JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IA-2014-03
Issued: 2014-10-28

JPCERT/CC Internet Threat Monitoring Report
[July 1, 2014 - September 30, 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.

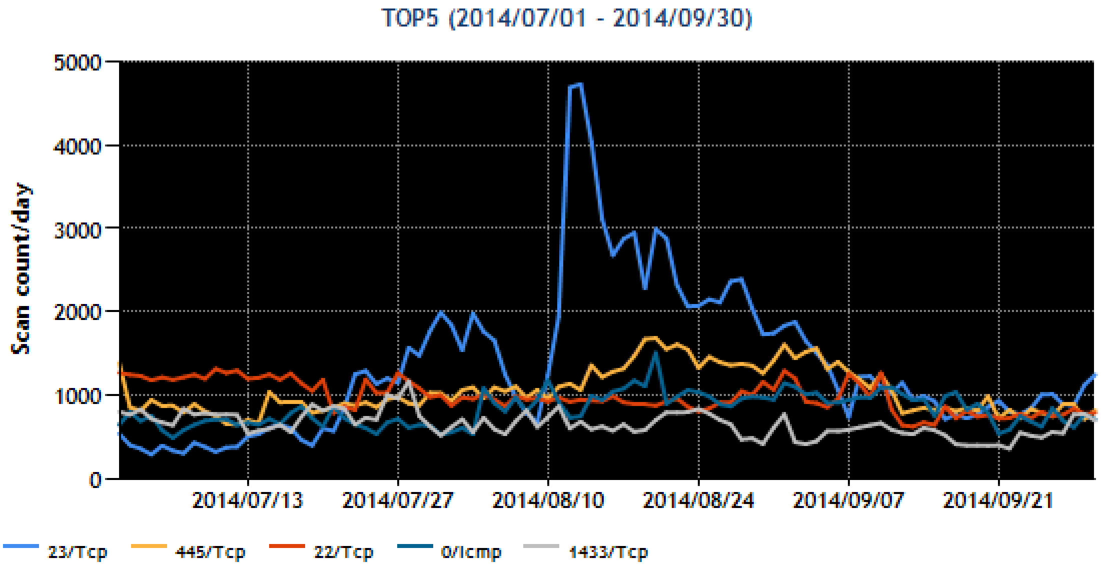
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Destination Port Numbers	This Quarter	Previous Quarter
23/TCP (telnet)	1	3
445/TCP (microsoft-ds)	2	1
22/TCP(ssh)	3	2
0/ICMP	4	4
1433/TCP (ms-sql-s)	5	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 each day by the top 5 destination ports over the 3 month period.



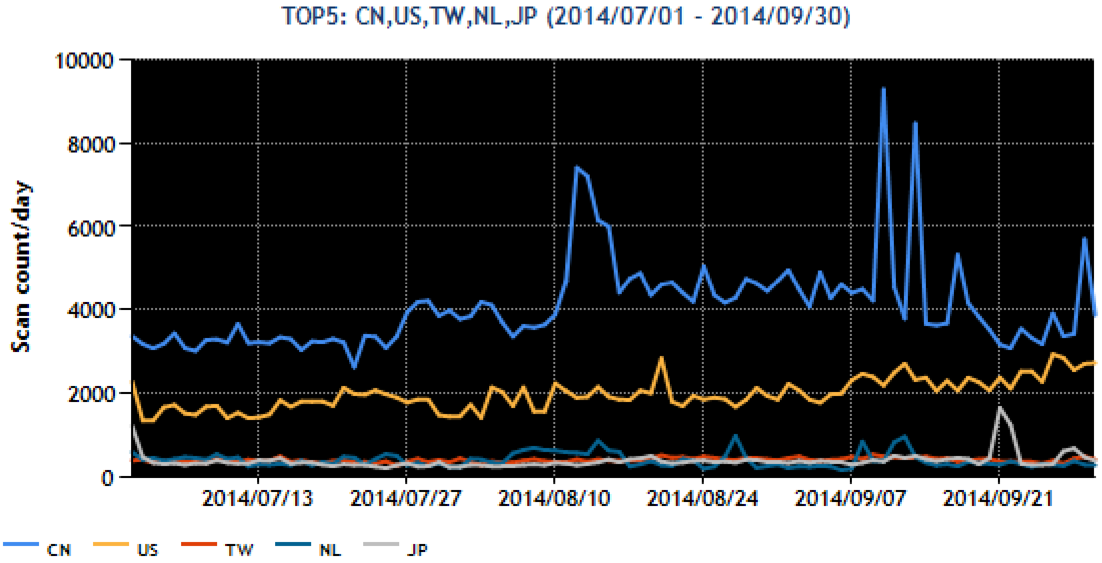
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2014]

