JPCERT CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IA-2015-03
Issued: 2015-07-29

JPCERT/CC Internet Threat Monitoring Report
[April 1, 2015 – June 30, 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.

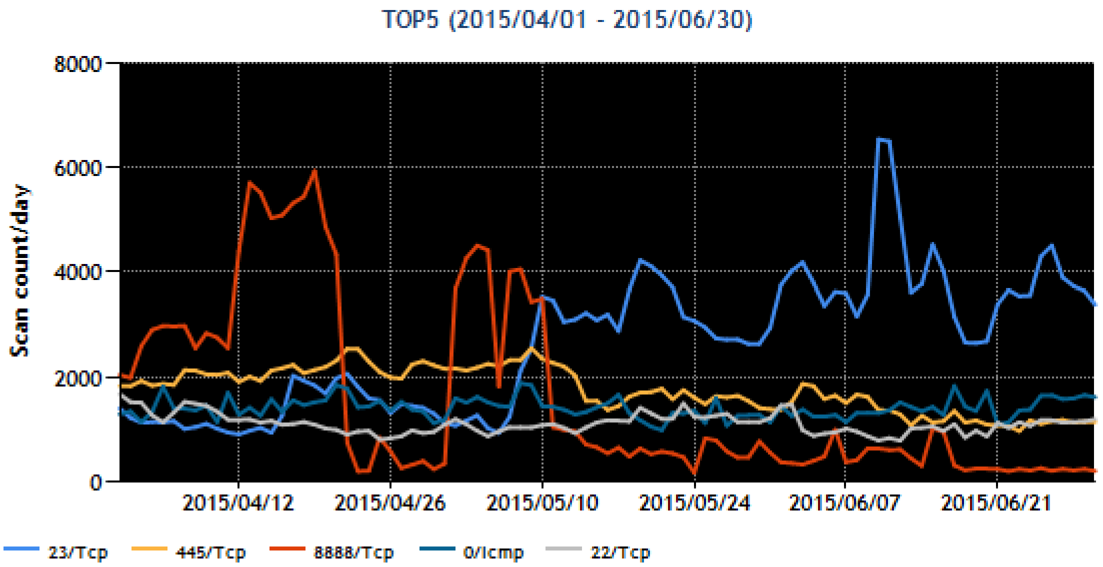
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	4
3	8888/TCP	13
4	0/ICMP	2
5	22/TCP (ssh)	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.



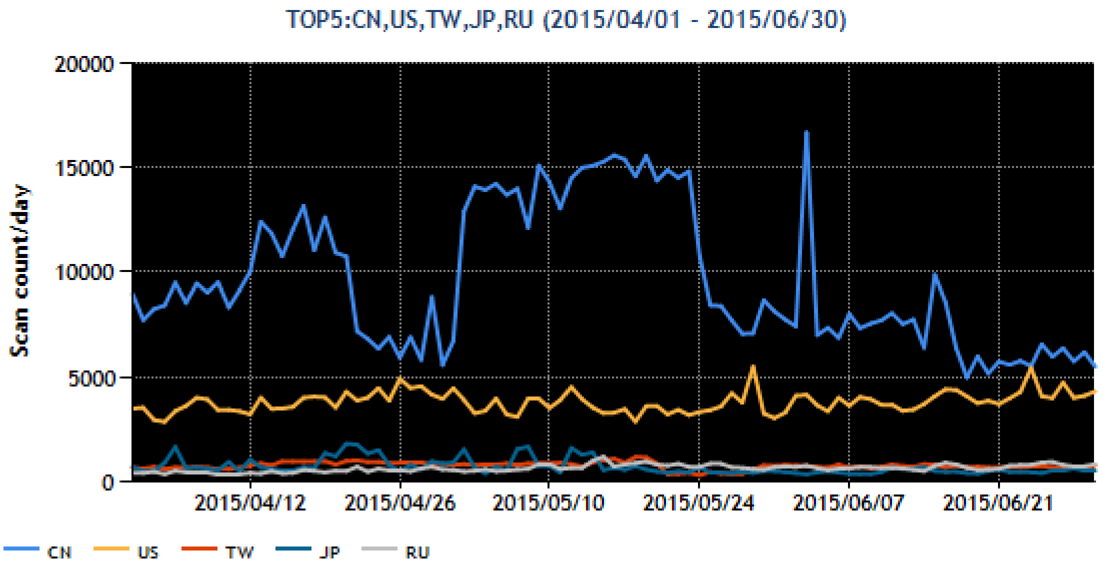
[Figure 1: Number of packets observed at top 5 destination ports from April through June 2015]

