JPCERT-IA-2015-01
Issued: 2015/01/27

JPCERT/CC Internet Threat Monitoring Report
[October 1, 2014 - December 31, 2014]

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.

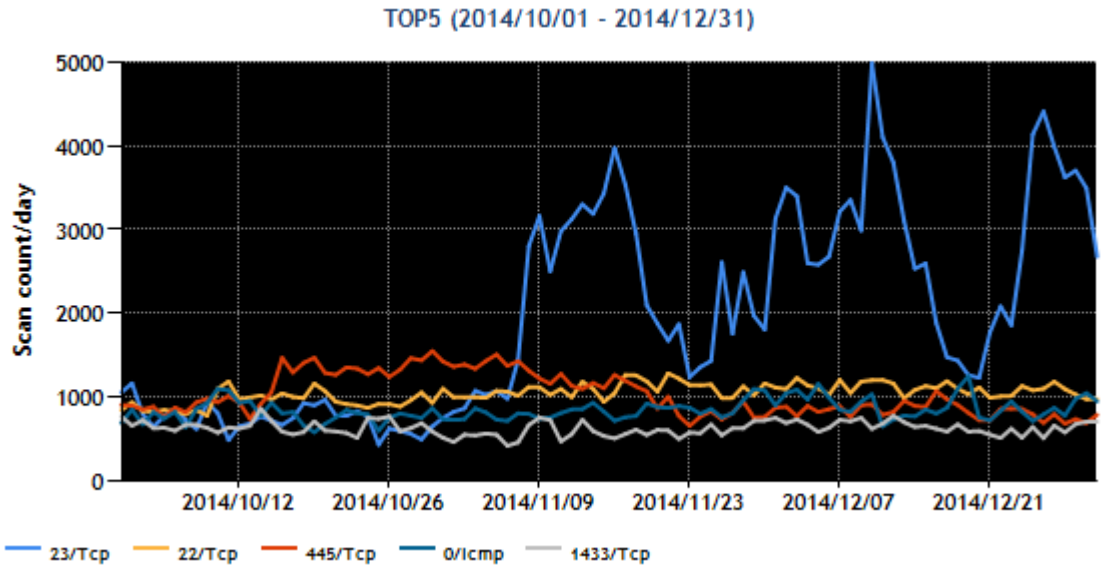
The top 5 destination port numbers for which packets were observed are listed in [Table 1].

[Table 1: Top 5 destination port numbers]

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



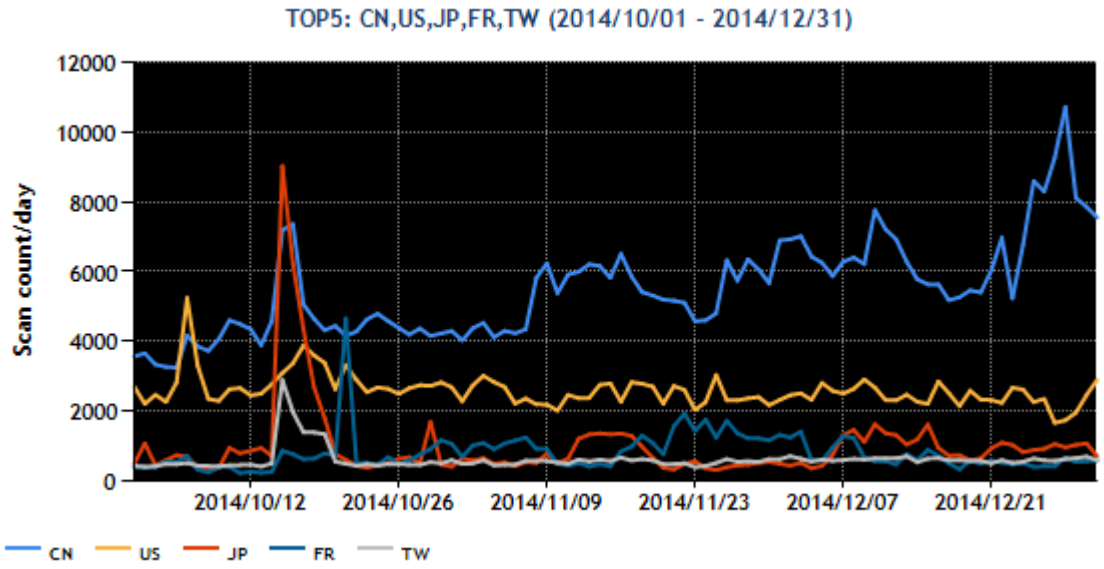
[Figure 1: Number of packets observed at top 5 destination ports from October through December 2014]

The top 5 source regions of packets observed are listed in [Table 2].

