Japan Computer Emergency Response Team Coordination Center

JPCERT-IA-2015-04
Issued: 2015-10-29

JPCERT/CC Internet Threat Monitoring Report [July 1, 2015 - September 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.

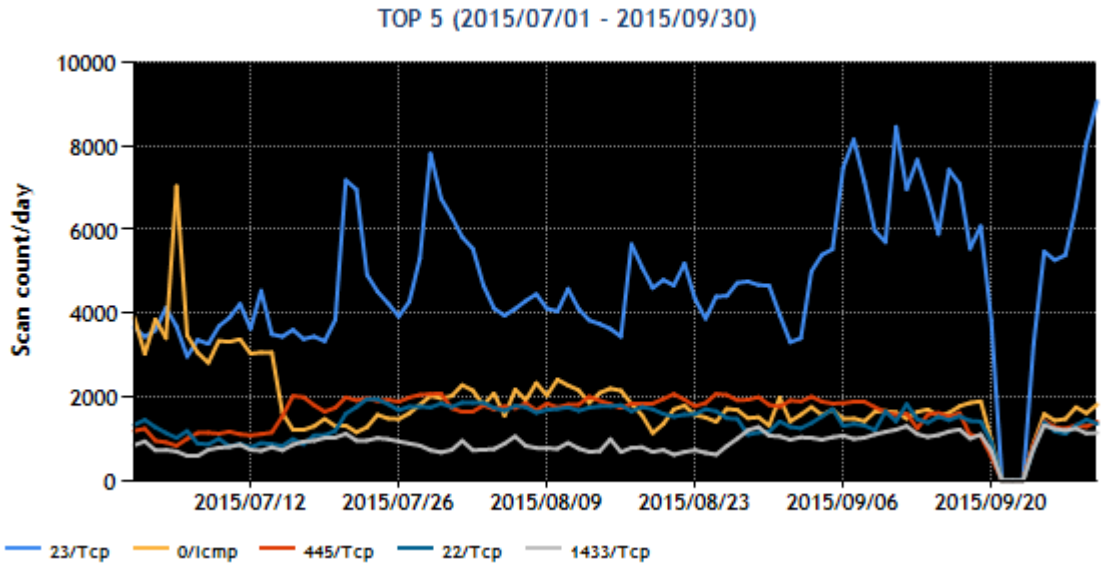
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	0/ICMP	4
3	445/TCP (microsoft-ds)	2
4	22/TCP (ssh)	5
5	1433/TCP (ms-sql-s)	6

*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. Observation data is missing for the period from 2:50 p.m. on September 20 to 9:20 a.m. on September 24, 2015 (GMT +9) due to equipment failure that occurred at the facility housing the Internet threat monitoring system, forcing system operation to be suspended.



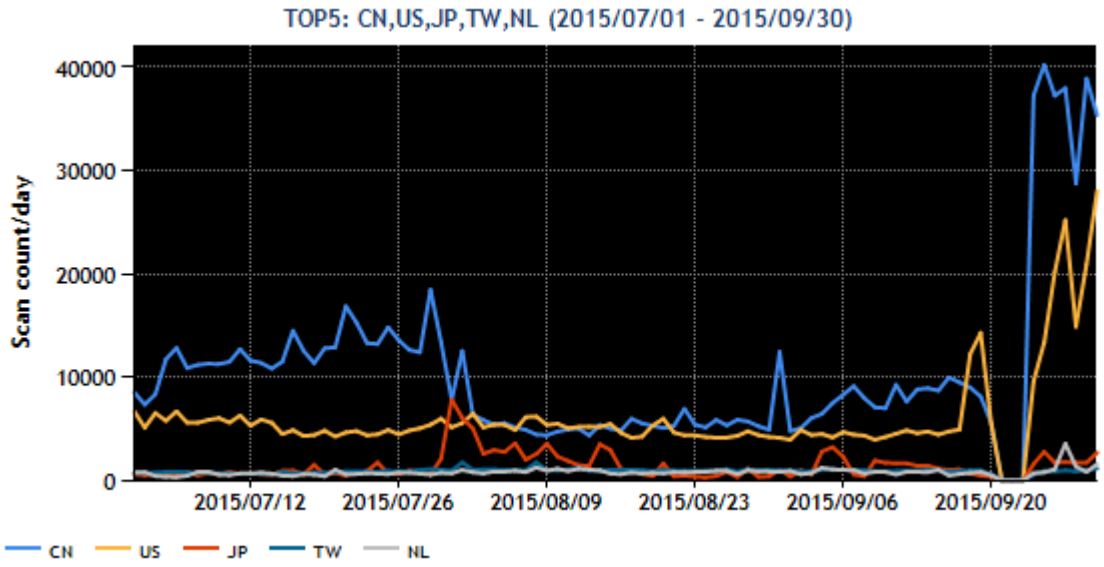
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2015]

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	Japan	4
4	Taiwan	3
5	Netherlands	6

