JPCERT-TBM-2019-01

Issued: 2019-1-16

JPCERT/CC Internet Threat Monitoring Report [October 1, 2018 - December 31, 2018]

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.

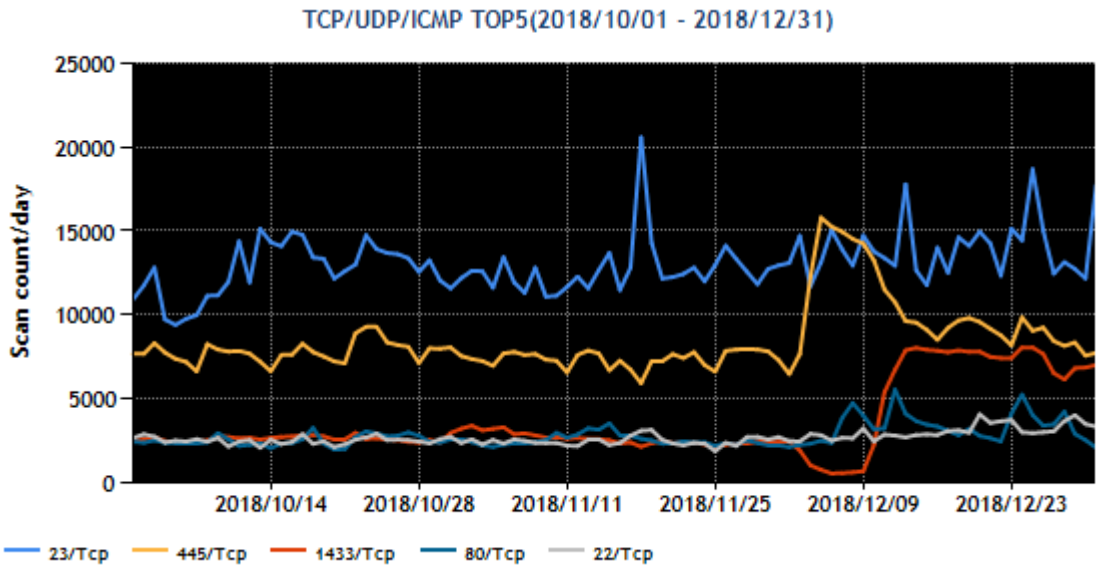
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[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	1433/TCP (ms-sql)	6
4	80/TCP (http)	3
5	22/TCP (ssh)	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 in [Figure 1].



[Figure 1 : Number of packets observed at top 5 destination ports from October through December 2018]

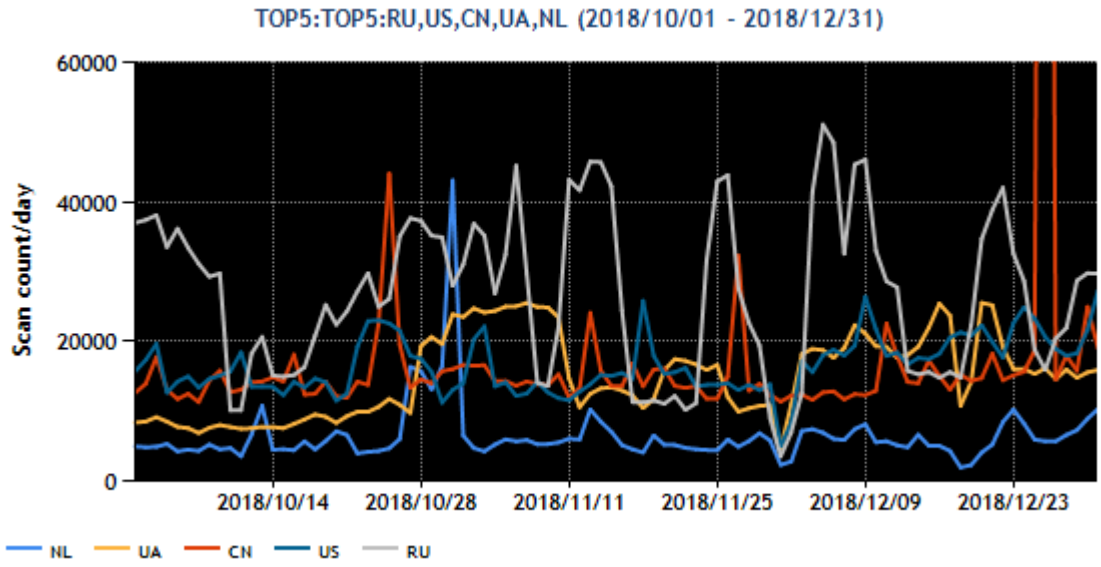
There was a sharp rise in the number of packets targeted to port 445/TCP around December 3. In addition, the number of packets targeted to 1433/TCP increased sharply around December 10. This phenomenon will be discussed in section 2.1 "Increase in the number of packets from sources that appear to be Windows environments."

