JPCERT/CC®

JPCERT-IA-2015-02
Issued: 2015-04-27

JPCERT/CC Internet Threat Monitoring Report
[January 1, 2015 - March 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.

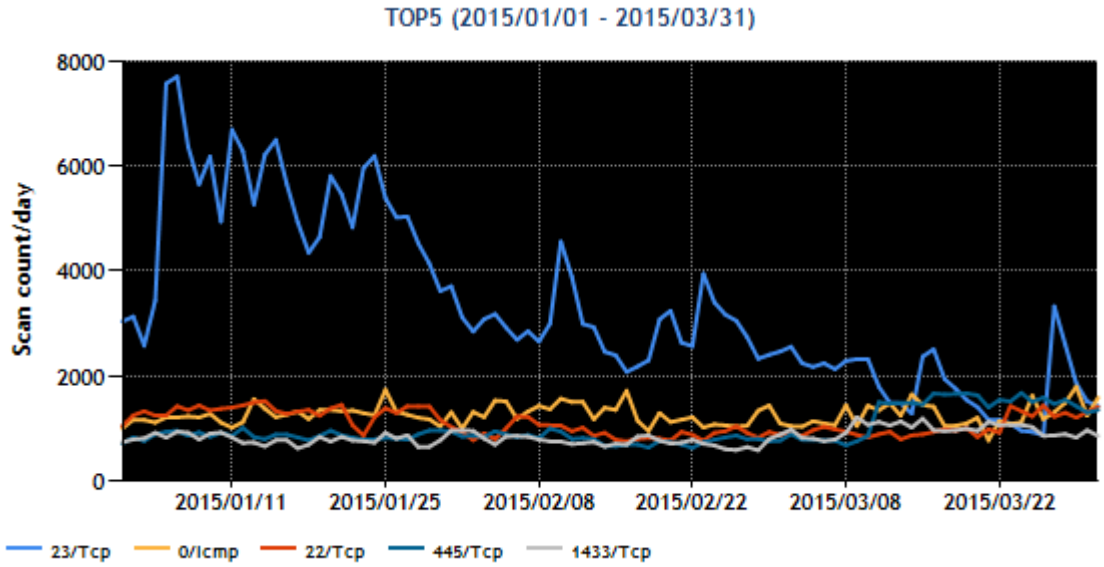
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

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



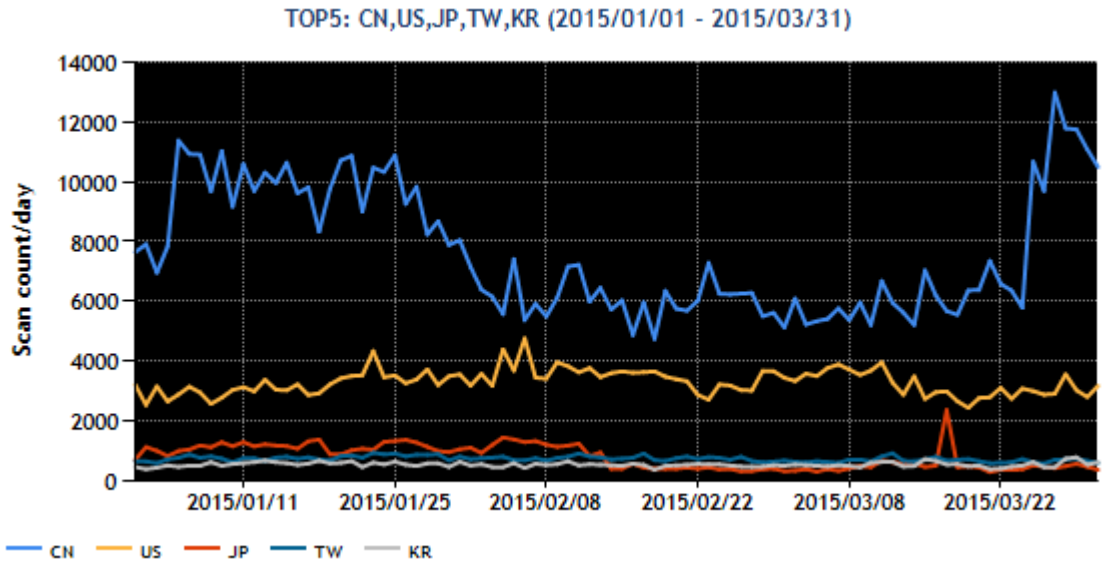
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2015]

