JPCERT/CC Internet Threat Monitoring Report

January 1, 2023 - March 31, 2023

JPCERT Coordination Center

April 27, 2023

JPCERT CC®

Table of Contents

1. Overview 3

2. Events of Note 6

2.1. Trend in the numbers of packets targeted to port 37215/TCP originating in various regions 6

3. References 11

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.

Data collected through sensors are analyzed, and if any problem is found, JPCERT/CC provides information to relevant parties who can address the problem and asks them to take appropriate steps.

This report will mainly show the analysis results of packets observed by JPCERT/CC's Internet threat monitoring system (TSUBAME) during this quarter.

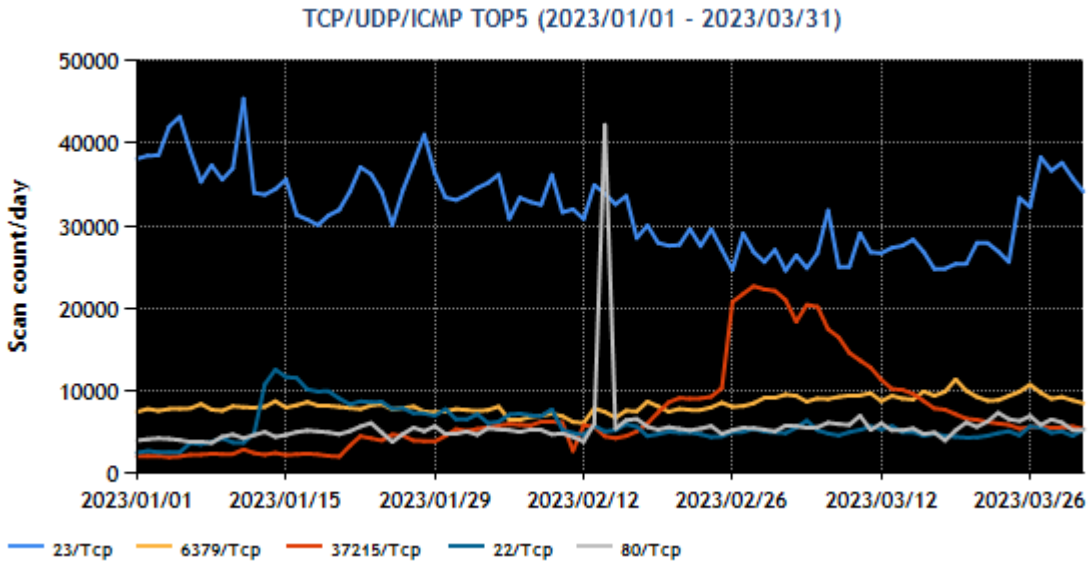
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	6379/TCP (redis)	2
3	37215/TCP	7
4	22/TCP (ssh)	4
5	80/TCP (Microsoft-ds)	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] .



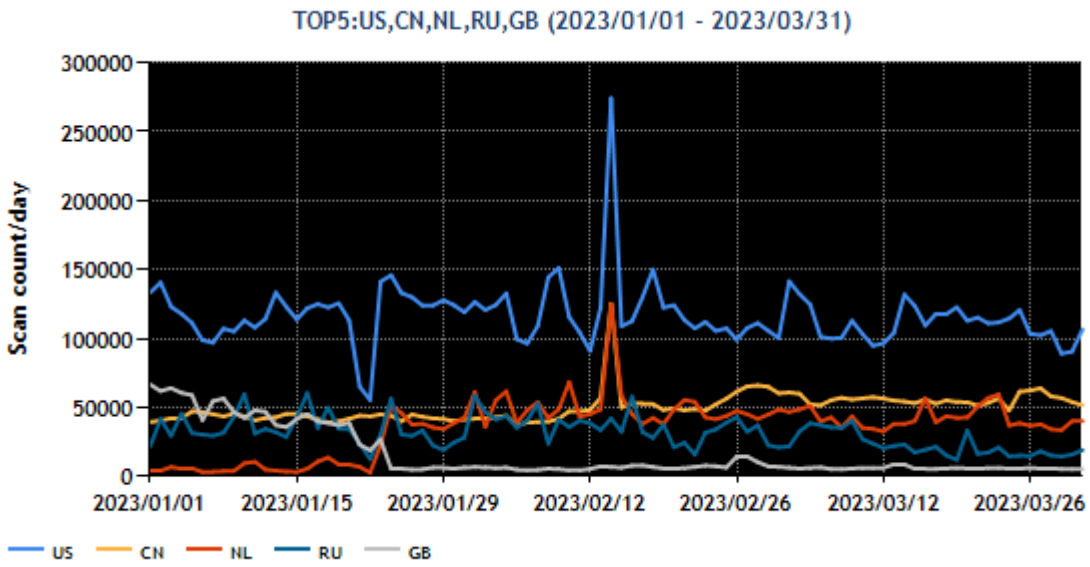
[Figure 1: Number of packets observed at top 5 destination ports from January through March 2023]

