JPCERT/CC Internet Threat Monitoring Report

January 1, 2022 ～ March 31, 2022

JPCERT Coordination Center

April 21, 2022

JPCERT CC®

Table of Contents

1. Overview

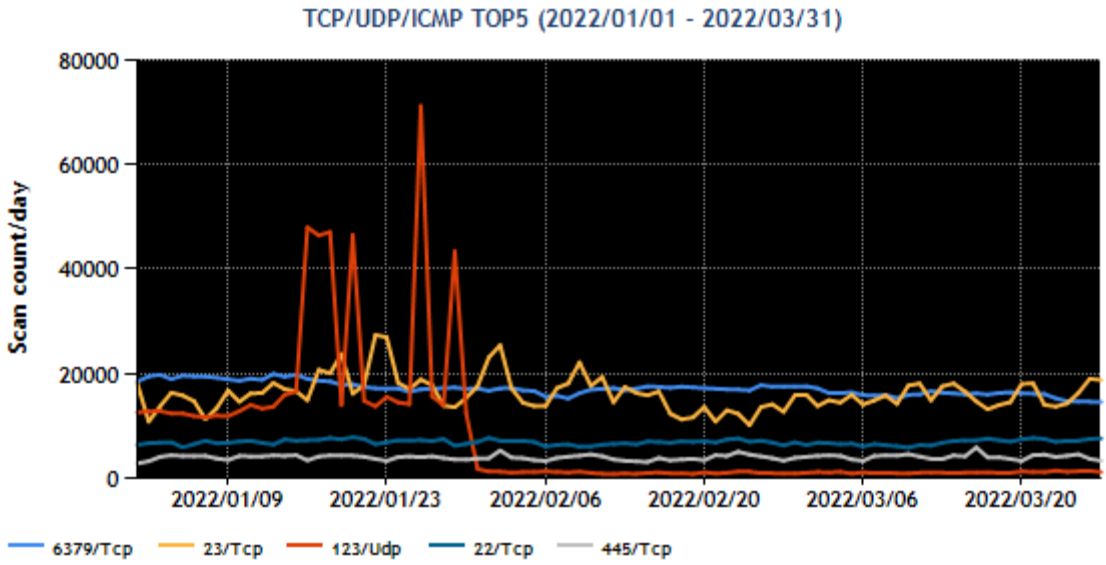
JPCERT/CC has placed multiple sensors across the Internet for monitoring to continuously gather packets which are dispatched to indefinite nodes on the Internet. These packets are categorized by the destination port number, source region, etc. Then this information is analyzed along with information 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	6379/TCP (redis)	1
2	23/TCP (telnet)	2
3	123/UDP (ntp)	6
4	22/TCP (ssh)	3
5	445/TCP (microsoft-ds)	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 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 January through March 2022]

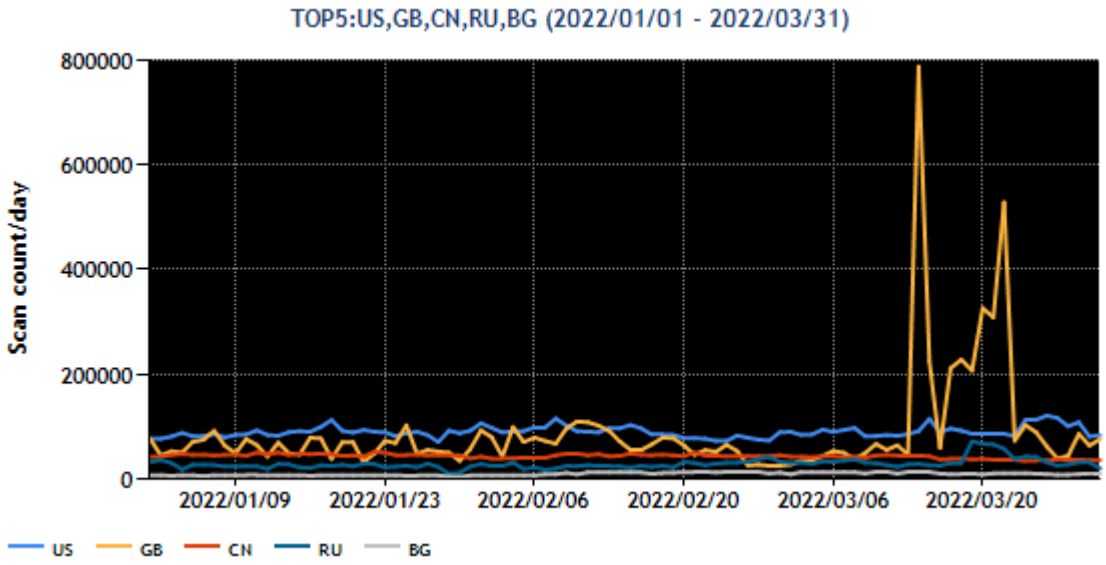
Port 6379/TCP (redis) received the greatest number of packets. During this period, packets targeted to port 6379/TCP appeared to decrease gradually, ending the period about 20% less than when it started. Port 23/TCP, which received the second most packets, saw a number of brief fluctuations. This was probably due to repeated attacks attempting to infect IoT and other devices with malware, causing the number of packets observed to increase for port 23/TCP.

