JPCERT-IA-2016-01
Issued: 2016-02-04

JPCERT/CC Internet Threat Monitoring Report [October 1, 2015 - December 31, 2015]

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.

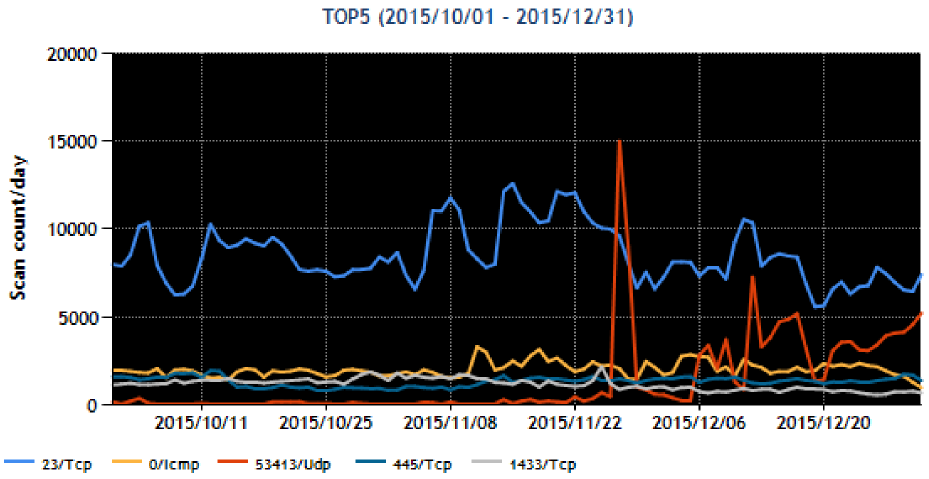
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	0/ICMP	2
3	53413/UDP	Not in top 10
4	445/TCP (microsoft-ds)	3
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.



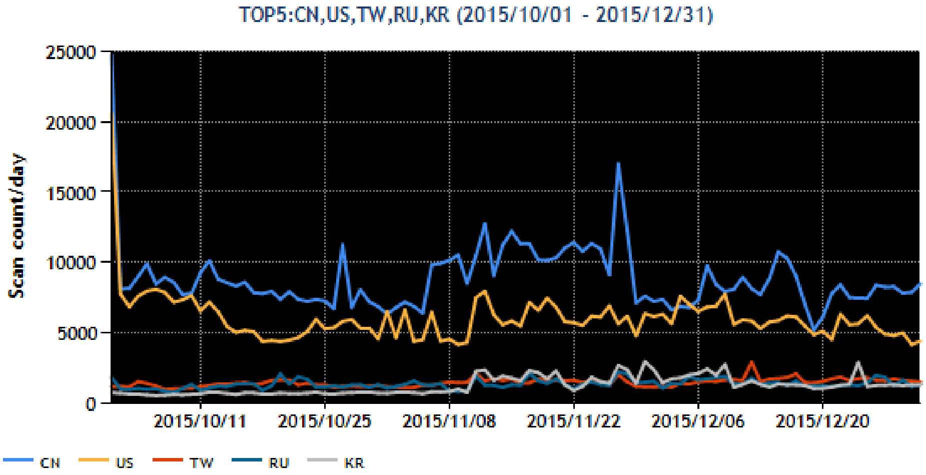
[Figure 1: Number of packets observed at top 5 destination ports from October through December 2015]

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	4
4	Russia	7
5	South Korea	8

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



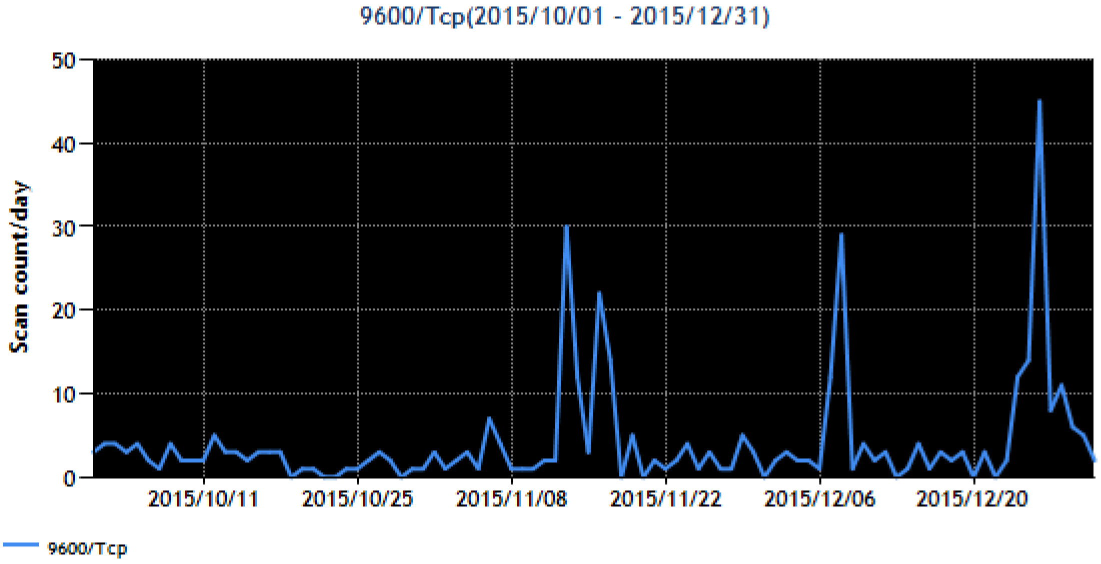
[Figure 2: Number of observed packets of the top 5 source regions from October through December 2015]

The number of packets targeted to 23/TCP was high during this quarter, as it was during the last quarter. Meanwhile, the number of packets targeted to 53413/UDP, mostly originating from China, showed a sudden increase on November 27 and 28, then continued to increase again from early December. These packets ranked second in the total number observed, rising from below top 10 in the previous quarter. Based on an analysis of observed packets, JPCERT/CC presumes that the packets were intended to scan for Netis/Netcore router products, which use 53413/UDP as a standard port. See "2.2 Router reconnaissance activities originating from IoT equipment" for information about related events. While some minor fluctuations were seen at other ports, there were no changes meriting attention.