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

[Chart 2: Top 5 source regions]

Source Regions	This Quarter	Previous Quarter
China	1	1
USA	2	2
Taiwan	3	4
Netherlands	4	3
Japan	5	5

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



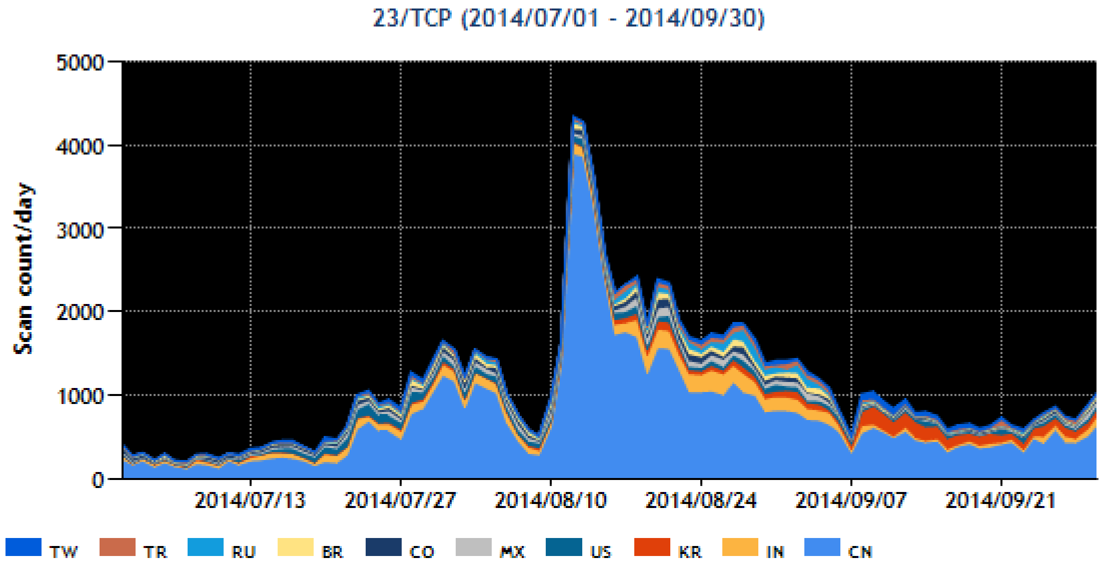
[Figure 2: Number of packets observed from the top 5 source regions from July through September 2014]

The number of packets targeted to 23/TCP increased in mid-August, rising to first place in the quarterly total. The phenomenon with regard to 23/TCP will be explained in detail in section 2.1. There were some increases and decreases at other ports, but there was nothing of note.

2 Events of Note

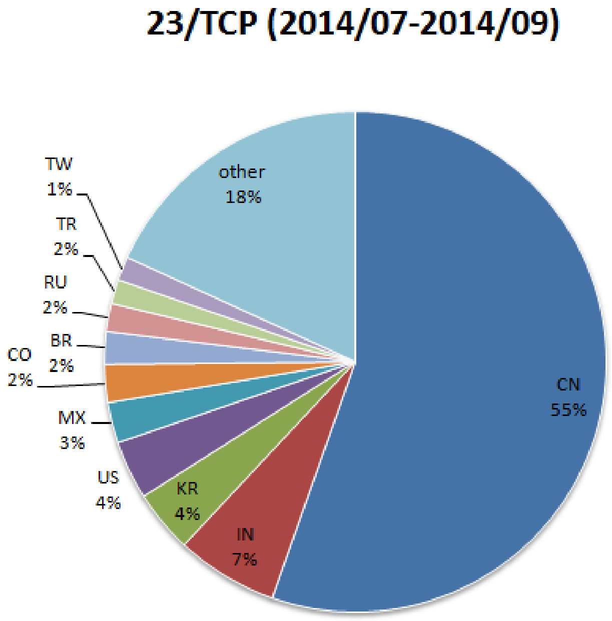
2.1 Increase in the number of packets targeted to 23/TCP

