JPCERT-TBM-2018-04
Issued: 2018-10-18

JPCERT/CC Internet Threat Monitoring Report
[July 1, 2018 - September 30, 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.

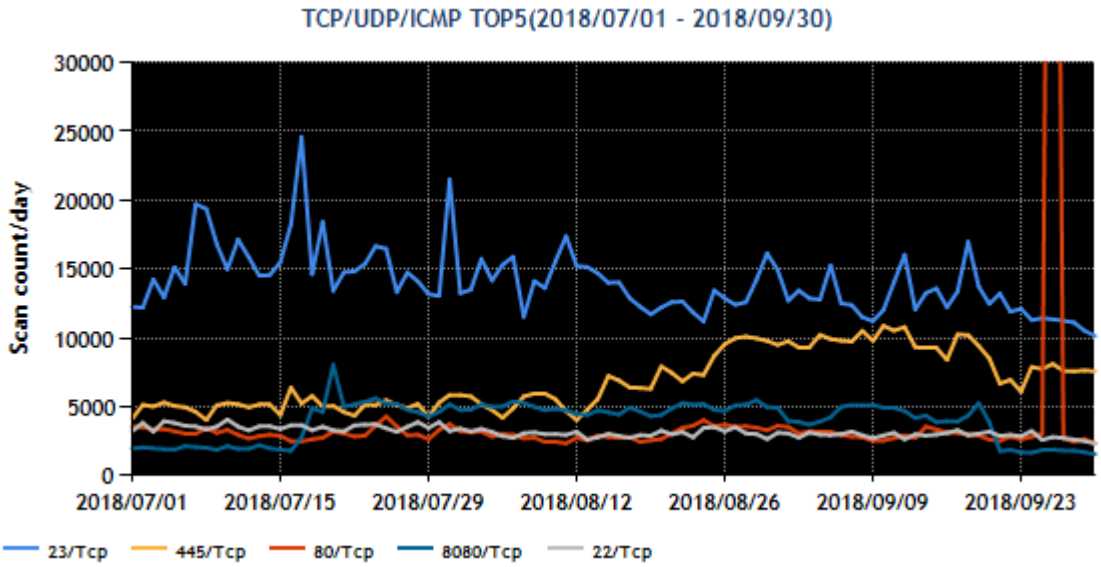
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[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	80/TCP (http)	3
4	8080/TCP	6
5	22/TCP (ssh)	4

*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.

The numbers of packets observed for the destination port numbers listed in [Chart 1] are shown in [Figure 1].



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

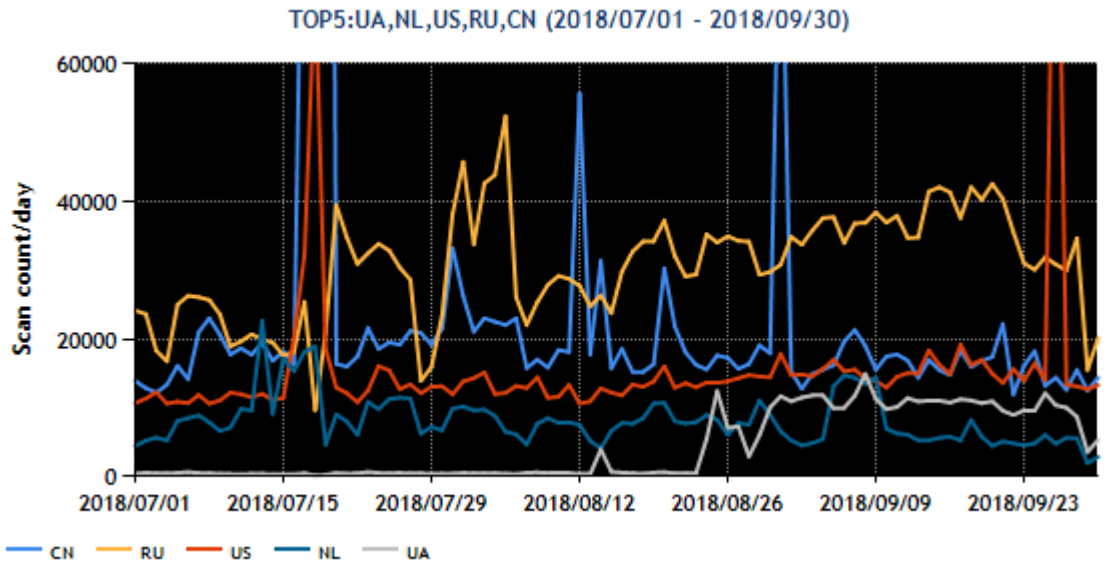
The number of packets targeted to 445/TCP has been increasing since August 12. This phenomenon will be discussed in section "2.1 Increase in the number of packets targeted to port 445/TCP".
The increase seen in the numbers of packets targeted to a number of ports including 8080/TCP is probably due to some malware changing the port targeted for scanning.