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	Japan	3
5	Russia	6

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



[Figure 2: Number of packets sent from the top 5 source regions, April through June 2015]

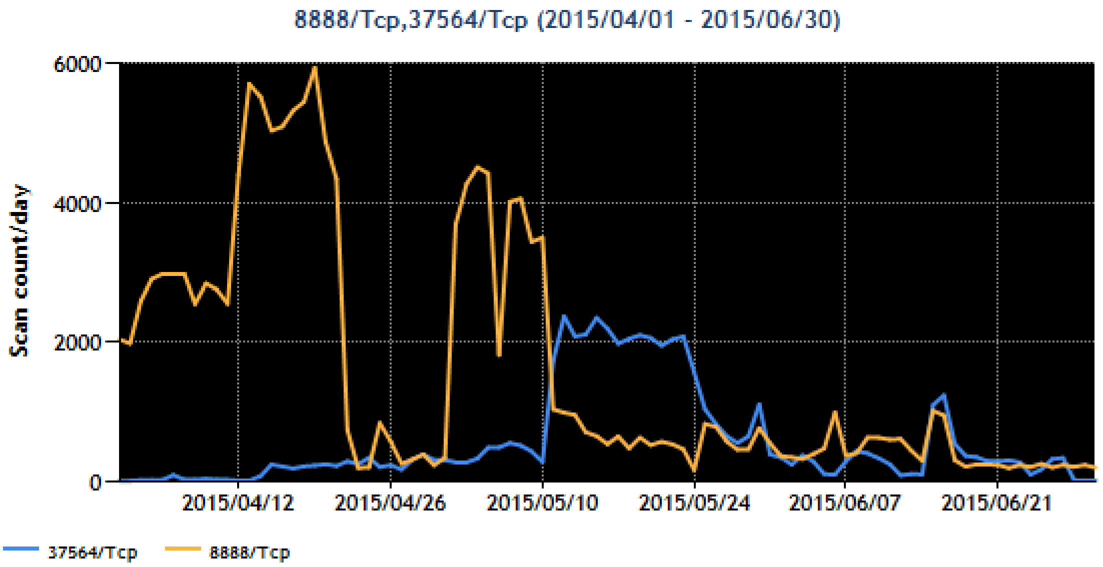
As for reconnaissance activities targeting network equipment with a built-in telnet server, which have been discussed in past Threat Monitoring Reports, the number of packets targeted to 23/TCP has increased again this quarter starting from around May 7. Packets targeted to 445/TCP, which was mentioned in the Internet Threat Monitoring Report (January-March 2015)(*2), increased between mid-March and mid-May, putting it in second place.

In addition, packets targeted to 8888/TCP have increased from around the middle of April. This appears to be related to the reconnaissance activities of open proxy servers and is examined in detail in 2.1.

2 Events of Note

2.1 Increase in packets presumed to be caused by the reconnaissance activities of open proxy servers

This quarter has seen an increase in the number of packets targeted to 8888/TCP, 37564/TCP and other port numbers from early April through mid-May (Figure 3). (*3) Packets targeted to 8888/TCP increased to the point where they were seen in greater numbers than packets targeted to 23/TCP (ranked 1st full-year) for about 6 weeks straight, rising from 13th to 3rd place.