As shown in Figure 3, the number of packets targeted to 23/TCP has increased from mid-July through early September. Reconnaissance activities targeting network equipment (servers) listening for telnet connections, which have been discussed in past Threat Monitoring Reports(*2,3,4), have once again become highly pronounced.



[Figure 3: Number of observed packets targeted to 23/TCP from July through September 2014]

As shown in Figure 4, China was the top source region for packets sent to 23/TCP observed during this quarter, making up approximately 55% of the total number of packets targeted to 23/TCP. Figures 1 and 3 indicate that the growth in packets originating in China, which accounts for the majority, is directly reflected in this quarter's trend for 23/TCP. A slight increase was also observed for India, the runner-up, and South Korea, which follows in third place.



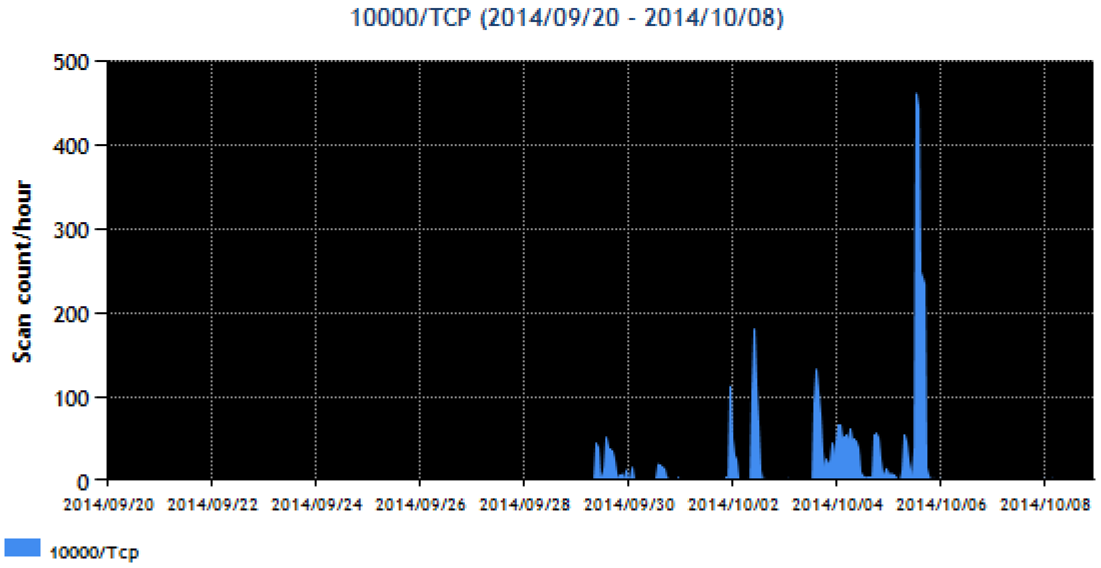
[Figure 4: Source regions of packets targeted to 23/TCP from July through September 2014]

Investigation of the source IP addresses of packets targeted to 23/TCP has revealed that a large number of network cameras, which were discussed in the Internet Threat Monitoring Report (Jan-Mar 2014) (*3), and specific broadband router products used overseas were in operation.

This quarter's increase is presumed to have been caused by a bot program installed in these network cameras and broadband routers, resulting in these devices frequently sending packets to a number of sensors.

