JPCERT/CC Internet Threat Monitoring Report

July 1, 2022 - September 30, 2022

JPCERT Coordination Center

October 26, 2022

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 works mainly with overseas National CSIRTs to deploy sensors at each organization and have them 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 by sensors located in Japan during this quarter.

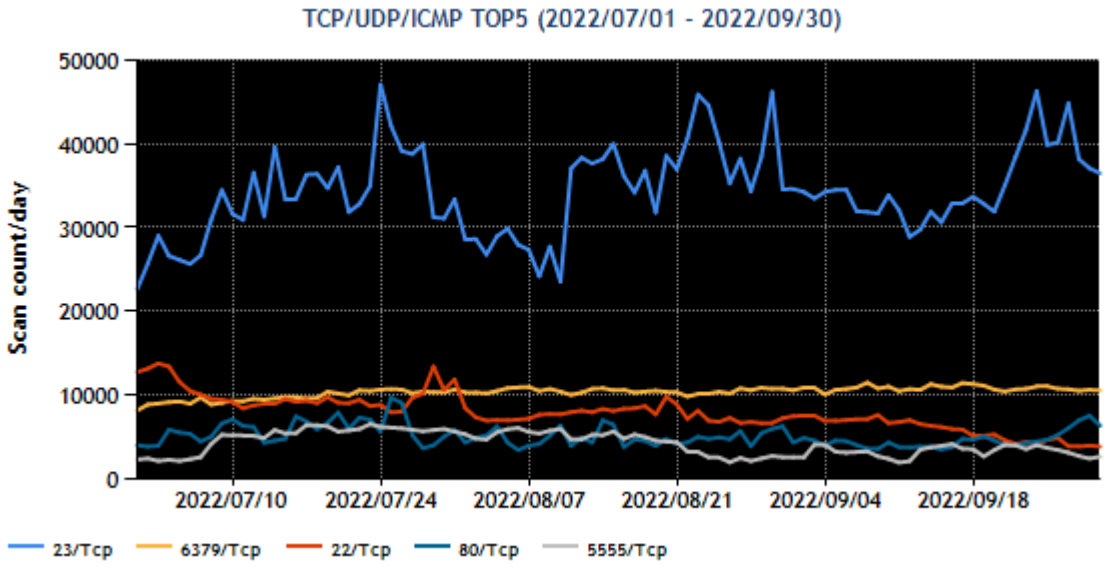
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP（telnet）	1
2	6379/TCP（redis）	2
3	22/TCP（ssh）	3
4	80/TCP （http)	4
5	5555/TCP	8

*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 July through September 2022]

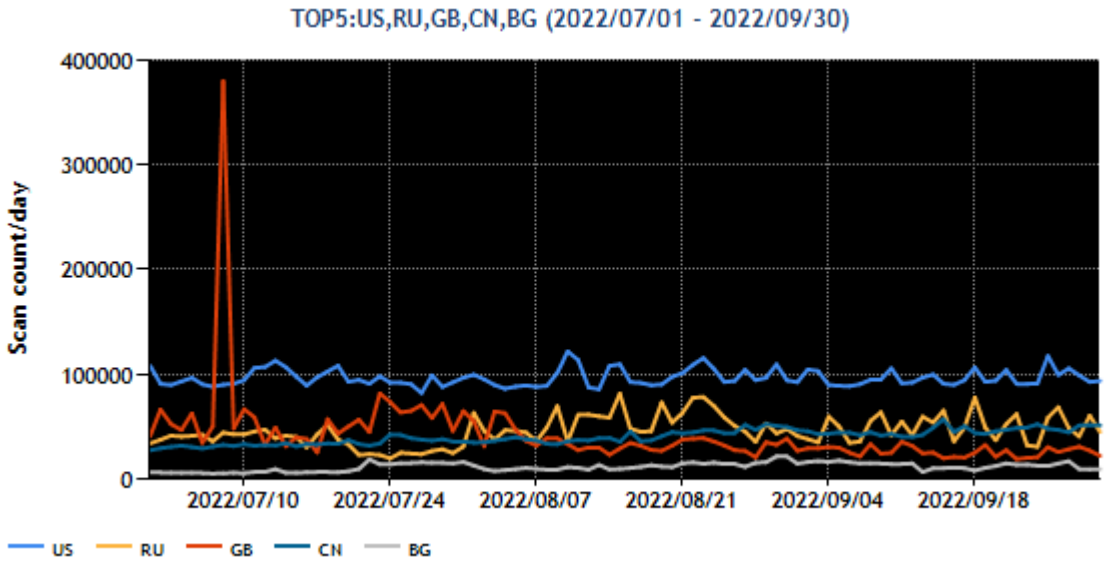
Port 23/TCP(telnet) received the largest number of packets with repeated fluctuations seen during the quarter. The number of packets targeted to port 6379/TCP continued to increase slightly throughout the quarter.