[Table 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	China	1
2	USA	2
3	Japan	5
4	France	9
5	Taiwan	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 October through December 2014]

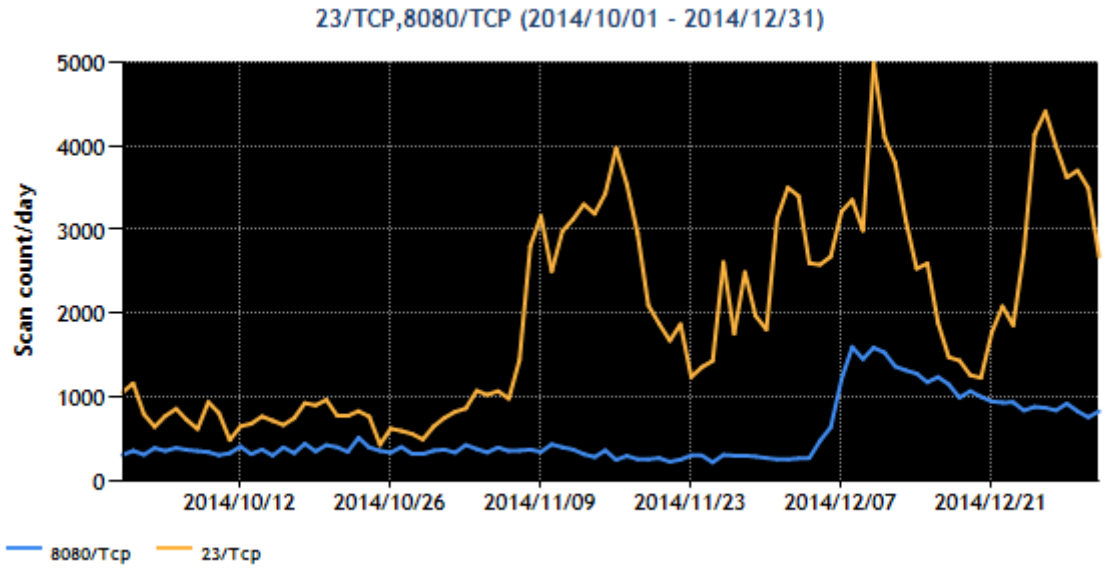
The number of packets targeted to 23/TCP rose sharply in early November and remained high for about a week before it fell again. Several prominent fluctuations were observed through December, amassing the largest number of observed packets during this quarter. This phenomenon will be explained in detail in section 2.1.

In mid-October, there was a rise in the number of packets originating from Japan. However, JPCERT/CC believes this data does not indicate any broad-based threat. It is presumed that a certain sensor was specified as the destination for P2P software communication, causing a large number of packets targeted to 12543/TCP and 12543/UDP to be captured temporarily. No other sensor showed any notable change. While some minor fluctuations were seen at other ports, there were no changes meriting attention.

2 Events of Note

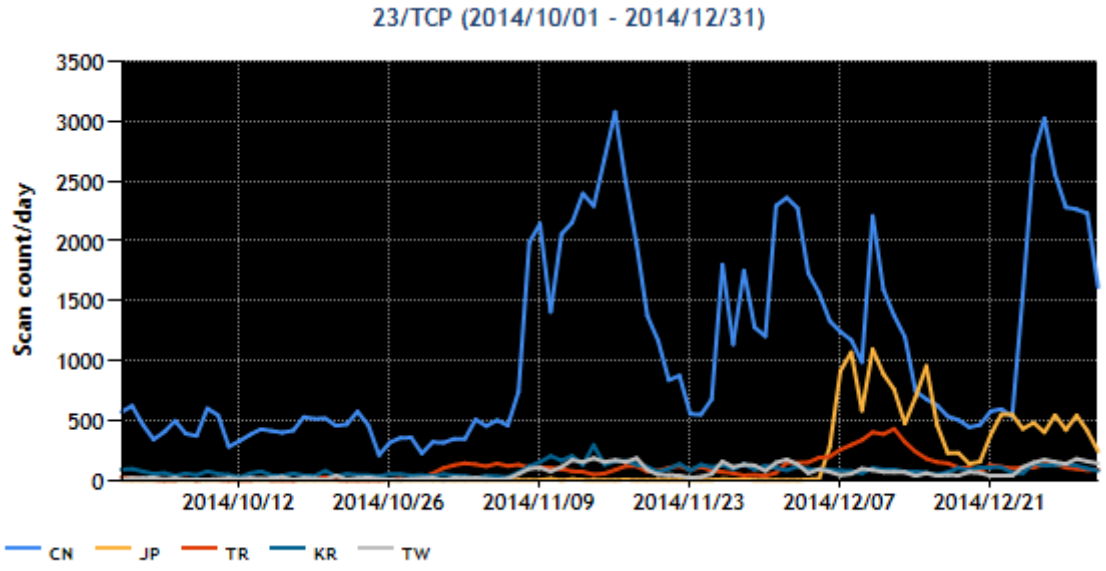
2.1 Increase in the number of packets targeted to 23/TCP and 8080/TCP