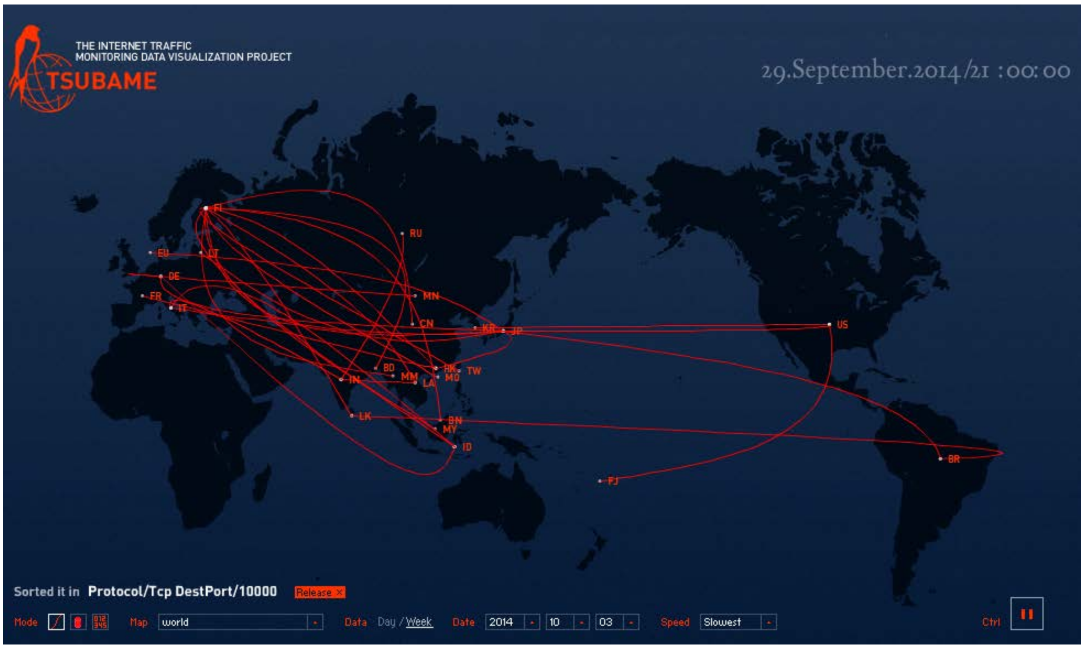
2.2 Increase in the number of packets targeted to 10000/TCP

As shown in Figure 5, the number of packets targeted to 10000/TCP has increased since late in September. (*5)



[Figure 5: Number of observed packets targeted to 10000/TCP from September 20 to October 9, 2014]

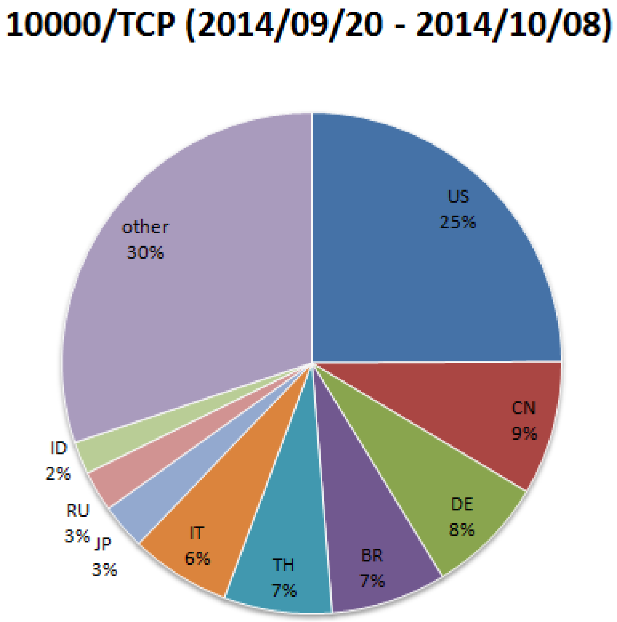
The United States was the source region accounting for the greatest number of packets targeted to 10000/TCP observed between September 20 and October 9, 2014. As shown in Figures 6 and 7, the other source regions were dispersed among various regions, including Japan.



