JPCERT-IA-2016-03
Issued: 2016-11-16

JPCERT/CC Internet Threat Monitoring Report [July 1, 2016 - September 30, 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].

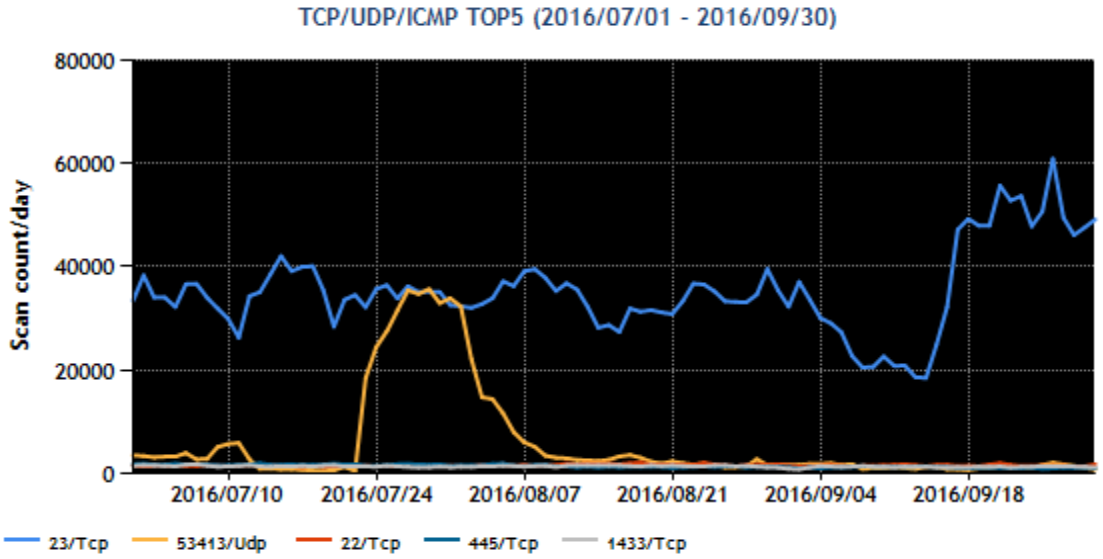
[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	53413/UDP	2
3	22/TCP	6
4	445/TCP (microsoft-ds)	5
5	1433/TCP (ms-sql-s)	3

*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.



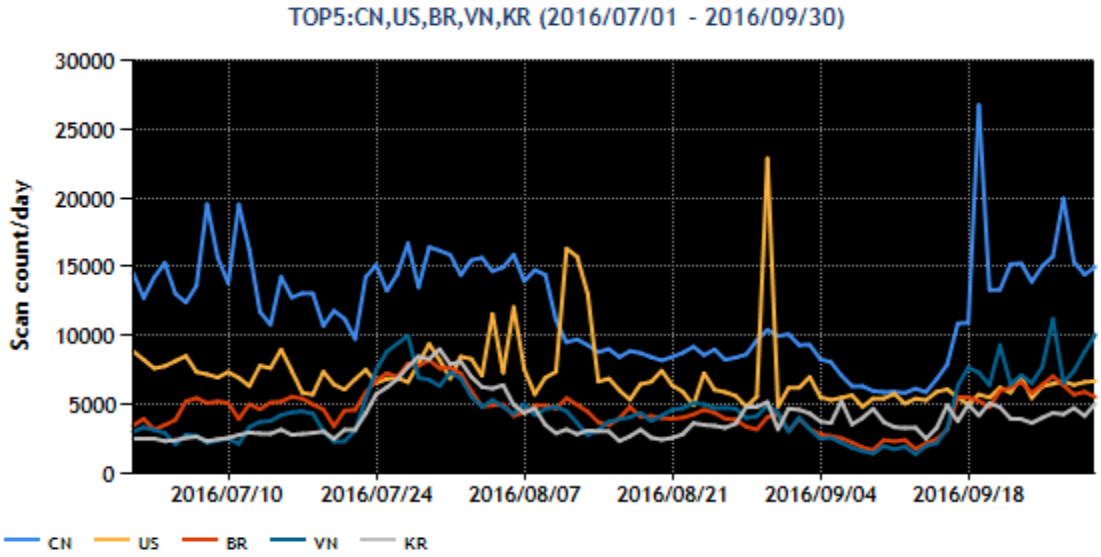
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2016]

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	Brazil	3
4	Vietnam	7
5	South Korea	5

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



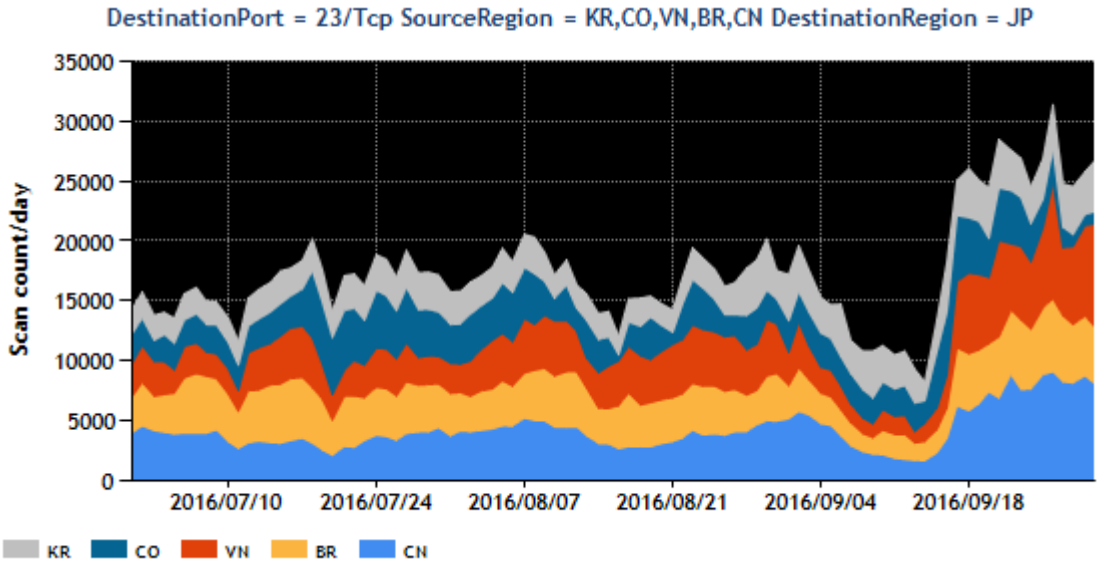
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2016]

