JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IA-2016-03
Issued: 2016-08-25

JPCERT/CC Internet Threat Monitoring Report

[April 1, 2016 - June 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.

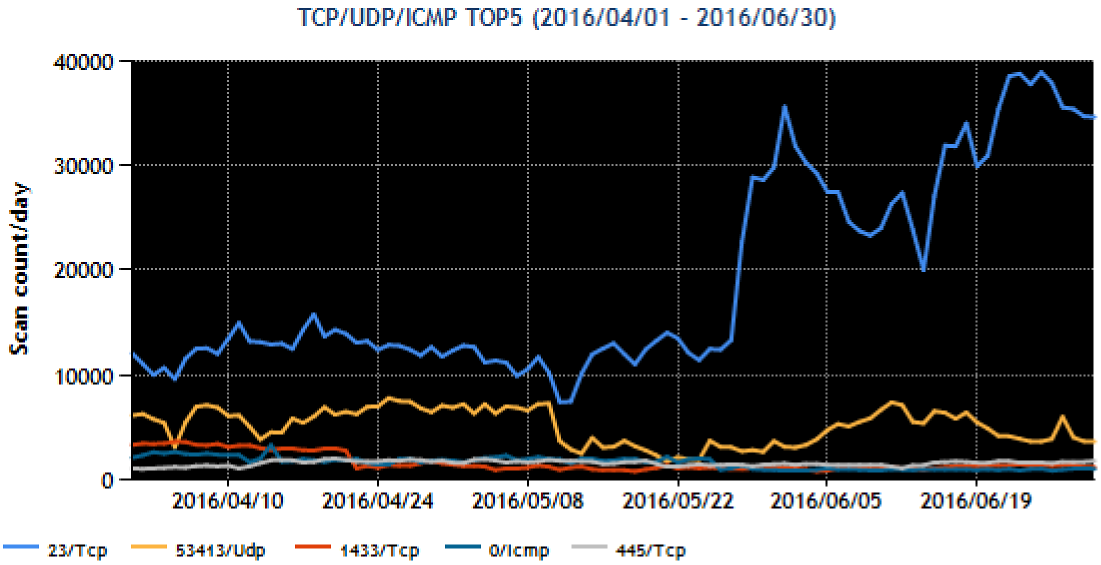
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	53413/UDP	2
3	1433/TCP (ms-sql-s)	5
4	0/ICMP	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.



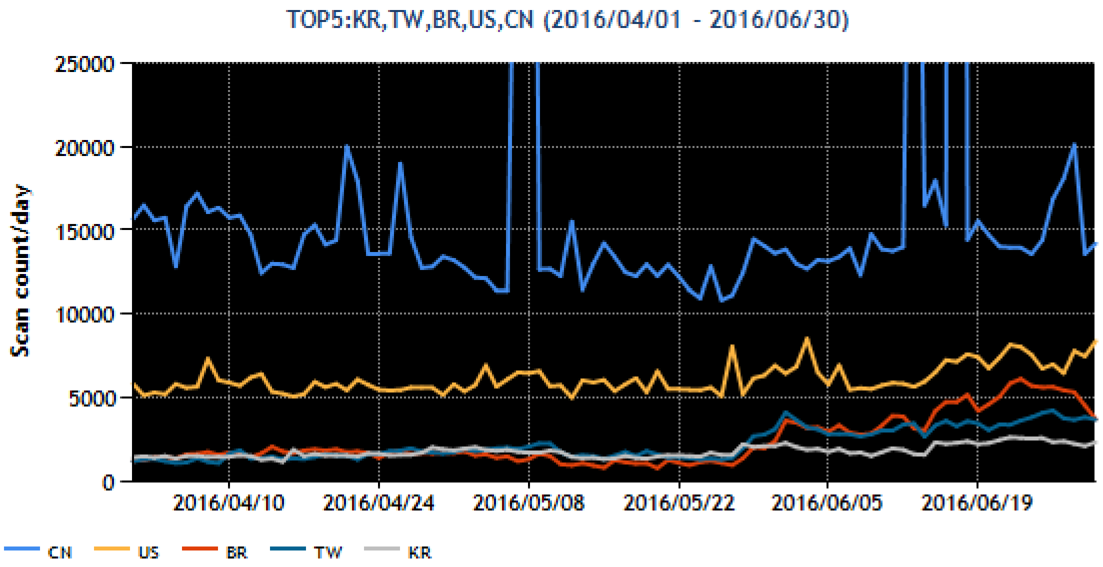
[Figure 1: Number of packets observed at top 5 destination ports from April through June 2016]

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	7
4	Taiwan	4
5	South Korea	3

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



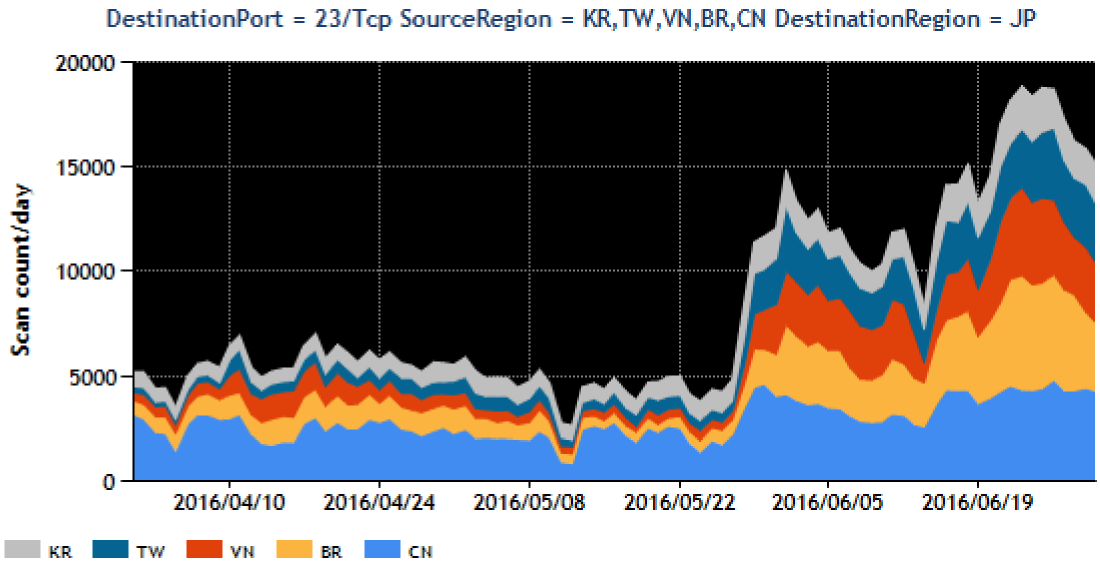
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2016]

