JPCERT/CC®

JPCERT-IA-2016-02
Issued: 2016-05-26

JPCERT/CC Internet Threat Monitoring Report

[January 1, 2016 - March 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.

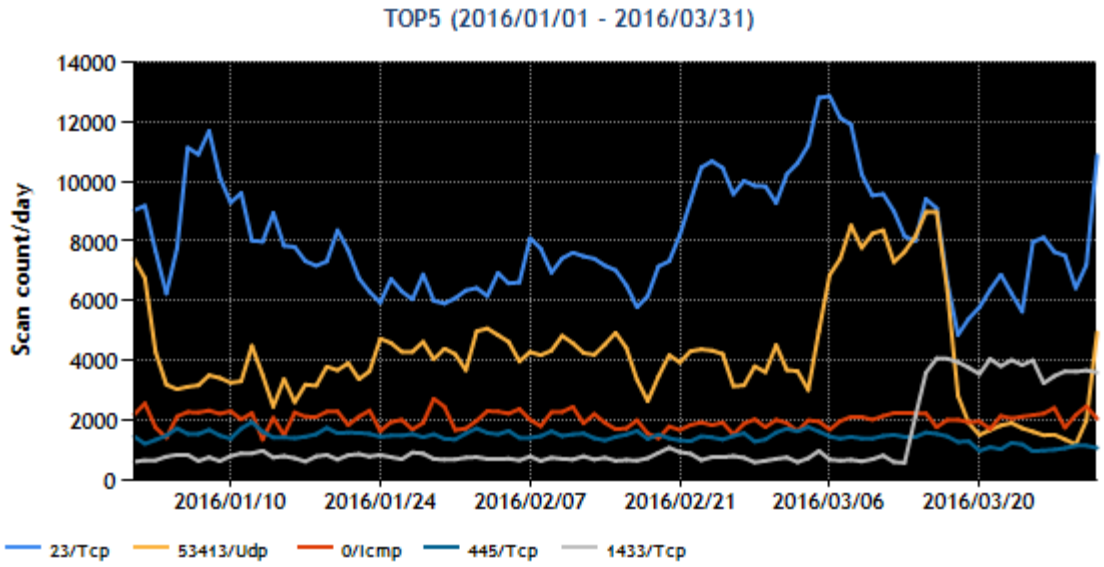
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	53413/UDP	3
3	0/ICMP	2
4	445/TCP (microsoft-ds)	4
5	1433/TCP (ms-sql-s)	5

*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.



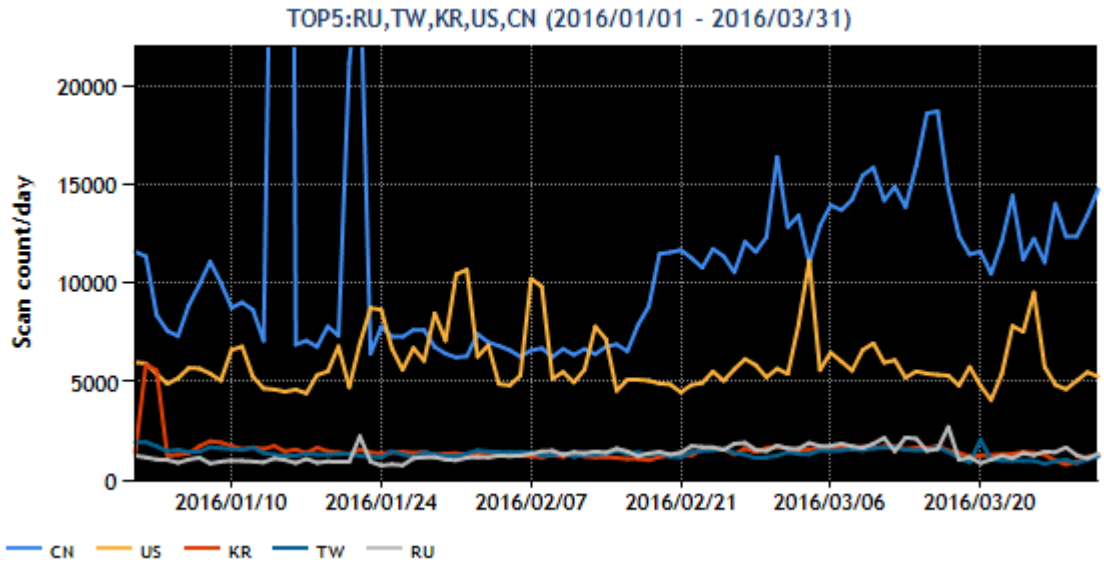
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2016]

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	South Korea	5
4	Taiwan	3
5	Russia	4