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	Great Britain	2
3	China	4
4	Russia	3
5	Bulgaria	6

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



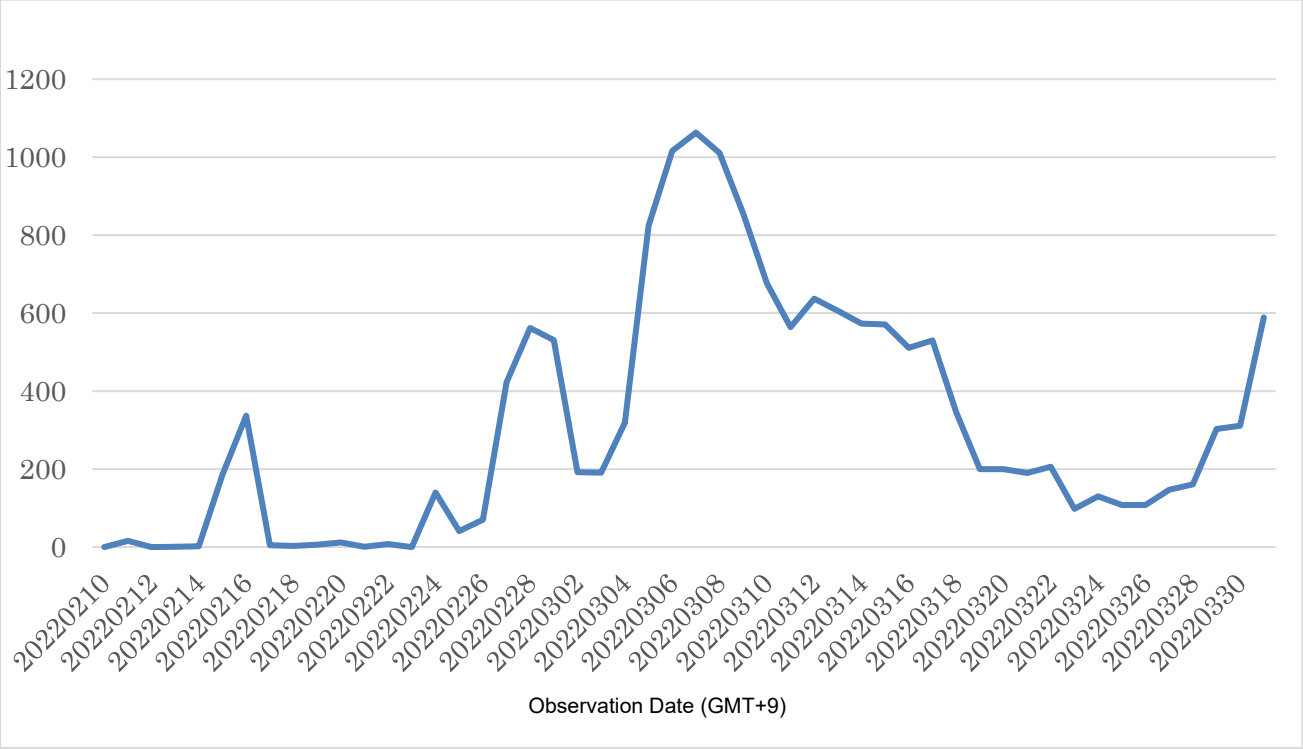
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2022]