Similarly, the top 5 source IP addresses by region with the greatest numbers of packets are shown in [Chart 2].

[Chart 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	China	2
2	Russia	3
3	USA	1
4	Netherlands	5
5	Ukraine	Not in top 10

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



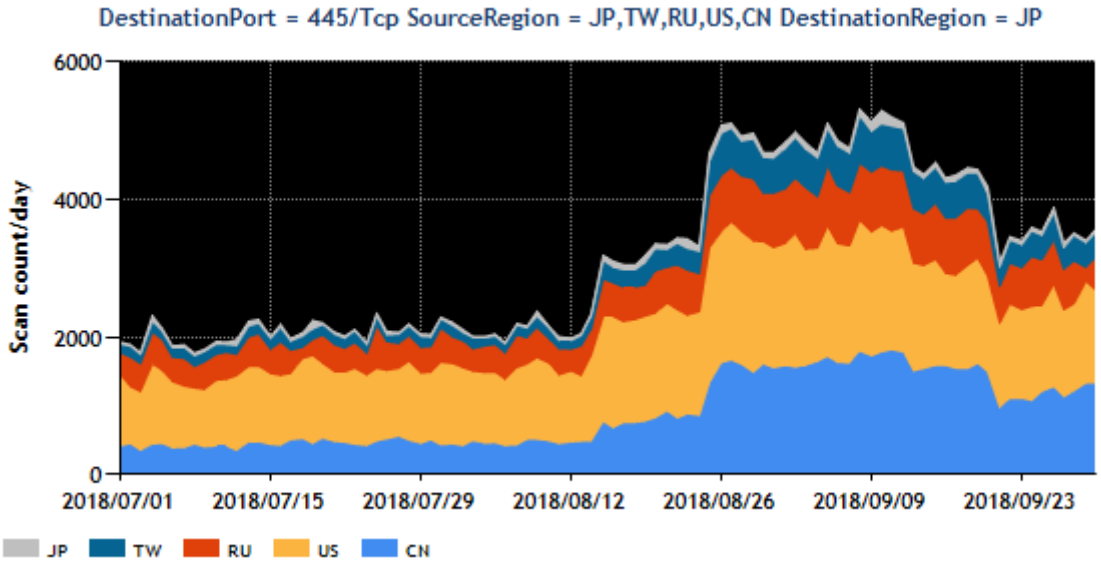
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2018]

In terms of source regions, the number of packets originating in Ukraine has been increasing from around August 20. The devices sending the packets all had the same port open. It is assumed that devices widely used in the region became infected with malware and are sending these packets.

2. Events of Note

2.1. Increase in the number of packets targeted to port 445/TCP

From around August 12, 2018, JPCERT/CC has been seeing an increase in the number of packets targeted to port 445/TCP(*2) [Figure 3]. The source IP addresses of these packets include IP addresses in Japan and abroad, and the number of packets has increased for both. This phenomenon is observed in other regions outside Japan as well.



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

As for packets targeted to port 445/TCP, those associated with the reconnaissance activity of WannaCry, etc. have been observed since May 2017(*3), but packets with different characteristics started being seen from August 12 as well. JPCERT/CC investigated domestic and overseas IP addresses where packets with these characteristics originated and found that, while over 80% of the sources were hosts running Windows 2003, there were also those running other versions including Windows 2008R2. Apparently, this is not a problem that only concerns Windows 2003.

Of the packets sent from within Japan, JPCERT/CC contacted managers of relevant IP addresses for packets that appeared to be sent from a company or other organization. Some of the managers have replied that they detected malware with anti-virus software, but details of detection results and malware samples have not been obtained. JPCERT/CC continues to collect information on this matter.

In most of the cases identified during this quarter, Windows 2003 was used as the operating system. It is strongly recommended that servers made accessible from the Internet run an operating system with necessary measures taken by the manufacturer against vulnerabilities(*4).

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) Observation Report for August 2018 (Japanese)
https://www.npa.go.jp/cyberpolice/detect/pdf/20180928_1_toukei.pdf

(3) Internet Threat Monitoring Report (Jul-Sep 2017)
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2017Q2_en.pdf

(4) Extended support for Windows Server 2003 ended on July 14, 2015.
https://www.microsoft.com/ja-jp/cloud-platform/windows-server-2003

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