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



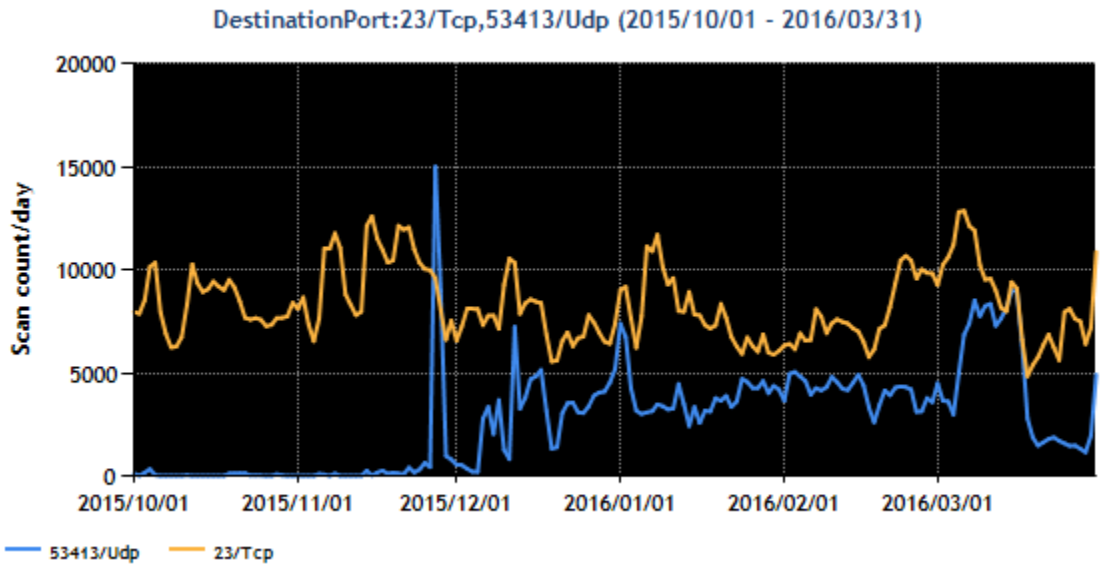
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2016]

Rankings of the top destination ports remained unchanged from the previous quarter. The number of packets targeted to ports used by routers and other equipment was high during this quarter. Many of these packets originated from equipment suspected of being infected with malware. Although it is not evident in Figures 1 and 2, the number of packets originating from within Japan has been increasing in 2016. This trend is described in detail in "2.1 Trends in the number of packets targeted to port 23/TCP." While some minor fluctuations were seen at other ports, there were no changes meriting attention.

2 Events of Note

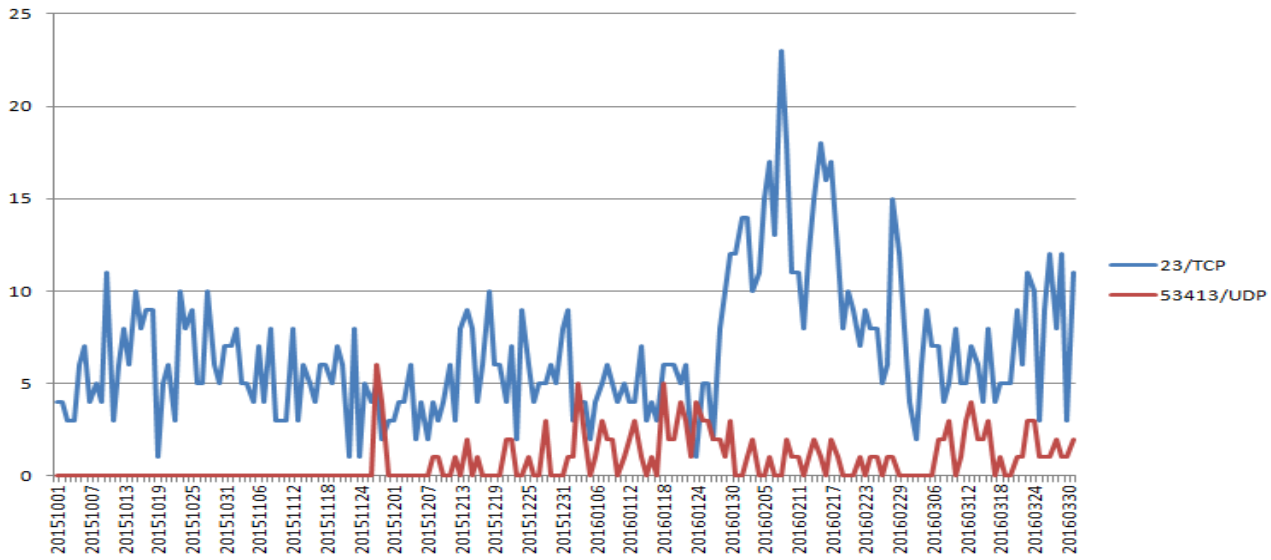
2.1 Trends in the number of packets targeted to port 23/TCP

Since around January 2011, JPCERT/CC has been observing packets targeted to port 23/TCP originating from various regions. Many of these packets are sent from routers, webcams and other products converted into bots by being infected with malware.
JPCERT/CC has recognized several types of malware which send packets to port 23/TCPt, and they all scan for an active port 23/TCP service (Telnet) before launching an attack on the equipment. Since late November 2015, some of the infected equipment has started sending packets to 53413/UDP as well. See Figure 3 for trends in the number of packets targeted to port 23/TCP and port 53413/UDP since October 2015.