Sorted it in Protocol/Tcp DestPort/10000

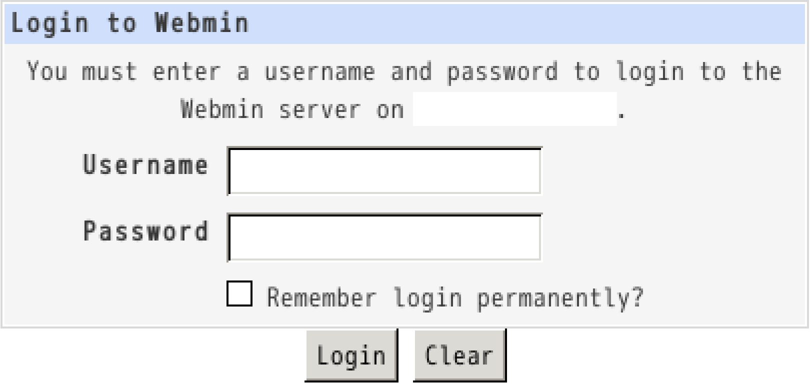
Mode Map world Data Day / Week Date 2014 10 03 Speed Slowest

[Figure 6: Visualization of packet transmission targeted to 10000/TCP on September 29, 2014]



[Figure 7: Source regions of packets targeted to 10000/TCP from September 20 to October 9, 2014]

The 10000/TCP port is used as the standard port of Webmin, which is a web-based system administration tool. Investigation of the IP addresses that transmitted packets targeted to 10000/TCP to sensors (Figure 8 shows an example of the investigation results) has confirmed that a large number of Webmins are in operation (according to the investigation, Japan accounted for a greater proportion of these Webmins than any other regions).



Login to Webmin

You must enter a username and password to login to the Webmin server on .

[Figure 8: An example of Webmin operating with the source IP address]

In late September, it was announced(*6) that a serious vulnerability was discovered in GNU bash, which is often used as a standard shell in Webmins. When this vulnerability is exploited, arbitrary code can be executed under the privilege of the user running the Webmin (JPCERT/CC has conducted verification using Webmin 1.700 (RPM) and a version of GNU bash impacted by CVE-2014-6271, and actually confirmed that arbitrary code can be executed). With a standard installation, Webmin runs under administrator (root) privilege, which means anyone exploiting this vulnerability would be able to execute arbitrary code under administrator privilege.

Packets targeted to 10000/TCP that were observed during this quarter are presumably for searching Webmins that could be used to exploit the vulnerability in GNU bash.

It is recommended to conduct an investigation to determine whether Webmin is installed on servers accessible via the Internet. If it is installed, implement appropriate security measures (applying patches and/or updates, implementing access control, reviewing security settings, etc.) referencing "Alert regarding increase in scans to TCP port 10000"(*7), in order to avoid being used as a springboard for attacks.

Further, system administration tools such as cPanel and Parallels Plesk Panel are also said to be impacted by the vulnerability in GNU bash(*8,9), so a countermeasure based on Webmin needs to be considered. While a certain amount of packets targeted to the standard ports used by cPanel and Parallels Plesk Panel (2082/TCP、2083/TCP、8443/TCP) has been observed from before, no fluctuations were seen either before or after late September.

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) @police Access Targeting Vulnerability in Bash Observed (2nd Report) <Japanese only>
https://www.npa.go.jp/cyberpolice/topics/?seq=14737

(6) Vulnerability in GNU Bash
https://www.jpcert.or.jp/at/2014/at140037.html

(7) Alert regarding increase in scans to TCP port 10000
https://www.jpcert.or.jp/at/2014/at140038.html

(8) cPanel Security Team: Bash CVE-2014-6217 and CVE-2014-7169
http://cpanel.net/cpanel-security-team-bash-cve-2014-6217-and-cve-2014-7169/

(9) [Hub] Shellshock vulnerability
http://kb.sp.parallels.com/jp/123006

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

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (office@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