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



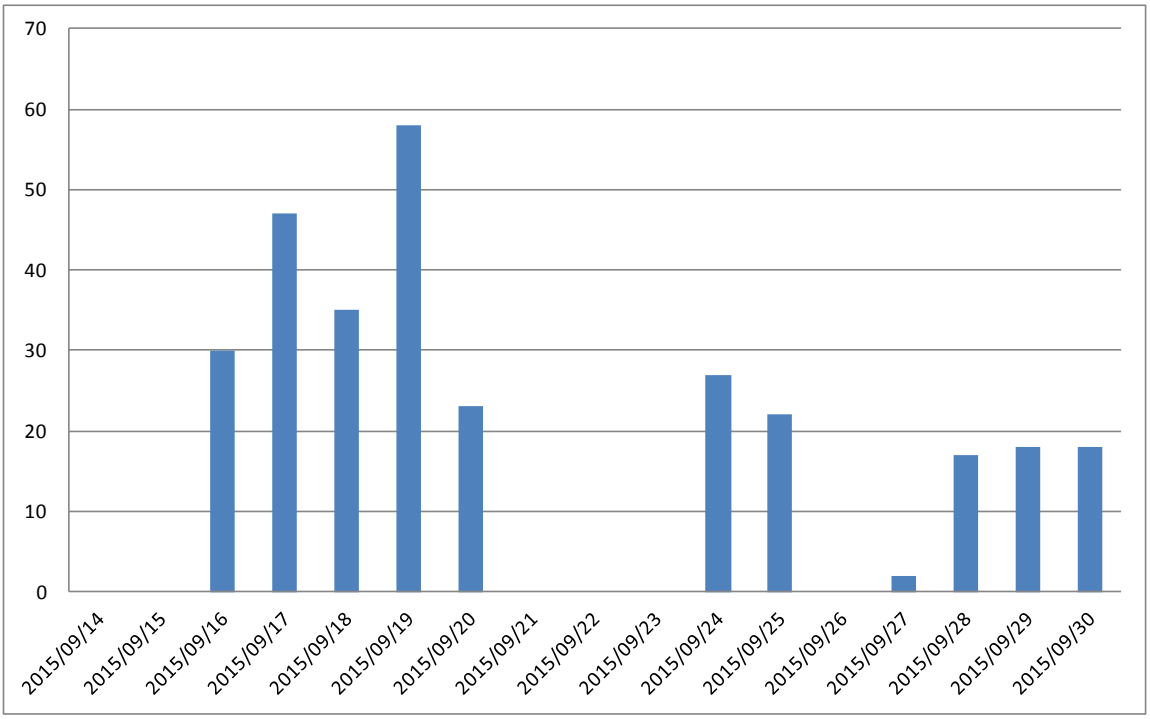
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2015]

Reconnaissance activities targeting network equipment with a built-in telnet server, which have been discussed in past Threat Monitoring Reports, have again resulted in the observation of a large number of packets targeted to 23/TCP during this quarter. From September 24 to early October, there was a rise mostly in the number of packets originating from China and the United States. However, this rise was due to a specific sensor having temporarily received a large number of SSDP M-SEARCH packets targeted to 1900/UDP. Since no other sensors showed any notable change, JPCERT/CC believes this data does not indicate any broad-based threat. While some minor fluctuations were seen at other ports, there were no changes meriting attention.

2 Events of Note

2.1 Packets sent to scan for Cisco routers implanted with SYNful Knock

From around mid-September, JPCERT/CC has continually been observing packets targeted to 80/TCP, which presumably were sent to scan for Cisco routers implanted with the SYNful Knock malware. The number of packets observed since mid-September 2015 is shown in [Figure 3].



[Figure 3: Number of observed packets presumably sent to scan for Cisco routers implanted with SYNful Knock]

On August 11, Cisco issued a security alert (*2) warning against attacks targeting Cisco IOS software platforms. According to this information, there have been confirmed cases of attacks in which attackers have gained access to Cisco routers in some way and implanted malware (a modified ROMmon image). Then on September 15, security vendor FireEye published(*3) the results of investigation on this malware (i.e., behavior and the method of determining infection), which it named SYNful Knock. In light of FireEye's article, Cisco published another article(*4) urging caution.

FireEye disclosed a method to detect the implanted SYNful Knock by sending a crafted packet which is used by the malware itself and analyzing the response. The packets observed by the Internet threat monitoring system since mid-September (Figure 3) are the same as the packets that appear in the scanning method disclosed by FireEye. Accordingly, JPCERT/CC presumes that these packets were sent to scan for Cisco routers implanted with SYNful Knock.

According to a team of computer scientists from the University of Michigan and the University of

California, Berkeley and others that investigated the status of SYNful Knock implant(*5), implants were discovered on Cisco routers in India, Mexico, the Philippines, and Ukraine as of mid-September, but none were found in Japan.

These events serve as a reminder that nodes that can be accessed from the Internet can become a target of attack. If a router is compromised, various risks can result, including intrusion into an internal network, malware infection, and stolen information. Readers are advised to implement adequate security measures (do not use a default password, update the firmware to incorporate vulnerability fixes, review security settings, etc.) to avoid being used as a springboard for attack.

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) Evolution in Attacks Against Cisco IOS Software Platforms
http://tools.cisco.com/security/center/viewAlert.x?alertId=40411
(3) SYNful Knock - A Cisco router implant - Part I
https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html
(4) SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks
http://blogs.cisco.com/security/synful-knock
(5) In Search of SYNful Routers
https://zmap.io/synful/

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