[Figure 3: Number of packets targeted to port 23/TCP and port 53413/UDP]

JPCERT/CC has been working to eliminate problems by investigating equipment at the source IP address of suspicious packets to infer the model, and by providing information as necessary to the manufacturer of the equipment, ISP and other relevant parties. These activities have been covered a number of times in past issues of the JPCERT/CC Internet Threat Monitoring Report(*2).
Until mid-January 2016, many of these packets were sent from overseas, but in late January there was an increase in the number of packets with a source IP address located in Japan. See Figure 4 for trends in the number of source IP addresses in Japan.



[Figure 4: Number of IP addresses in Japan sending packets targeted to said ports]

Investigations conducted by JPCERT/CC have identified cases in which the following equipment manufactured by Japanese vendors was infected with malware.

- Controller equipment for renewable energy facilities
- Communication equipment for commercial use
- Equipment for collecting data such as temperature, humidity, atmospheric pressure, water volume, etc.

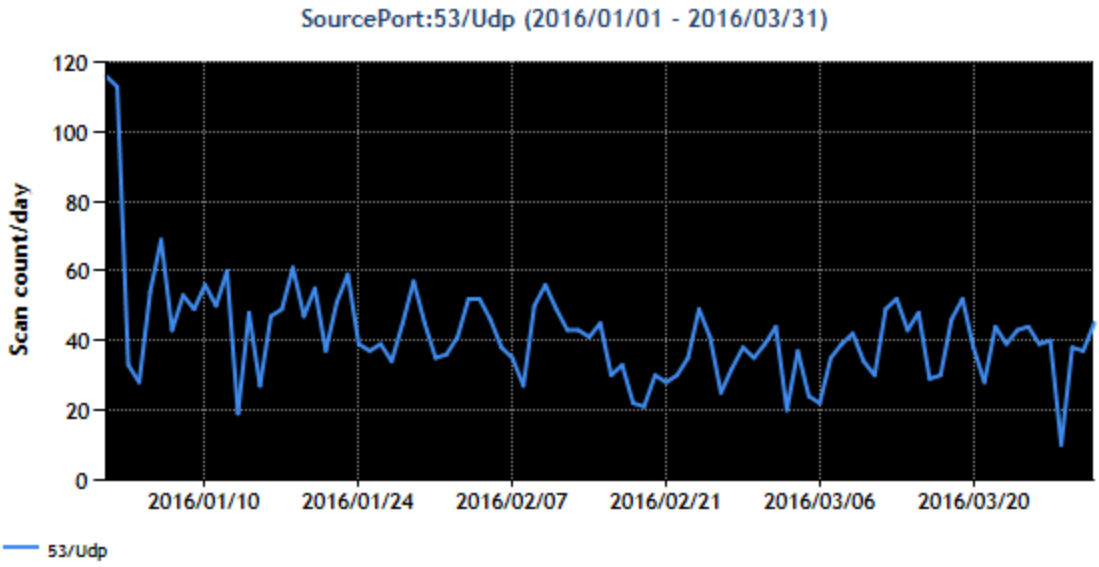
All or some of the following applied to these pieces of equipment.

1. Not a product that can be easily purchased at mass retailers, etc.
2. Usage in protected network environments such as internal networks is recommended
3. Listening for service requests on port 23/TCP
4. Connected to an ISP providing an inexpensive fixed IP address service

To help reduce the number of suspicious packets, JPCERT/CC contacted the product developers to fix problems inherent in the products, and the administrators of source IP addresses to fix problems caused by the products that are in operation.

2.2 Coordination on DNS reply packets sent from open resolvers 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. 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]

Since open resolvers are also used to carry out reflection attacks in addition to DNS Water Torture attacks, it is requested that these be eliminated. In late January, there was a report that a number of businesses came under a DDoS attack(*3). JPCERT/CC believes that multiple protocols were used in these attacks and that the attacks also included reflection attacks exploiting open resolvers in Japan.
JPCERT/CC provided relevant information to administrators of the 100 organizations that the packets were sent from and requested that appropriate steps be taken. Some of the administrators have already reported their investigation results. There were multiple cases in which an embedded Linux board with an Internet connection was an open resolver, and cases in which equipment was used without applying filter rules published by the equipment vendor as countermeasure information.

JPCERT/CC has been contacting the administrators of source IP addresses and working to address both the problems inherent in the products and problems caused by the products that are in operation.

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) Threat Advisory: #OpKillingBay Expands Targets
https://community.akamai.com/docs/DOC-5781

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 2015