As shown in Figure 3, the number of packets targeted to 23/TCP has steadily increased since early November as it went through a series of fluctuations. Reconnaissance activities targeting network equipment with a built-in telnet server, which have been discussed in past Threat Monitoring Reports[*2,3,4,5], have once again become highly pronounced. Further, there was an increase in the number of packets targeted to 8080/TCP[*6,7,8] in early December.



[Figure 3: Number of observed packets targeted to 23/TCP and 8080/TCP from October through December 2014]

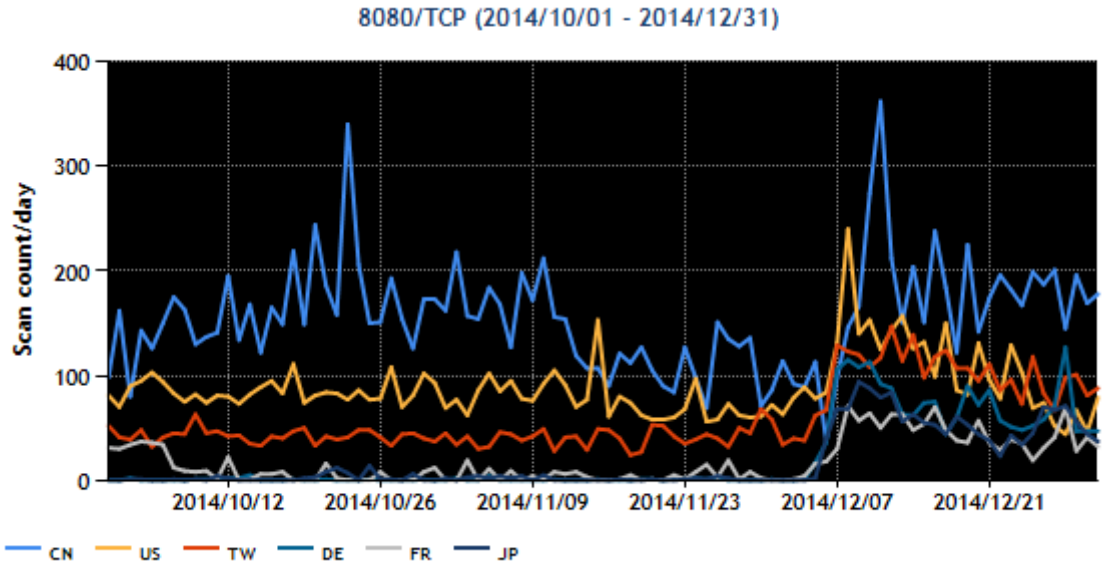
Figure 4 shows the observed number of packets targeted to 23/TCP during this quarter by major source region. While China stands out among the source regions in the number of packets observed, the number of packets originating from Japan rose sharply in early December.



[Figure 4: Number of observed packets targeted to 23/TCP from October through December 2014 (by source region)]

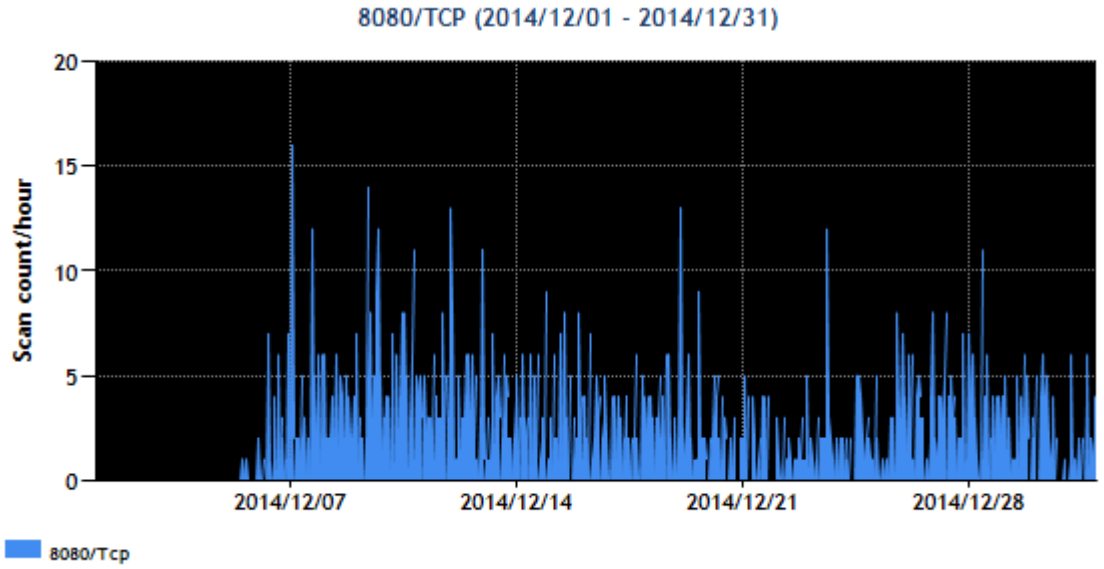
Figure 5 shows the observed number of packets targeted to 8080/TCP during this quarter by major

