JPCERT-IA-2014-02
Issued : 2014-04-21

JPCERT/CC Internet Threat Monitoring Report [January 1, 2014 – March 31, 2014]

1 Overview

JPCERT/CC has placed multiple sensors across the internet for monitoring to continuously gather packets. These packets are categorized by the destination port number, source region, etc. When analyzing this information along with information about vulnerabilities, malware and attack tools to obtain information on attacking activities and their symptoms. This report will mainly show the analysis results of packets targeted to Japan during the period January 1, 2014 through March 31, 2014 (herein, "this quarter")

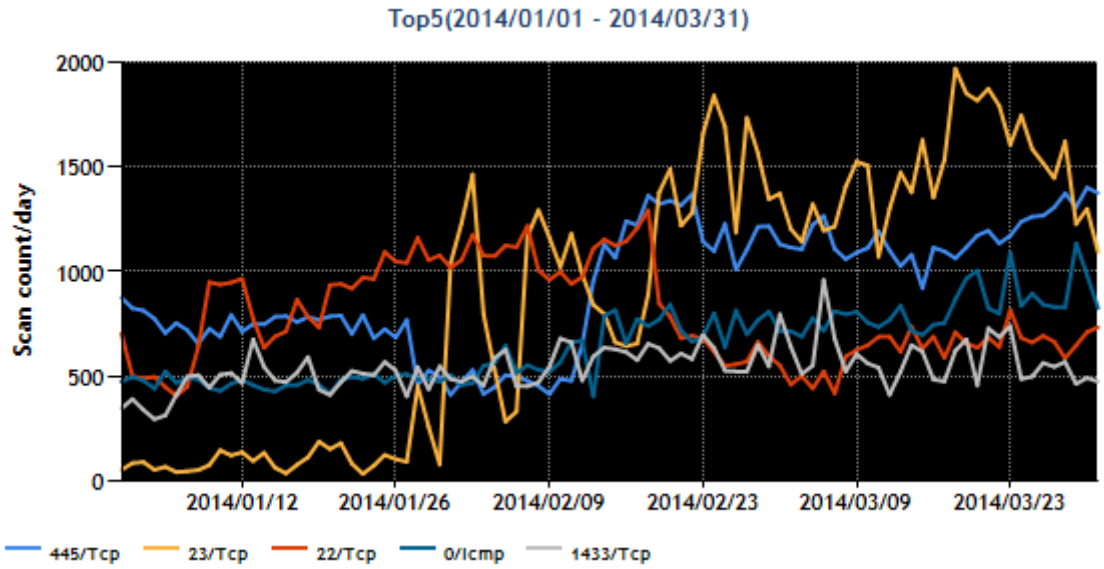
The top 5 destination port numbers for which packets were observed to receive packets during this quarter are listed in [Chart 1]

[Chart1: Top 5 Destination Port Numbers]

October - December 2013		January - March 2014	
1	445/TCP (microsoft-ds)	1	445/TCP (microsoft-ds)
2	0/ICMP	2	23/TCP (telnet)
3	1433/TCP (ms-sql-s)	3	22/TCP (ssh)
4	22/TCP (ssh)	4	0/ICMP
5	3389/TCP (ms-wbt-server)	5	1433/TCP (ms-sql-s)

* 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 for that service / protocol.

[Figure1] shows the change over the 3 month period in the packets that the top 5 destination ports received.