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	Russia	2
2	USA	3
3	China	1
4	Ukraine	5
5	Netherlands	4

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



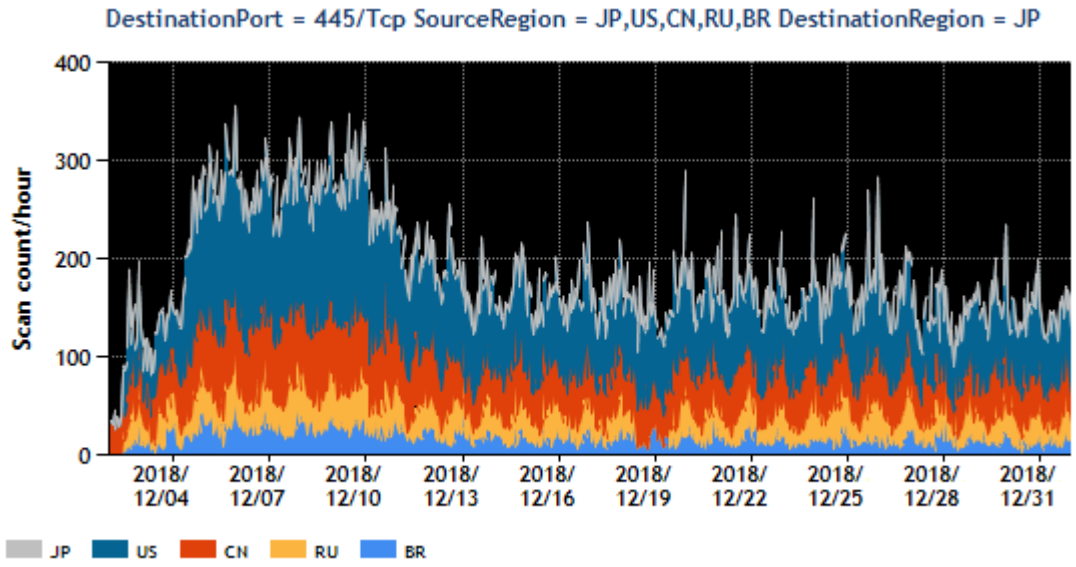
[Figure 2 : Number of observed packets of the top 5 source regions from October through December 2018]

In terms of source regions, the number of packets originating in Ukraine started increasing from August 20 in the previous quarter and has remained high this quarter. Meanwhile, the number of packets originating in China exceeded that of other regions only for a short period of time, and accordingly China fell to third place in the ranking.