source region. China is the most prominent, with repeated fluctuations seen since early November. The number started rising for the United States (2nd), Taiwan (3rd), Germany (4th) and France (5th) in early December, as was the case with Japan (6th).



[Figure 5: Number of observed packets targeted to 8080/TCP from October through December 2014 (by source region)]

Figure 6 shows the observed number of packets originating from Japan and targeted to 8080/TCP.



[Figure 6: Number of observed packets targeted to 8080/TCP in December 2014 (originating from Japan)]

Investigation of the source node of some of these packets has revealed that while network cameras and specific broadband router products used overseas—which were discussed in the Jan-Mar 2014 issue of

this report(*2)—accounted for a majority of these packets until November, QNAP's NAS products (herein, QNAP NAS) have also come to be seen in large numbers since late November. Source IP addresses of packets targeted to 23/TCP and 8080/TCP have pointed to QNAP NAS installed in various regions in Japan, South Korea, Taiwan, the United States, Germany and France.
The 8080/TCP port is used as the standard port of the administration screen of QNAP NAS. Since QNAP NAS uses the GNU bash as its shell interpreter, devices using old firmware will be susceptible to the vulnerability announced in late September(*9). Arbitrary code can be executed on QNAP NAS by exploiting this vulnerability(*10,11,12). JPCERT/CC investigated packets targeted to 8080/TCP after late November and confirmed that they were requests presumably intended to exploit the vulnerability of QNAP NAS's GNU bash.

Packets targeted to 23/TCP and 8080/TCP that have been observed since late November were presumably sent by QNAP NAS hijacked through the vulnerability of GNU bash, and used as a springboard to search for QNAP NAS and other devices with the same vulnerability. JPCERT/CC has also confirmed that some of these QNAP NAS, though limited in number, have been sending packets targeted to 10000/TCP since late December. Since these packets target only QNAP NAS with the said vulnerability, products other than QNAP NAS will probably not be affected, even if they have the GNU bash vulnerability.

If myQNAPcloud service is activated to enable remote access to QNAP NAS (depending on the installation method, this service may be configured during the standard setup procedure and thus may be activated unintentionally), implement appropriate security measures (checking and updating the firmware version, assessing the impact of an attack, etc.) referencing "Alert regarding increase in scans to TCP port 8080"(*13), in order to avoid being used as a springboard for attacks.

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 2012)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html
(3) JPCERT/CC Internet Threat Monitoring Report (Apr-Jun 2012)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html
(4) JPCERT/CC Internet Threat Monitoring Report (Jan-Mar 2014)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html
(5) JPCERT/CC Internet Threat Monitoring Report (Jul-Sep 2014)
https://www.jpcert.or.jp/tsubame/report/report201407-09.html
(6) @police Access Targeting Vulnerability in Bash Observed (3rd Report) <Japanese only>
http://www.npa.go.jp/cyberpolice/topics/?seq=15063
(7) @police Internet Monitoring Results (Nov 2014) <Japanese only>
http://www.npa.go.jp/cyberpolice/detect/pdf/20141218.pdf
(8) @police Internet Monitoring Results (Dec 2014) <Japanese only>
http://www.npa.go.jp/cyberpolice/detect/pdf/20150113.pdf
(9) Vulnerability in GNU Bash
https://www.jpcert.or.jp/at/2014/at140037.html
(10) Protect Your Turbo NAS from Remote Attackers - Bash (Shellshock) Vulnerabilities
http://www.qnap.com/i/en/support/con_show.php?cid=61
(11) An Urgent Fix on the Reported Infection of a Variant of GNU Bash Environment Variable Command Injection Vulnerability
http://www.qnap.com/i/jp/support/con_show.php?cid=74
(12) The Shellshock Aftershock for NAS Administrators
https://www.fireeye.com/blog/threat-research/2014/10/the-shellshock-aftershock-for-nas-administrators.html
(13) Alert regarding increase in scans to TCP port 8080
https://www.jpcert.or.jp/at/2014/at140055.html

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 2014