Port 23/TCP (telnet) received the greatest number of packets with repeated fluctuations seen during the quarter. Packets targeted to port 6379/TCP continued to increase slightly throughout the quarter. Packets targeted to port 37215/TCP started to edge up from around January 18[(2)], then rose sharply over a period of about 10 days from around February 26, moving up to third in the rankings. Sources of the packets included IP addresses in Japan. This phenomenon will be discussed in "2.1. Trend in the numbers of packets targeted to port 37215/TCP originating in various regions."
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	China	4
3	Netherlands	Not in the top 10
4	Russia	2
5	Great Britain	3

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



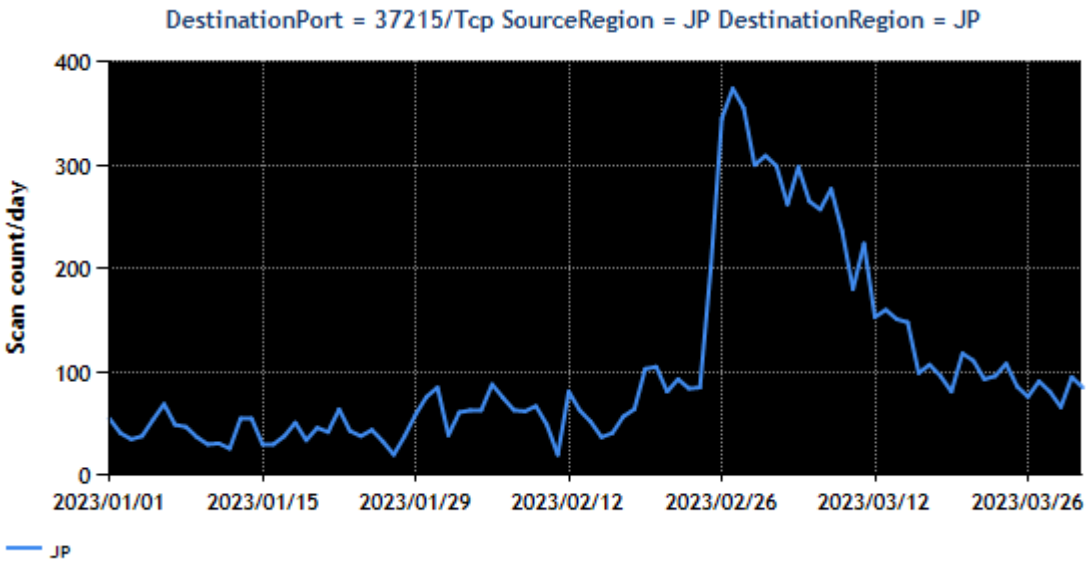
[Figure 2: Number of observed packets of the top 5 source regions from January through March 2023]

The United States remained the top source region throughout the quarter. Packets from China increased gradually, growing about 1.5 times (on a 10-day average) over the quarter. From around January 23, changes were observed in the numbers of packets originating in the United Kingdom and the Netherlands (packets from the Netherlands grew about 8 times on a 10-day average). JPCERT/CC believes this is due to the fact that IP address ranges previously allocated to the United Kingdom were reallocated to the Netherlands. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