This quarter, the number of packets targeted to 23/TCP increased sharply from around May 27. This phenomenon will be explained in detail in section 2.1 "Increase in the number of packets targeted to port 23/TCP." There is nothing in particular worth noting with regard to the top 5 destination port numbers. Next, with regard to the top 5 source regions, Brazil rose to third place in the number of packets from seventh in the previous quarter. This is because a large number of packets targeted to 23/TCP were observed originating in Brazil, which ranked second among the source regions for 23/TCP. 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 May 27, 2016, JPCERT/CC has been observing increased numbers of packets targeted to port 23/TCP. The source region is not limited to a certain region, and the packets are observed from multiple regions. (Figure 3)



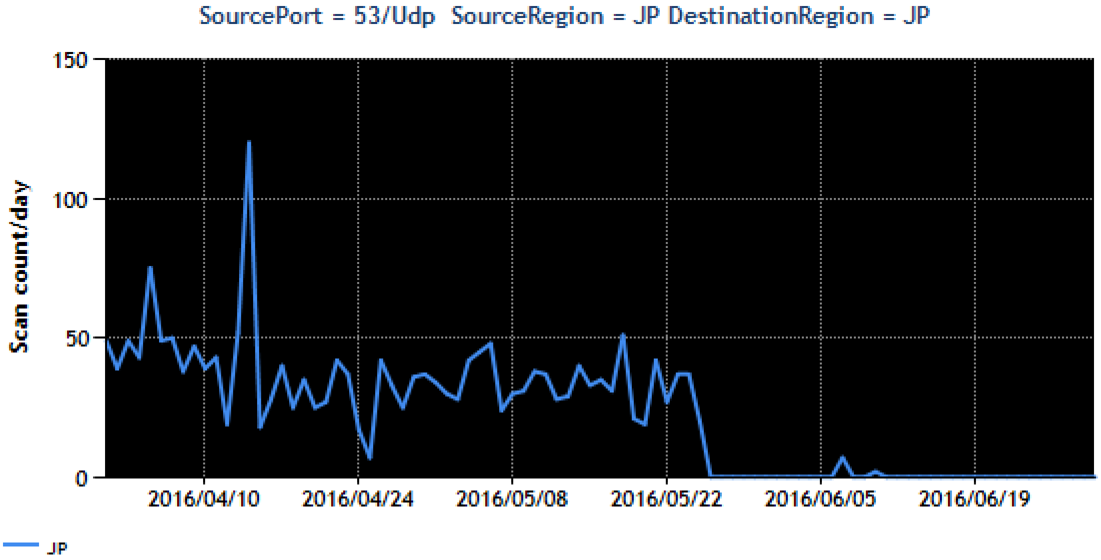
[Figure 3: Number of packets targeted to port 23/TCP]

As for the increase seen since May 27, JPCERT/CC confirmed the existence of CCTVs and other equipment that display a web interface for authentication by tracing the source IP addresses. The equipment (that appear to be CCTVs) sending suspicious packets include a number of products in Japan. Based on these and other investigation results, JPCERT/CC contacted product developers to resolve problems inherent in the products, and administrators of IP addresses where relevant equipment is operating to resolve problems found in products in operation.

In this way, JPCERT/CC is working to resolve problems by investigating equipment located at the source IP addresses of suspicious packets to infer the type of equipment, and by providing relevant information to equipment manufacturers, ISPs, and other related parties as necessary. Similar cases have been described several times in past issues of the JPCERT/CC Internet Threat Monitoring Report(*2).

2.2 Reduction in the number 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 a response to name resolution request packets sent by a third party to open resolvers using falsified IP addresses of TSUBAME's sensors, as part of a DNS Water Torture attack(*3). 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]

JPCERT/CC has not observed packets that appear to be DNS Water Torture attacks using open resolvers, etc., in Japan since May 25(*4). While this can be due to more effective countermeasures implemented by BIND and other DNS software, DNS operators, and so on, or because attackers have stopped using this method of attack, the truth is unknown.

Since DNS Water Torture attacks using open resolvers may resume anytime, JPCERT/CC will continue to monitor trends in the number of observed packets sent from port 53/UDP and respond if any abnormality is found.

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) Internet Threat Monitoring Report
https://www.jpcert.or.jp/tsubame/report/index.html

(3) Internet Infrastructure Review (IIR) Vol.31
http://www.iij.ad.jp/company/development/report/iir/031/01_03.html

(4) DNS Water Torture Attack: Countermeasures and Trends 2016 <Japanese only>
http://dnsops.jp/event/20160624/DNS_Summer_Days_2016_suematsu.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

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). For the latest information, please refer to JPCERT/CC's website.

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