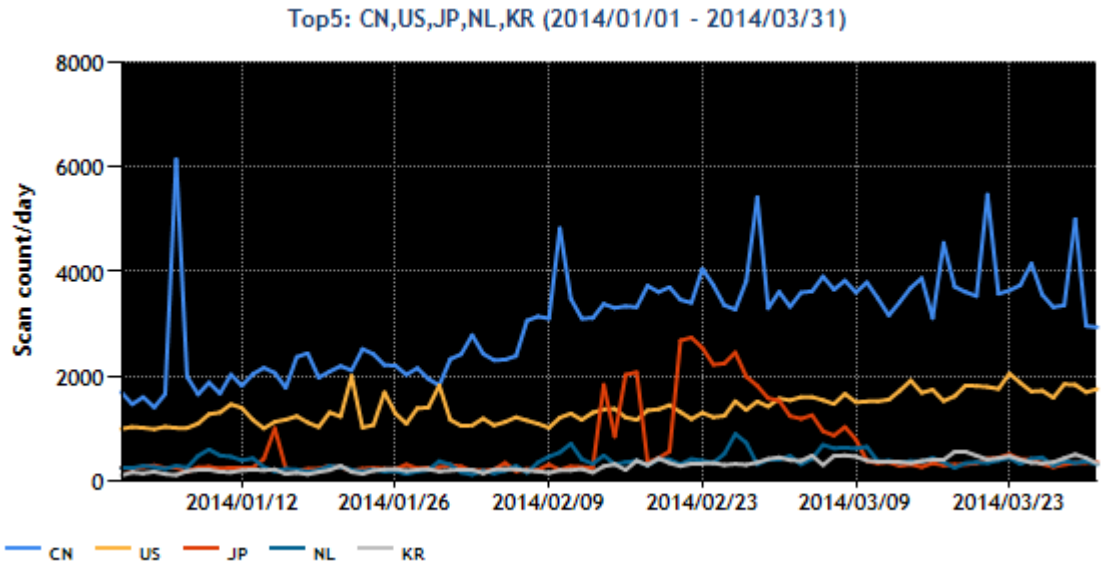
[Figure1: Number of packets observed at top 5 destination ports from January through March, 2014

The top 5 source regions for which packets were observed to come from this quarter are listed in [Chart2]

[Chart2: Top 5 source region]

October - December 2013		January - March 2014	
1	China	1	China
2	USA	2	USA
3	Netherlands	3	Japan
4	Japan	4	Netherlands
5	Russia	5	South Korea

[Figure2] shows the change over the 3 month period in packets sent from the top 5 source regions



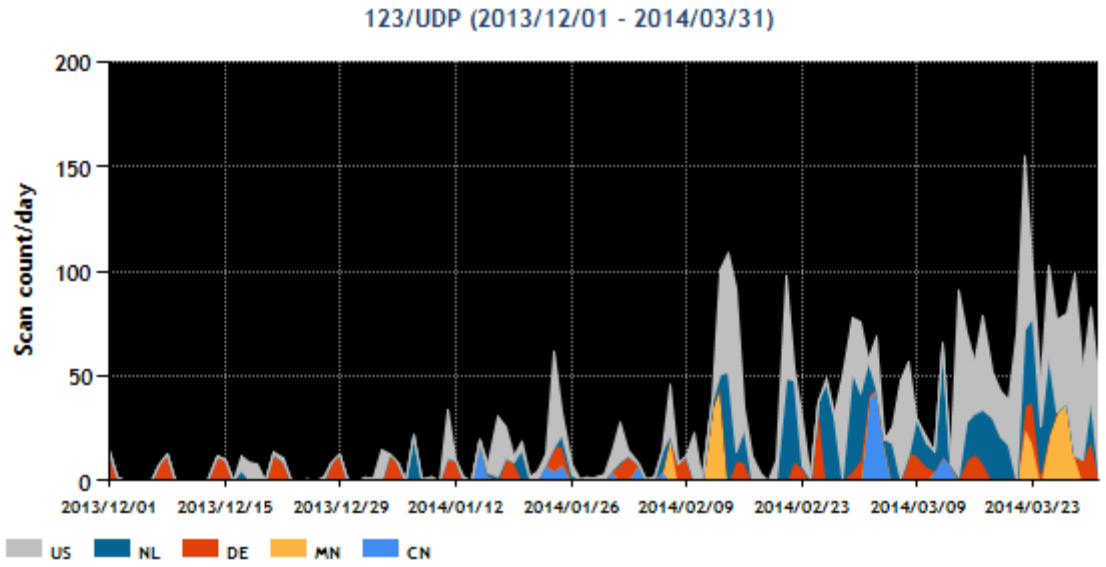
[Figure2: Number of packets observed from the top 5 source regions from January through March]

After late January, there was an increase in packets to 445/TCP and 23/TCP. What was observed at 23/TCP, which received the second most packets this quarter will be described in section 2.2. Around mid-February, an increase in the number of packets from Japan was observed. This was due to a particular sensor receiving a large number of packets targeted at 13832/TCP, 43962/TCP and 12591/TCP. JPCERT/CC surveyed the services and product vulnerabilities related to these port numbers; however, no relevant information could be discovered, and no other sensor saw such a change - so it was determined that this data did not represent a widespread threat. There were some increases and decreases at other ports but there was nothing of note.