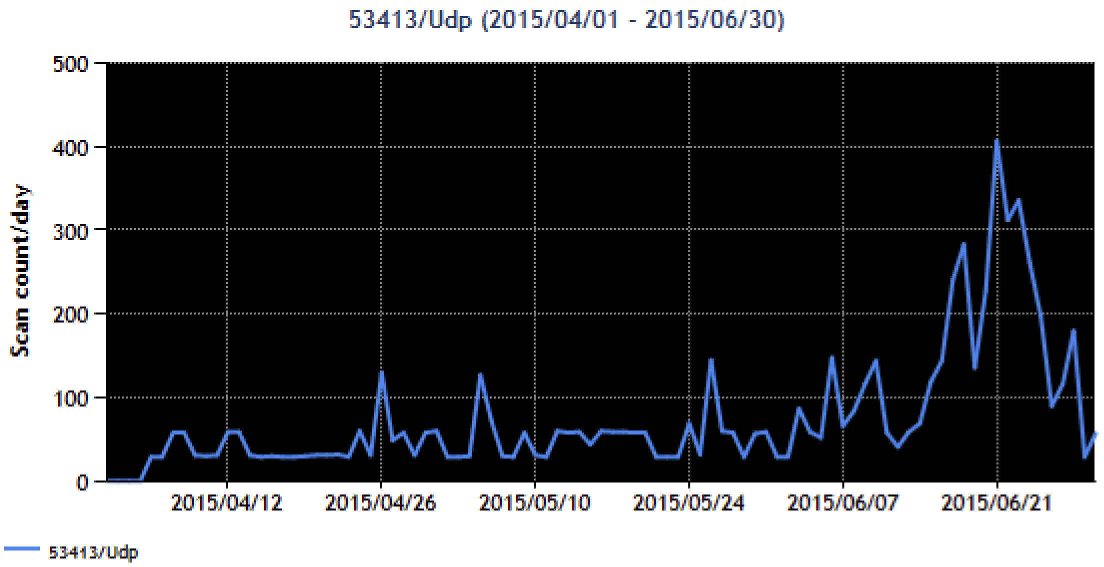


[Figure 3: Number of observed packets targeted to 8888/TCP and 37564/TCP from April through June 2015]

The first thing that comes to mind when considering the purpose of sending a large amount of packets to these port numbers is the existence of a number of overseas websites listing the IP addresses and port numbers of open proxy servers. In the past, TSUBAME has often observed surges in the number of packets targeted to port numbers that are not used for normal services. From the packets captured during this quarter, JPCERT/CC has searched for packets that have the same source IP address as packets targeted to 8888/TCP and 37564/TCP, and in some cases has found packets targeted to the port numbers of known open proxy servers. When the list of the corresponding open proxy server was examined, 8888/TCP and other port number information were newly added to the list, meaning it is highly likely that the packets were sent with the aim of searching for open proxy servers. There is no known major proxy server software that uses these port numbers as standard, which gives rise to the suspicion that a proxy server operating inside a certain package software product is exposed to the Internet due to inappropriate network access control. In any case, JPCERT/CC presumes that the number of these packets temporarily increased because the administrator of an open proxy server list became aware of these port numbers and added them as search ports.

2.2 Increase in packets targeted to 53413/UDP

The number of packets targeted to 53413/UDP increased for 2 weeks starting from around June 10, 2015 (Figure 4).



[Figure 4: Number of observed packets targeted to 53413/UDP from April through June 2015]

This port number is rarely used in products commonly used in Japan. According to a Trend Micro blog article posted on August 27, 2014, Netis/Netcore routers have a vulnerability that allows attackers to remotely execute any commands provided by the routers by sending a modified packet to this port number(＊4). The product vendor solved this problem by updating the firmware by September 5. Trend Micro has also confirmed that the port number can no longer be accessed(＊5).

An investigation by JPCERT/CC has revealed that the surge in packets seen in mid-June was caused by an attack exploiting this vulnerability to have bots infect the routers. The attack was carried out using the following method.

1. The attacker sends an authentication packet to the router's 53413/UDP to complete the authentication
2. A crafted 53413/UDP packet is sent into the router to use a command provided by the router to download a script file from an external server on the Internet. The script file is then executed after rewriting the execute permission, converting the router into a bot

Surges in attack packets corresponding to this method were observed a number of times after the vulnerability information and bug fix were released in September 2014. More devices may be converted into bots as the vulnerability remains unfixed, possibly making damages caused by DDoS attacks even more serious. (*6)

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) JPCERT/CC Internet Threat Monitoring Report (Jan-Mar 2015)
https://www.jpcert.or.jp/tsubame/report/report201501-03.html

(3) National Police Agency @Police
Internet Monitoring Results (May 2015) <Japanese only>
https://www.npa.go.jp/cyberpolice/detect/pdf/20150624.pdf

(4) Trend Micro Security Blog
Netis Routers Leave Wide Open Backdoor
http://blog.trendmicro.co.jp/archives/9725
http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/

(5) Trend Micro Security Blog
Netis Router Backdoor “Patched” But Not Really
http://blog.trendmicro.co.jp/archives/10050

(6) Shadow Server
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 Fiscal Year."

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