2 Events of Note

2.1 Existence of packets and tools intended to scan for control equipment

The number of packets targeted to 9600/TCP temporarily increased a number of times since mid-November. The number of packets observed since October 2015 is shown in [Figure 3].



[Figure 3: Number of observed packets targeted to 9600/TCP]

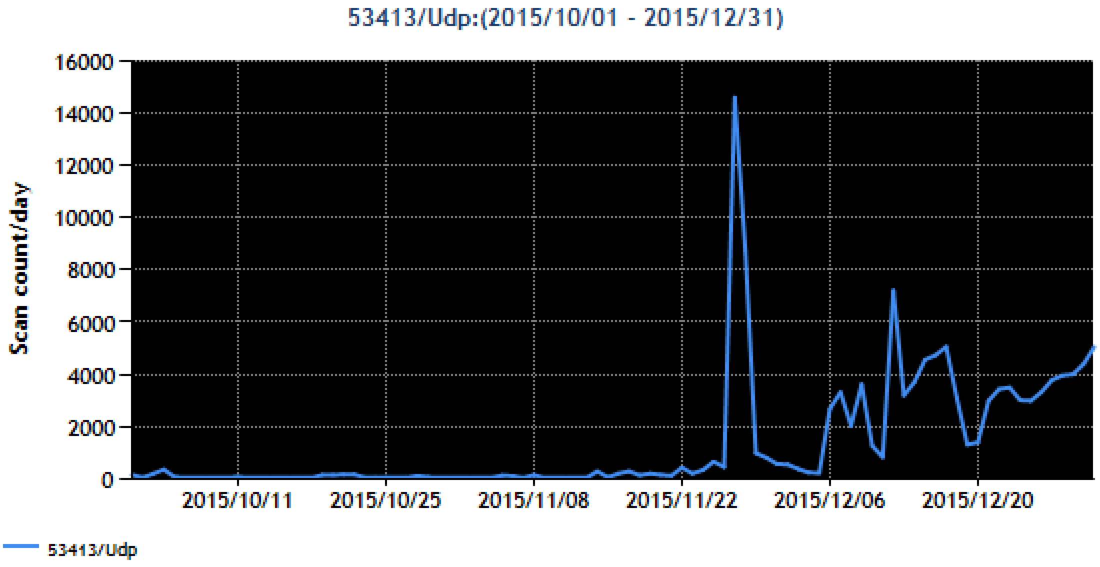
This port number is not used for any common software service. Therefore, JPCERT/CC started analyzing this event by investigating the types of server software and equipment that use this port number.

Further, when the first notable rise in the number of packets was seen on November 13 and 14, many of the packets were sent from a specific IP address. JPCERT/CC investigated which port numbers were scanned by this source IP address in the past, and found that it was those used by industrial control systems (ICSs). Then, upon investigating whether these port numbers were being used for communication by control equipment, JPCERT/CC learned that 9600/TCP was used for this purpose according to manuals of a Japanese control equipment vendor and elsewhere. Further information regarding the source IP address led to a website run by an institute that seemed to research on overseas ICS security. This website gave information including a security issue concerning a product of the above vendor and provided a proof-of-concept code, etc., apparently for demonstration purposes. These disclosures seem to have been posted around the time when the increase in the number of packets was observed.

From around December 20, the number of source IP addresses also increased along with the number of packets, which presumably include scans conducted by visitors to the website. These circumstances indicate that ICS equipment is also being studied as a subject of security research, and if vulnerabilities and tools are released, such equipment could be targeted by interested attackers.

2.2 Router reconnaissance activities originating from IoT equipment

As stated in Chapter 1, the number of packets targeted to 53413/UDP, mostly from China, showed a sudden increase on November 27 and 28, then continued to increase again from early December. The number of packets observed since October 2015 is shown in [Figure 4].



[Figure 4: Number of observed packets targeted to 53413/UDP]

This port number is rarely used by products commonly used in Japan. According to a blog article posted by Trend Micro on August 27, 2014, Netis/Netcore routers contain a vulnerability that can be exploited by sending crafted packets to this port number, which will enable the attacker to remotely execute any standard commands on the router. The product vendor updated the firmware to fix this problem by September 5, 2014. This matter was also discussed in the Internet Threat Monitoring Report (Apr-Jun 2015) (*2).

After more than a year since the release of the firmware update, there appear to be many Netis/Netcore routers connected to the Internet without updating the firmware to fix the vulnerability. (*3)

Since mid-November, JPCERT/CC has observed increased numbers of packets that appear to be scanning for such vulnerable routers. Some of these packets were originated from equipment other than PCs, such as webcams and set-top boxes infected with malware, including equipment with IP addresses that appear to be located in Japan.

These circumstances point to ongoing reconnaissance activities that use embedded equipment (other than PCs) infected with malware that turns it into a bot, which then scans for routers with vulnerabilities. In other words, vulnerable embedded equipment is used to look for other vulnerable embedded equipment.

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 (Apr-Jun 2015)
https://www.jpcert.or.jp/tsubame/report/report201504-06.html

(3) Vulnerable Netis Router Scanning Project
https://netisscan.shadowserver.org/

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

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