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	3
4	Taiwan	5
5	South Korea	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 January through March 2015]

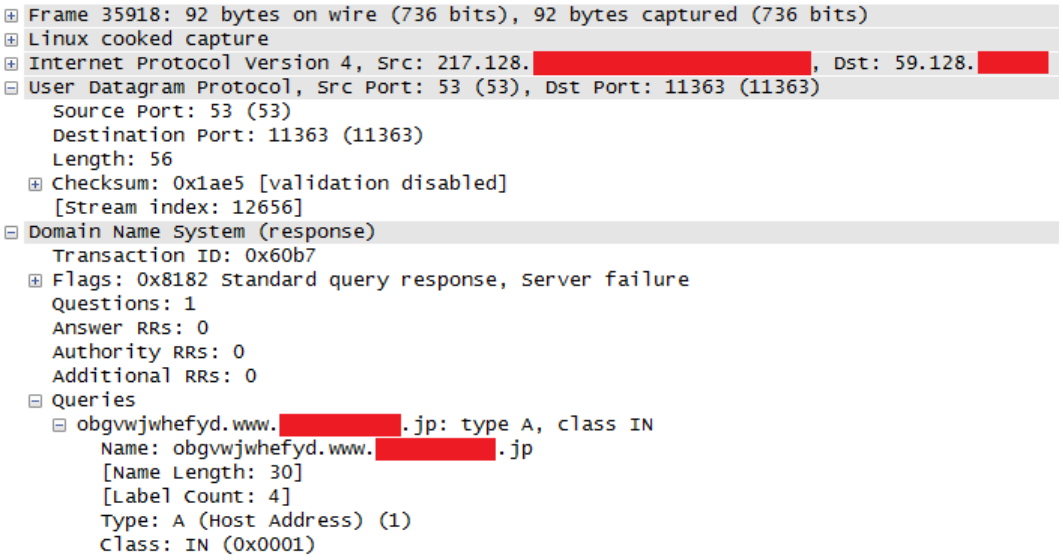
During this quarter, the number of packets targeted to 23/TCP has fallen since January. The phenomenon with regard to 23/TCP will be explained in detail in section 2.2. Further, the number of packets targeted to 445/TCP has been increasing since mid-March. While the cause of the increase is unclear, users of Windows operating systems and Windows Server products are advised to take appropriate security measures (applying security updates, avoiding the use of simple passwords for log-on authentication, etc.) as recent activities of the new Conficker variant raise concerns. While some minor fluctuations were seen at other ports, there were no changes meriting attention.

2 Events of Note

2.1 Observation of DDoS attacks using open resolvers including devices in Japan

In a past Threat Monitoring Report [(*2)], JPCERT/CC described a case of DDoS attack targeting overseas domains, which employed a method of attack using open resolvers to send queries for a large number of nonexistent FQDNs, in an attempt to flood the targeted authoritative DNS servers (herein, "DNS Water Torture"). In early February, JPCERT/CC observed large numbers of UDP packets with a source port of 53 (herein, "DNS answer packets") targeting domestic domains with a top-level domain of ".jp" (herein, "domestic domains") and ICMP error packets indicating that the destination DNS service port was unreachable (see Figure 3) [(*3)].

JPCERT/CC believes this may be the first case of DDoS attack targeting domains with the top-level domain .jp in which the DNS Water Torture method was used.



[Figure 3: Packet with source port number 53/UDP captured in February 2015 (displayed with Wireshark)]