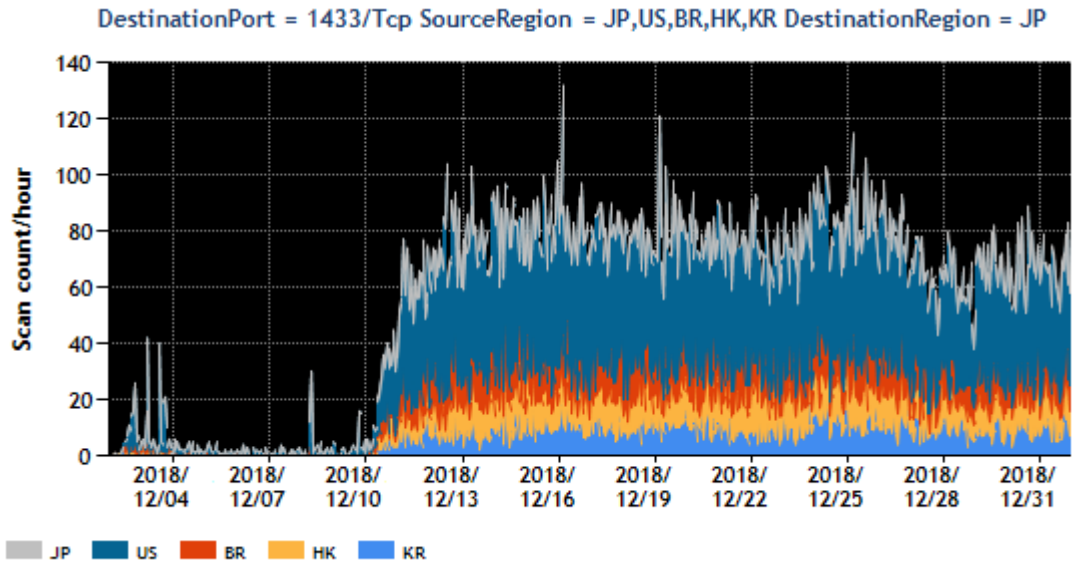
2. Events of Note

2.1. Packets from sources that appear to be Windows environments

Since around December 3, 2018, the number of packets targeted to port 445/TCP has remained high [Figure 3]. In addition, packets targeted to port 1433/TCP have also increased since around December 10 [Figure 4]. These packets include those with a source IP address in Japan and those originating abroad, with greater numbers of packets seen for both compared to before. This phenomenon is observed not only with packets received in Japan but also with those reaching other regions.



[Figure 3: Number of observed packets targeted to port 445/TCP by major source regions]



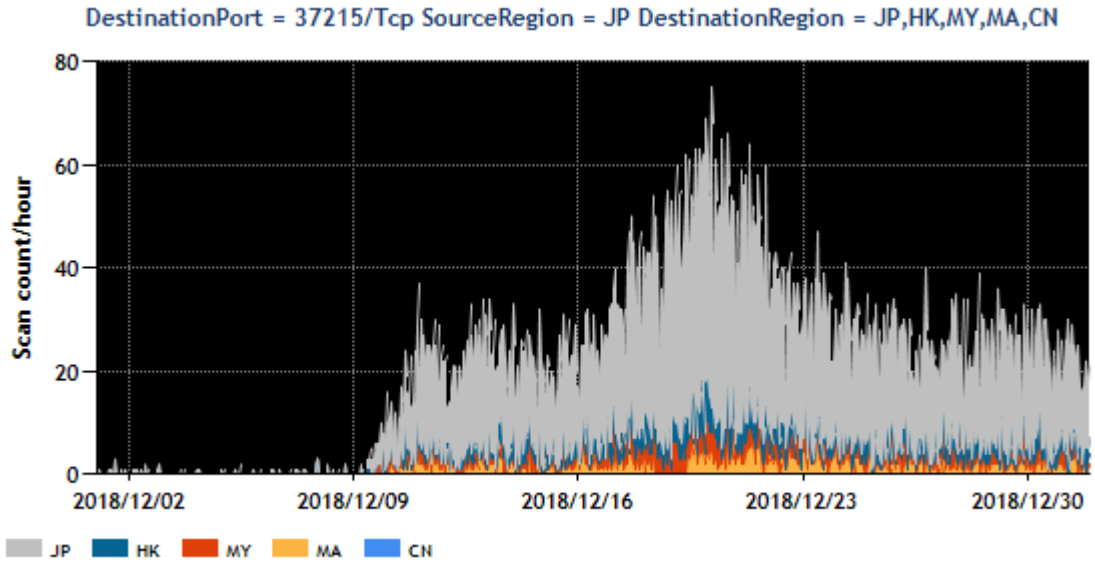
[Figure 4 : Number of observed packets targeted to port 1433/TCP by major source regions]

According to an investigation conducted by JPCERT/CC, IIS and SMB are running on many of the hosts that are sending packets to these two ports, which suggests that these are Windows environments. Sources included Windows 2003 as well as newer versions of the operating system such as 2008 and 2012, and SMB ports were open in some cases while closed in others. As such, no common characteristics were found. JPCERT/CC still has not been able to identify the malware that has infected these hosts and is sending the packets.

To collect information regarding this matter, JPCERT/CC is contacting all the entities managing the source IP addresses of these packets that appear to have been sent from a company or other organizations in Japan.

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

Since around December 9, 2018, the number of packets originating in Japan and targeted to port 37215/TCP has increased(*2) [Figure 5]. Similar packets are also widely observed by sensors deployed overseas. JPCERT/CC has investigated the sources of these packets and found that they were broadband routers manufactured by a Japanese vendor and impacted by a vulnerability in the Realtek SDK (CVE-2014-8361)(*3). These routers were using IP addresses allocated to a number of Internet service providers, etc. It is presumed that these routers had the vulnerability left unaddressed and were infected with a Mirai variant. JPCERT/CC is contacting the entities managing the relevant IP addresses to urge users of vulnerable routers infected with malware to implement countermeasures.



[Figure 5 : Number of observed packets targeted to port 37215/TCP by major source regions]

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)
https://twitter.com/nicter_jp/status/1072774530202972160

(3) [Findings from the honeytrap] Observations on attacks targeting ports 52869/TCP and 8081/TCP (Japanese) https://sec-chick.hatenablog.com/entry/2019/01/05/145542

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 2018 Fiscal Year."