In mid-March, sharp rises were seen a number of times in packets originating in the United Kingdom (GB). These packets were sent from RECYBER PROJECT NETBLOCK, causing packets targeted to a large number of ports to be observed during a short period of time. Singapore saw the number of packets go down and changed places with Bulgaria in the rankings.

2. Events of Note

2.1. Increase in the number of backscatter packets originating in Ukraine

Around mid-February, JPCERT/CC started observing TCP packets originating in Ukraine with SYN and ACK flags set, which tend to be seen when subjected to a DDoS attack. [Figure 3]
JPCERT/CC assumes that these were packets returned by attacked servers with SYN and ACK flags set (backscatter packets), in response to packets sent to them with a SYN flag set spoofing TSUBAME, that is, with the IP address of a TSUBAME sensor set as the source address. Such backscatter packets are observed in the case of a SYN flood attack, which is a form of DDoS attack.



[Figure 3: Number of backscatter packets originating in Ukraine]

On February 15, there was information disseminated on social media(2) from Ukraine that the country is under DDoS attack. Among the source addresses of the backscatter packets observed around February 15, IP addresses of nodes used as web servers in Ukraine were identified. The ports targeted by the attack were 80/TCP and 443/TCP.

According to information from domestic and foreign security vendors(3), DDoS attacks are carried out in multiple methods, and we believe that TSUBAME may have observed backscatter packets that were the aftermath of some of these attacks.

Such backscatter packets have been observed continuously since February 15, and we believe that DDoS attacks targeting Ukraine are continuing. Table 3 lists the main targets that we were able to investigate from external data.

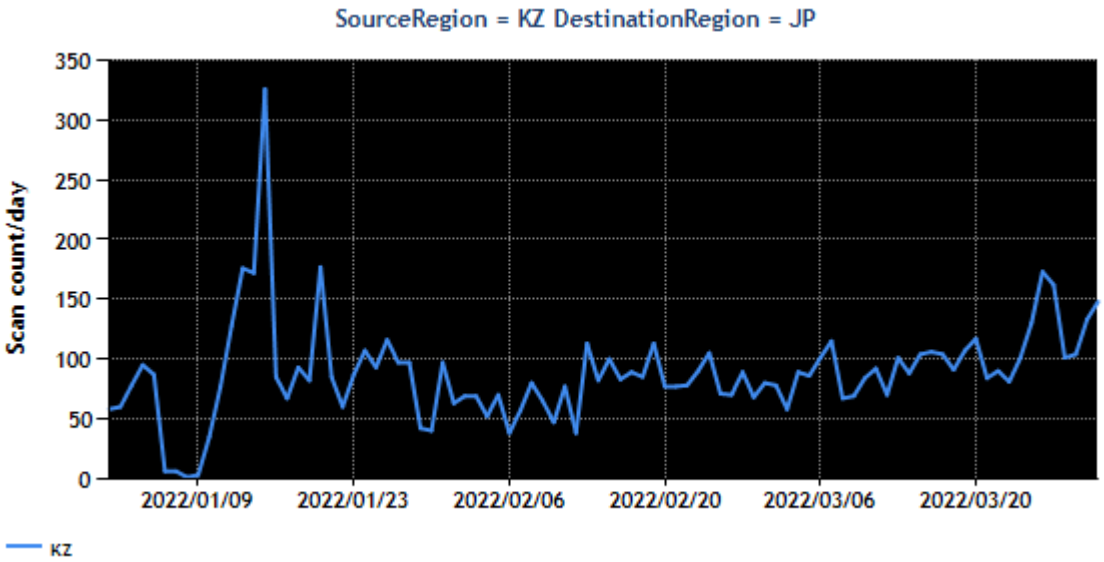
[Chart 3： Organizations that appear to be sending backscatter packets]

Office of the Verkhovna Rada of Ukraine
Office of the President of Ukraine
Ukrainian National Information Agency
State Special Communications Service of Ukraine
PrivatBank
State Savings Bank of Ukraine
TASCOMBANK
Kharkov Metropolitan
Ukrainian Media Holding
Naftogaz Of Ukraine
Companies that provide services and software for financial institutions
News sites
Fixed-line ISPs and mobile carriers
Hosting providers
CDN providers

JPCERT/CC provided Ukraine's CERT-UA with information about observation trends.