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	3
3	Great Britain	2
4	China	4
5	Bulgaria	6

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



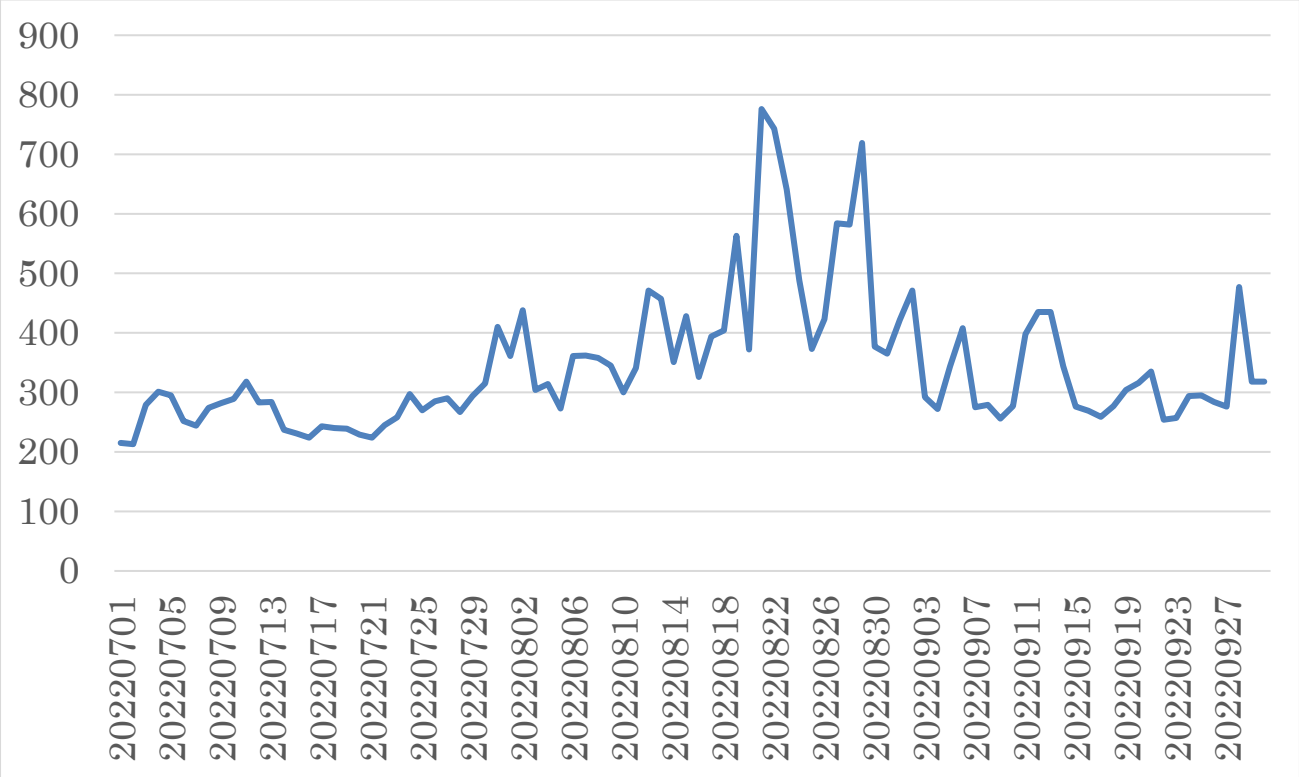
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2022]