2 Events of Note

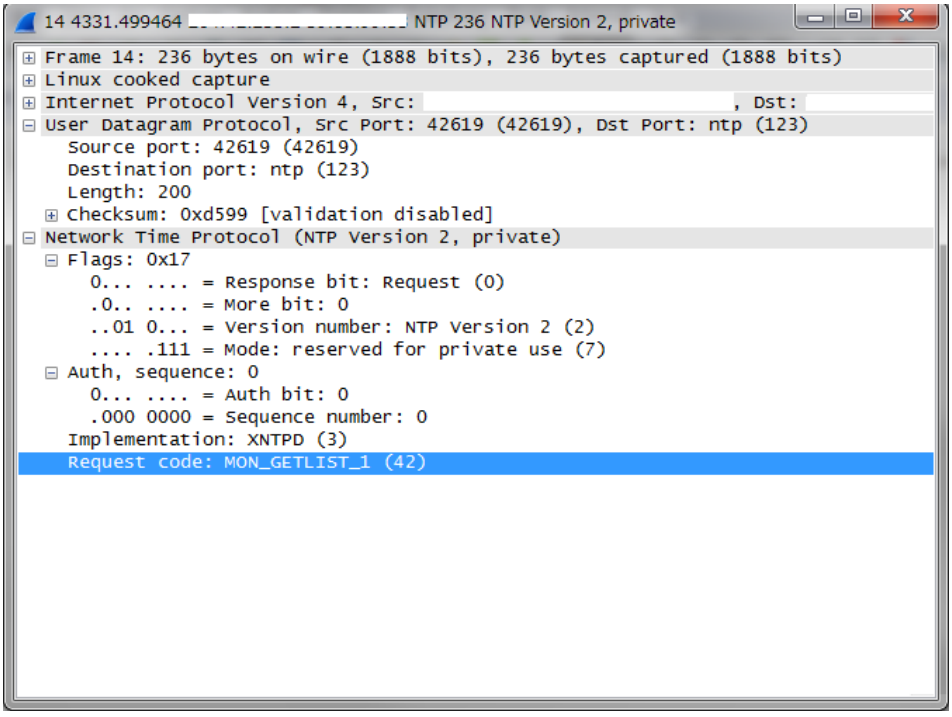
2.1 Increase in packets to port 123/UDP

An increase in packets to port 123/UDP reported in the previous Internet Threat Monitoring Report[*2] continued this quarter. In particular, an increase in packets from USA and Netherlands was noteworthy.



[Figure3: Number of packets observed targeted to 123/UDP during December 2013 through March 2014]

According to information from CloudFlare, Inc., [*3,4] DDoS attacks (up to around 400Gbps) leveraging NTP servers in Europe were observed in February 2014. Also, domestic observation sensors periodically received scan packets believed to target the monlist function in NTP servers. (Figure4 shows a packet observed at one of the domestic sensors)



[Figure4 : Packet to 123/UDP in January 2014 (displayed using Wireshark)]

