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