2.2. Temporary decline in the number of packets originating in Kazakhstan

Packets captured by TSUBAME's sensors are affected not only by the status of the source but also by changes in the status of the paths that the packets are sent through. In other words, even when there is no significant change in the status of the source, if the transmission path of packets is shut down or becomes unstable, for instance, the number of packets observed will decrease.
From January 5 to 10, 2022, the number of packets observed originating in Kazakhstan (KZ) decreased.[Figure 4]



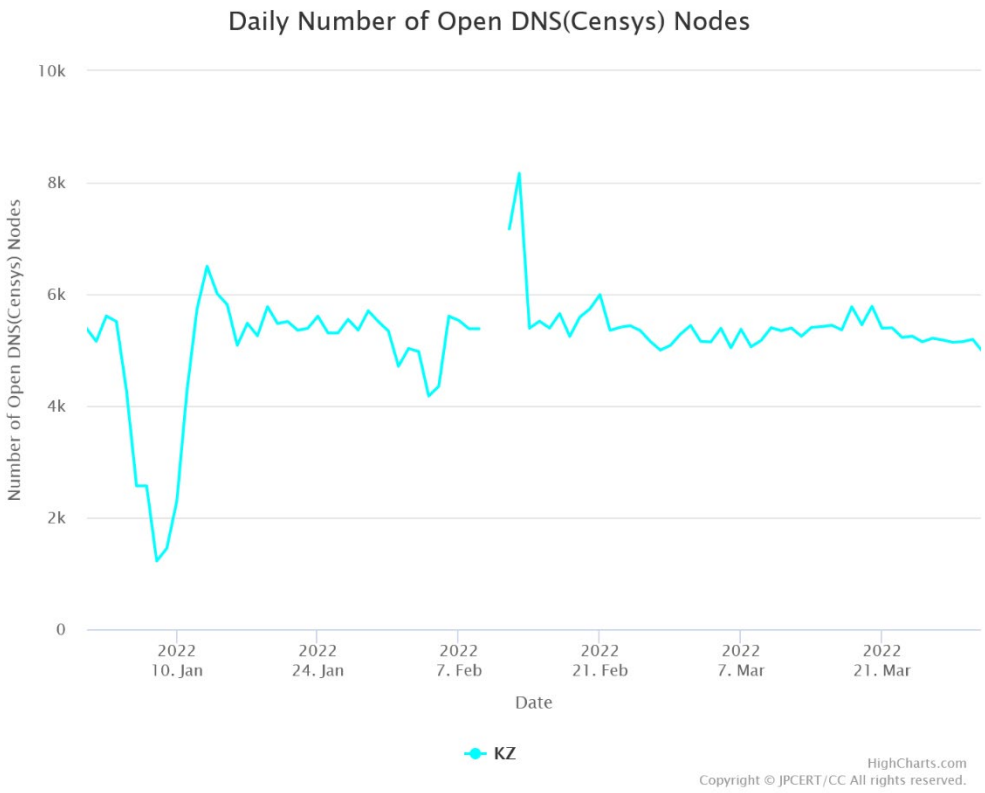
[Figure 4: Number of observed packets originating in Kazakhstan]

In Kazakhstan, it was reported that demonstrations were held to protest the price of liquefied petroleum gas announced on January 1, and that protests subsequently spread across the country.(4) On January 5, the Kazakh president declared a nationwide state of emergency and requested the Collective Security Treaty Organization (CSTO) to send peacekeeping forces.