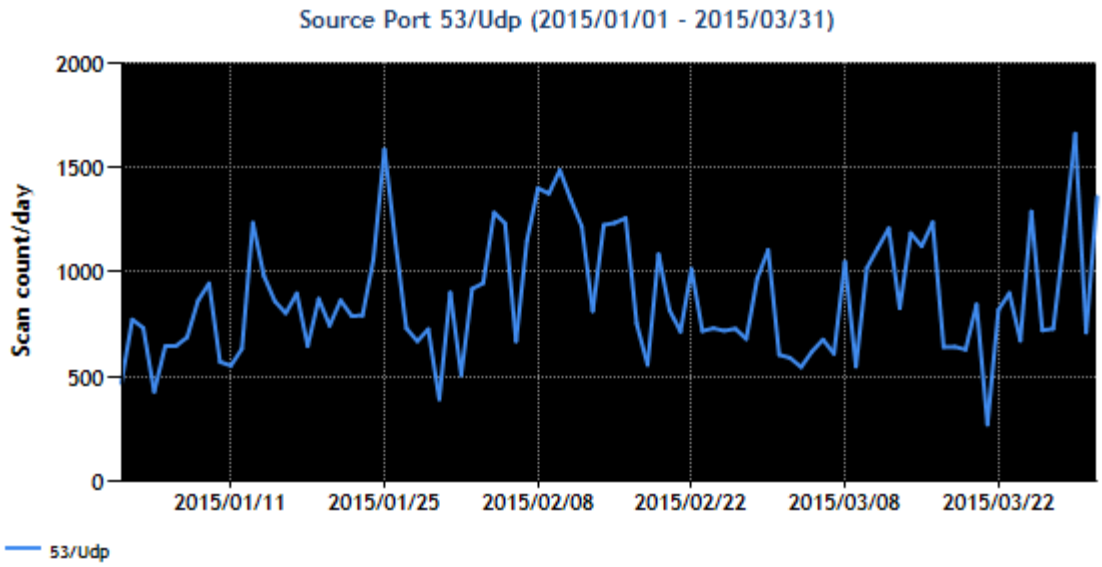
The domestic domains that were targeted in the DNS Water Torture attacks were registered on authoritative DNS servers operated by a domain registration service provider in Japan. These authoritative DNS servers managed the domains of a number of domestic websites with a large user base (herein, authoritative DNS servers managing multiple domains are referred to as "shared DNS servers"). Consequently, it is presumed that as the shared domestic DNS servers became overloaded by the attack, domains managed by the same shared DNS servers (e.g. operators providing cloud-based services and online games) other than the targeted domestic domains also experienced name resolution failure, giving rise to such problems as access to websites getting denied and e-mails failing to reach their destinations.

With these shared domestic DNS servers failing to respond, open resolvers that took part in the attack as well as the cache DNS servers of ISPs, etc., that exist between the shared domestic DNS servers become overloaded with queries waiting for a response from the shared DNS servers. Accordingly, it is presumed that users of these cache DNS servers also experienced such problems as access to websites getting denied and e-mail delivery errors.

Upon examining the WHOIS information, JPCERT/CC found that the domestic domains were initially registered on shared domestic DNS servers when the attack occurred, but were later registered on shared DNS servers operated by an overseas operator. It is presumed that this change was made as a countermeasure against the attack.

In early March, DNS answer packets and ICMP error packets indicating that the DNS service port was unreachable were observed with respect to domains managed by shared DNS servers operated by a major U.S. registrar. The shared DNS servers of this registrar are sometimes used by Japanese website operators to register their domains. Therefore, domains using these DNS servers may have experienced failures such as denied access to websites due to the attack.

Figure 4 plots the number of UDP packets observed with source port number 53 during this quarter. Although not all the packets in the graph are DDoS attack packets, JPCERT/CC has been observing many packets that appear to be related to DDoS attacks.



[Figure 4: Number of UDP packets observed with source port number 53 from January through March 2015]

There is a large number of open resolvers in Japan that are involved in not only the DNS Water Torture attacks targeting domestic domains that JPCERT/CC has confirmed during this quarter, but also other DNS Water Torture attacks and DNS amplification attacks targeting overseas domains that occur on a daily basis. While it may be unintended, the fact that so many open resolvers are taking part in DDoS attacks is a matter of grave concern for our country. In order to reduce the number of open resolvers that are being used as springboards for attack, please pay attention to the following points in particular.