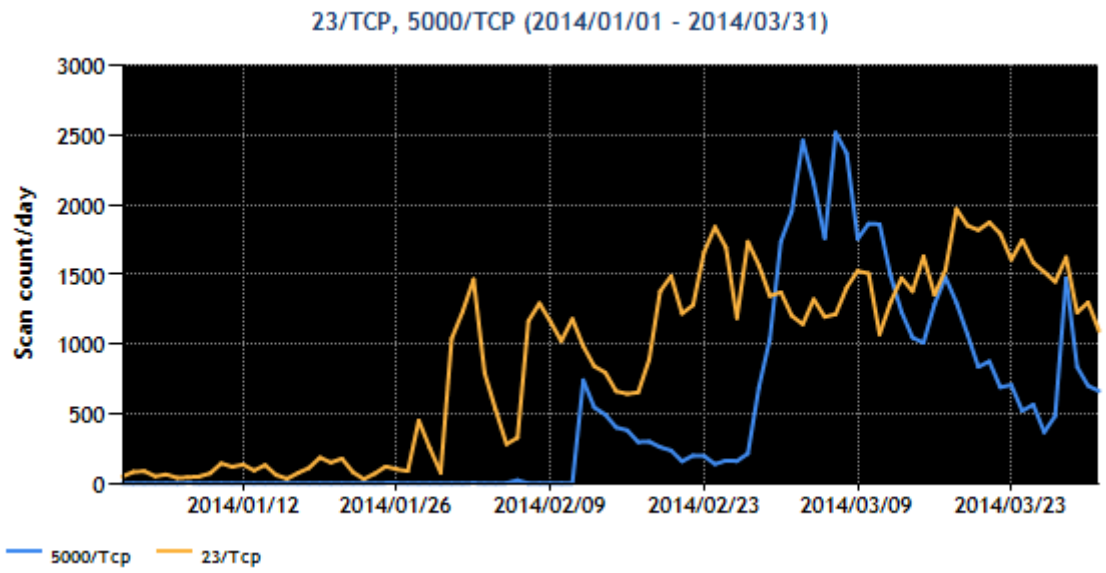
There is a possibility that scans looking for NTP servers and DDoS attacks leveraging NTP servers may

continue, so servers and network devices that run NTP server program should be checked and proper security countermeasures (patches, updates, access restrictions, check security settings, etc.) [*5, 6] should be put in place so that they are not leveraged in attacks.

2.2 Increase in packets to 23/TCP and 5000/TCP

There was an increase in the number of packets to 23/TCP observed since late January of this quarter. There is a recurrence in activities searching for network devices that have servers listening on telnet. (Previous Internet Threat Monitoring Reports [*7,8] described activities searching for telnet servers.)

A characteristic observed this quarter was while the increase in packets to 23/TCP was being observed, an increase in packets to 5000/TCP was also observed beginning in early February. It was ranked 6th largest in number of packets this quarter. This was probably due to network devices infected by malware searching for 5000/TCP used by vulnerable NAS products[*9] , in addition to searching for port 23/TCP.



[Figure5: Number of Packets to 23/TCP and 5000/TCP]

The top region observed sending packets to 23/TCP and 5000/TCP this quarter was China who sent around 60% of packets to 23/TCP and around 30% of packets to 5000/TCP (both in number based percentage). JPCERT/CC investigated the IP addresses sending the packets to 23/TCP and 5000/TCP and found that at a lot of the IP addresses a network camera product provided by a specific foreign vendor was running. We observed scanning activities from a domestic IP address and verified that this product was placed there.

Network cameras and NAS products placed on the internet are also targets for scanning activities[*10,11,12] ,

so it is necessary to have the proper security measures (patches, updates, access restrictions, check security settings, etc.) implemented in these devices.

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 (October – December 2013) <Japanese only>
https://www.jpcert.or.jp/tsubame/report/report201301-03.html

(3) Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

(4) Understanding and mitigating NTP-based DDoS attacks
http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks

(5) Vulnerability Note VU#348126
NTP can be abused to amplify denial-of-service attack traffic
https://www.kb.cert.org/vuls/id/348126

(6) Alert regarding DDoS attacks leveraging the monlist function in ntpd
https://www.jpcert.or.jp/english/at/2014/at140001.html

(7) JPCERT/CC Internet Threat Monitoring Report (January – March 2012) <Japanese only>
https://www.jpcert.or.jp/tsubame/report/report201201-03.html

(8) JPCERT/CC Internet Threat Monitoring Report (April – June 2012) <Japanese only>
https://www.jpcert.or.jp/tsubame/report/report201204-06.html

(9) Vulnerability Note VU#615910
Synology DiskStation Manager arbitrary file modification
https://www.kb.cert.org/vuls/id/615910

(10) Destination port used to search for vulnerable NAS, sudden increase in access to 5000/TCP <Japanese only>
http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf

(11) More Device Malware: This is why your DVR attacked my Synology DiskStation (and now with Bitcoin Miner!)
https://isc.sans.edu/forums/diary/More+Device+Malware+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+and+now+with+Bitcoin+Miner/17879

(12) IoT Worm Used to Mine Cryptocurrency
http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Information Security Countermeasure Promotion Activities for the 2013 Fiscal Year".