Russia saw the number of packets go up from early August and changed places with China in the rankings. The number of packets from South Korea started to decrease from around August 7, and the country fell to sixth place in the rankings, with Bulgaria, which saw minimal changes, moving up to fifth.

2. Events of Note

2.1. Observation of backscatter packets

The observation of packets with SYN and ACK flags and those with ACK and RST flags ("backscatter packets"), which are seen when subjected to a DDoS attack, is shown in [Figure 3].
Such backscatter packets are observed in the case of a SYN flood attack, which is a form of DDoS attack. This type of DDoS attack sends attack packets with a SYN flag and randomly set source address to the target server. The server sends back answer packets with SYN and ACK flags. It is assumed that these answer packets were observed because the randomly set sources of attack packets happened to include those with the same IP address as a TSUBAME sensor.



[Figure 3: Number of IP addresses that sent packets with the characteristics of backscatter packets]

In a past issue of the Internet Threat Monitoring Report, JPCERT/CC discussed an increase in the number of backscatter packets originating in Ukraine. A few characteristic events were seen in this quarter as well, which are discussed below.

1. Backscatter packets from Japan observed around September 6
2. Backscatter packets from Taiwan observed around early August

[Chart 3] shows the observation of backscatter packets sent from Japan during the quarter, for which the sending organizations could be inferred. The number of source IP addresses for backscatter packets temporarily increased around September 6.

[Chart 3: Observation of backscatter packets from Japan]

*Source IP addresses: Services provided by the organizations that own the addresses are listed

Source IP addresses*	2022-09-01	2022-09-02	2022-09-03	2022-09-04	2022-09-05	2022-09-06	2022-09-07	2022-09-08	2022-09-09	2022-09-10
Cloud service provider A		○								
Government site A						○				
Portal site A						○				
Portal site B						○				
Portal site C						○				
Portal site D						○				
Portal site E						○				
Portal site F						○				
Portal site G						○				
General shopping mall A						○				
Video streaming service A						○	○			
Power company A							○			
Internet media business A								○		
Internet media business B								○		

The sources of these packets included sites of a major e-commerce company, major portal site, Internet media, video service, critical infrastructure provider, and government. The source port number for almost all the packets was 443/TCP, which indicates that a SYN flood attack targeting ports used by HTTPS was being carried out.

Similar packets were also received in early August from IP addresses used in Taiwan. [Chart 4] shows the observation of backscatter packets sent from Japan during the quarter, for which the sending organizations could be inferred.

[Chart 4: Observation of backscatter packets from Taiwan]

*Source IP addresses: Services provided by the organizations that own the addresses are listed

Source IP addresses*	2022-08-01	2022-08-02	2022-08-03	2022-08-04	2022-08-05	2022-08-06	2022-08-07	2022-08-08	2022-08-09	2022-08-10
CDN (government/finance) A		○								
CDN (government/finance) B		○								
Telecommunications carrier A		○								
E-commerce site A				○						
Government site A					○					
CDN (government/finance) C						○				
Security vendor A							○			
Finance (bank) A										○
E-commerce site B										○
Finance (insurance) A										○
Information and communications A										○
Power company A										○
Finance (bank) B										○
Finance (bank) C										○
Finance (bank) D										○
Finance (bank) E										○
Finance (bank) F										○
Finance (bank) G										○

The sources included a number of financial institutions, a life insurance company, and government sites using a content delivery network (CDN). The source port number was 443/TCP, which indicates that a SYN flood attack targeting ports used by the HTTPS was likewise being carried out.

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

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 2022.