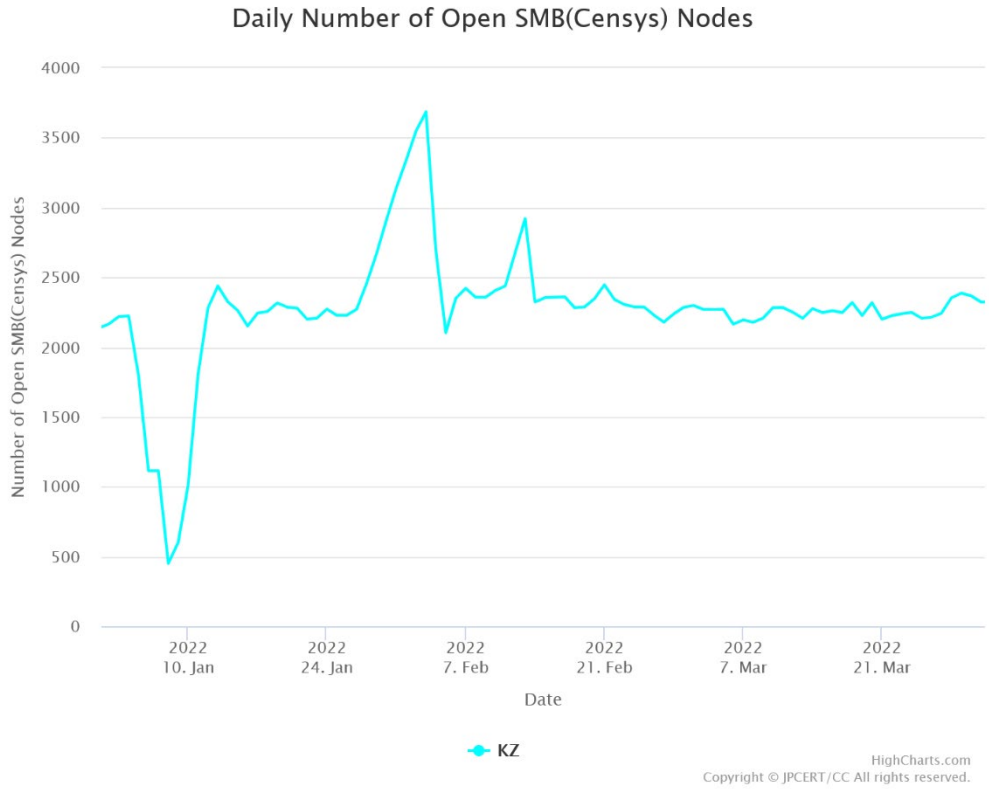
NetBlocks, an NGO that monitors the state of cyber security and Internet governance, presumes that the Internet was shut down across the country from January 5 to January 10.(5)(6)

In Mejiro, a verification test project conducted with the aim of visualizing Internet risks, JPCERT/CC provides information about Internet nodes that are accessible via the Internet as Mejiro indexes.

Mejiro uses data collected by crawlers and aggregated in UTC, and it shows drops in the numbers of open resolvers observed between January 5 and 10. [Figure 5] [Figure 6]



[Figure 5: Number of open resolver nodes in Kazakhstan]



[Figure 6: Number of open SMB nodes in Kazakhstan]

Given the temporary nature of the changes in the observation data of TSUBAME and Mejiro, JPCERT/CC believes the changes were due to the impact of communication restrictions, rather than changes in botnet activities or the status of open resolvers in Kazakhstan.

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)Defence of Ukraine
https://twitter.com/DefenceU/status/1493628291844083723

(3)360 Netlab
https://twitter.com/360Netlab/status/1493797519725367302

(4)Prime Minister Askar Mamin resigns amid protests against fuel prices (Japanese)
https://www.jetro.go.jp/biznews/2022/01/d97c27fec4aaf775.html

(5)NetBlocks
https://twitter.com/netblocks/status/1480713969295933443

(6)Kazakhstan's Internet Shutdown Offers Lessons for Russia-Ukraine Crisis
https://www.nytimes.com/2022/02/18/technology/kazakhstan-internet-russia-ukraine.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 2021.