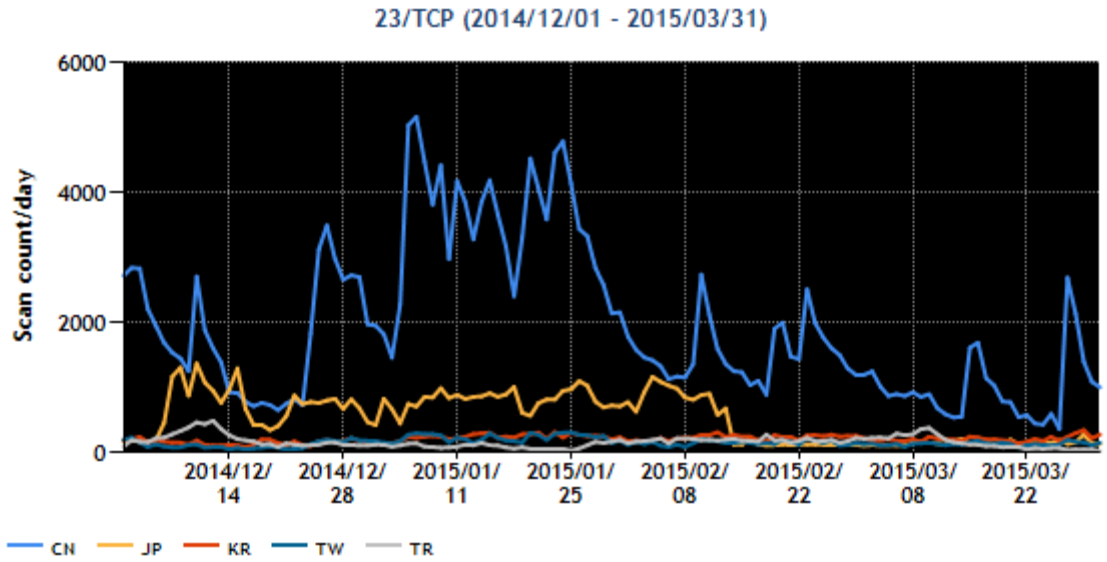
1. If DNS servers are used, please review the settings, such as the range of recursive queries that are accepted, and restrict access to the minimum necessary extent. (*4,5,6)
2. If gateway routers facing the Internet or other network devices equipped with DNS server or DNS forwarder functionality are used, please ensure that the settings are configured so as not to respond to DNS queries from an unspecified host. It is recommended that the settings are verified using the information published by each product vendor as a reference. (*6,7)
3. If public servers such as a web server are being operated, make sure that no unnecessary DNS server is in operation.

As part of its activities aimed at reducing the number of open resolvers, JPCERT/CC is investigating DNS answer packets and ICMP error packets observed by its Internet threat monitoring system indicating that the DNS service port was unreachable, and requesting the administrators of the domestic IP addresses

that were identified as the source to conduct an investigation.

2.2 Decrease in the number of packets targeted to 23/TCP

As indicated in Figure 5, the number of packets targeted to 23/TCP has fallen since January during this quarter. While China accounts for approximately 54% of the packets targeted to 23/TCP, the number of packets originating in China fell dramatically since January, which resulted in an overall decline. The reason for the decrease in the number of packets originating in China is unknown. The number of packets originating in Japan has also been declining since early February. The increase in the number of packets targeted to 23/TCP originating in Japan observed during the previous quarter, as described in section "2.1 Increase in the number of packets targeted to 23/TCP and 8080/TCP" (*8) of the previous Threat Monitoring Report, was assumed to have been caused by a malware infection of QNAP network attached storage (NAS) products (herein, "QNAP NAS") with a known vulnerability (so-called Shellshock).



[Figure 5: Number of observed packets targeted to 23/TCP from December through March 2015 (by source region)]

In order to reduce the number of malware infections that are being used as springboards for attack, JPCERT/CC has conducted a thorough investigation of the source nodes of observed packets targeted to 23/TCP. As a result, JPCERT/CC requested the administrators of IP addresses, etc., when QNAP NAS operating in Japan were identified (nodes allocated with a dynamic IP address may have received multiple contacts). Administrators contacted by JPCERT/CC responded, saying that they would take appropriate measures, that they have dealt with suspicious users identified on their NAS, that they had removed the relevant equipment, and so on.

As indicated in Figure 5, the number of packets targeted to 23/TCP originating in Japan has fallen since

early February. While the possibility of a change in malware behavior cannot be completely ruled out, JPCERT/CC believes that anti-malware measures implemented by QNAP NAS users in response to its request had an impact.

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 (Apr-Jun 2014)
https://www.jpcert.or.jp/tsubame/report/report201404-06.html
(3) National Police Agency@Police
Internet Monitoring Results (Feb 2015) <Japanese only>
https://www.npa.go.jp/cyberpolice/detect/pdf/20150331.pdf
(4) Japan Registry Services Co., Ltd. (JPRS)
Open resolvers: Inappropriate settings of DNS servers <Japanese only>
http://jprs.jp/important/2013/130418.html
(5) Japan Network Information Center (JPNIC)
Note on open resolvers <Japanese only>
https://www.nic.ad.jp/ja/dns/openresolver/
(6) JPCERT/CC
Open resolver verification site <Japanese only>
http://www.openresolver.jp/
(7) JVN#62507275 A number of broadband routers known to function as open resolvers <Japanese only>
https://jvn.jp/jp/JVN62507275/
(8) JPCERT/CC Internet Threat Monitoring Report (Oct-Dec 2014)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html#2.1

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