During this quarter, there was a sharp increase in the number of packets targeted to port 23/TCP around September 15. This phenomenon will be discussed in detail in "2.1 Increase in the number of packets targeted to port 23/TCP". Furthermore, increased numbers of packets targeted to port 53413/UDP were observed for about 2 weeks from July 23. This phenomenon is believed to be the result of reconnaissance and attack activities targeting foreign-made routers as in similar phenomena observed in the past. There is nothing in particular worth noting with regard to the remainder of the top 5 destination ports. Next, with regard to the top 5 source regions, Vietnam rose to fourth place from seventh in the previous quarter. This is because Vietnam was the source region for about 10% of the packets targeted to 23/TCP, which was the top destination port and accounted for more than half 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 port 23/TCP

From around September 17, 2016, JPCERT/CC has been observing increased numbers of packets targeted to port 23/TCP. The increase in the number of packets was not limited to a certain source region but was observed in multiple regions (Figure 3). Furthermore, @police reported an increase in the number of packets that appear to be scanning ports 23/TCP and 2323/TCP as well as increased activities by the Mirai malware, which attempts to log into websites running telnet(*2). These reports seem to corroborate TSUBAME's observation results.



[Figure 3: Number of packets targeted to port 23/TCP]

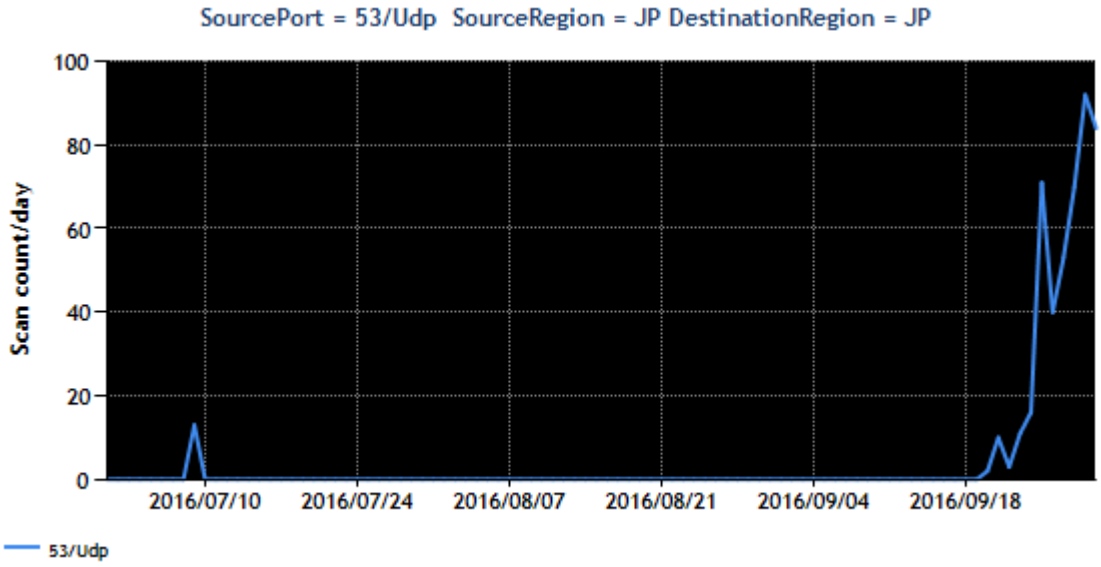
Investigation into the source of the packets scanning port 23/TCP, etc., often leads to specific product models or reveals that IP addresses managed by specific ISPs are assigned. The former is often due to a problem in the initial setup process after the product is introduced, and the latter is presumably due to a problem on the part of the service providers deploying a large number of devices on specific networks.
As part of its efforts to reduce the number of suspicious packets, JPCERT/CC has been investigating devices installed at source IP addresses to infer their models and providing information to the manufacturers, with the expectation that they would improve the products, and to the relevant ISPs, with the expectation that they would issue notices urging the users of the devices to change settings. To address the latter problem, JPCERT/CC started new activities in this quarter to identify vendors that deploy numerous surveillance cameras and built-in communication equipment for specific industries on networks, and that provide maintenance services. The vendors are identified using the following information and requested to take appropriate steps.

- Responses from web servers operating on port 80, etc., at source IP addresses
- Strings sent when requesting login using telnet, SSH, etc.

During this quarter, JPCERT/CC provided information to one equipment manufacturer and one service provider.

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 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]

DNS Water Torture attacks originating in Japan using open resolvers, etc., have been observed since September 20. Although DNS Water Torture attacks started to be seen frequently from around 2014, they had not been observed for some time. The reason these attacks are now being observed again is unclear. 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) @police
Internet Monitoring Results (Sep 2016) <Japanese only>
https://www.npa.go.jp/cyberpolice/detect/pdf/20161020.pdf

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