2. Events of Note

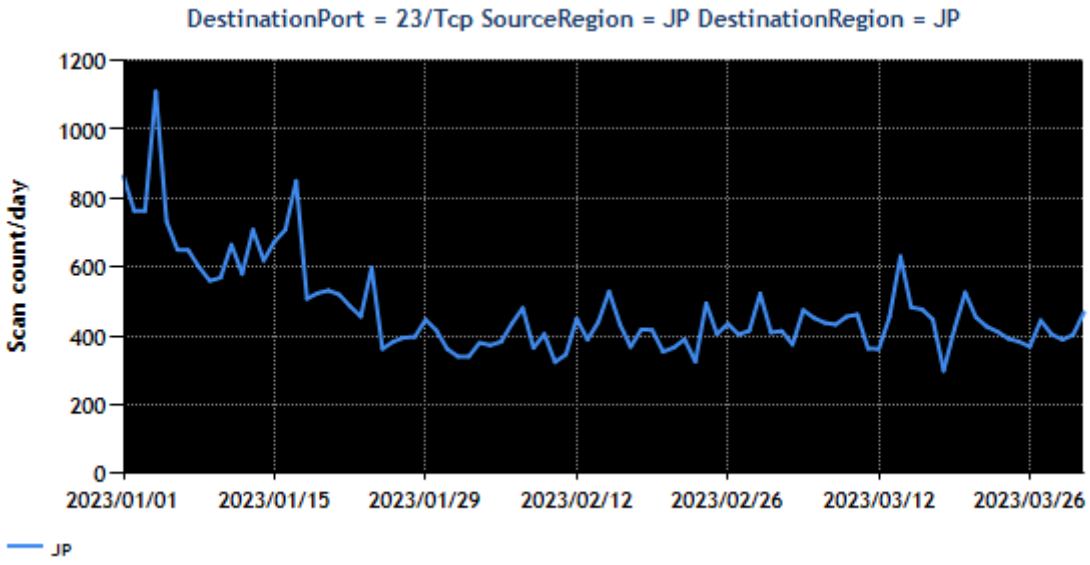
2.1. Trend in the numbers of packets targeted to port 37215/TCP originating in various regions

Packets targeted to port 37215/TCP originating in Japan that have a distinctive characteristic of Mirai (i.e., initial sequence number matches the destination IP address; hereinafter, "Mirai-type packets") increased from around mid-February to mid-March. Following a temporary increase from February 19 to 21[(3)(4)], these packets increased again from around February 25. By February 28, they reached about 6 times the 10-day average until February 18, before the increase, then gradually decreased until around March 18. (Figure 3)



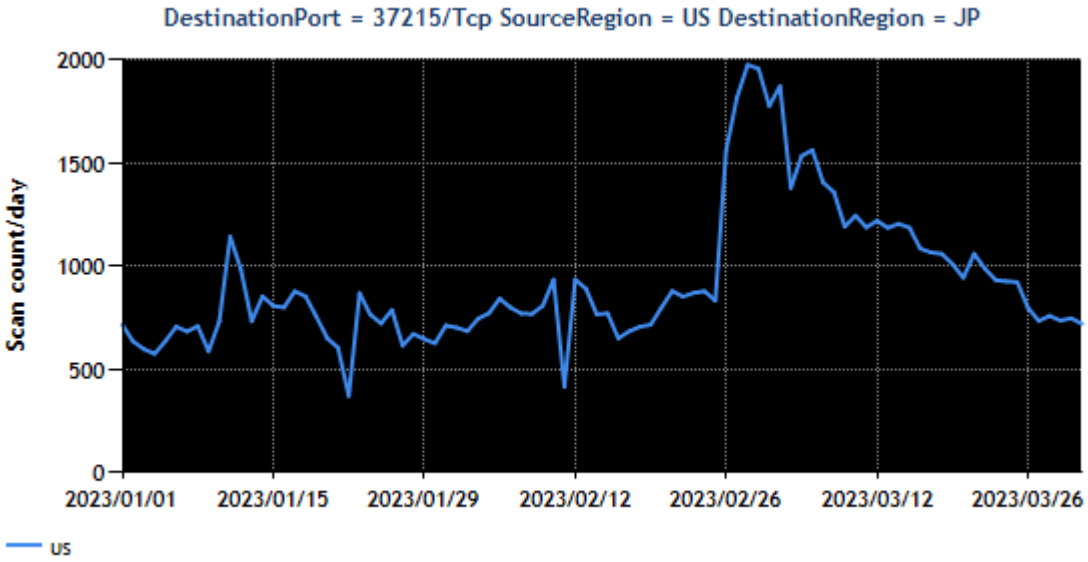
[Figure 3: Packets targeted to port 37215/TCP originating in Japan]

Sources of these packets were also sending packets targeted to port 23/TCP (telnet), not just port 37215/TCP. [Figure 4] shows the trend in the number of packets targeted to port 23/TCP originating in Japan. There is no distinctive patterns corresponding to the changes shown in [Figure 3].

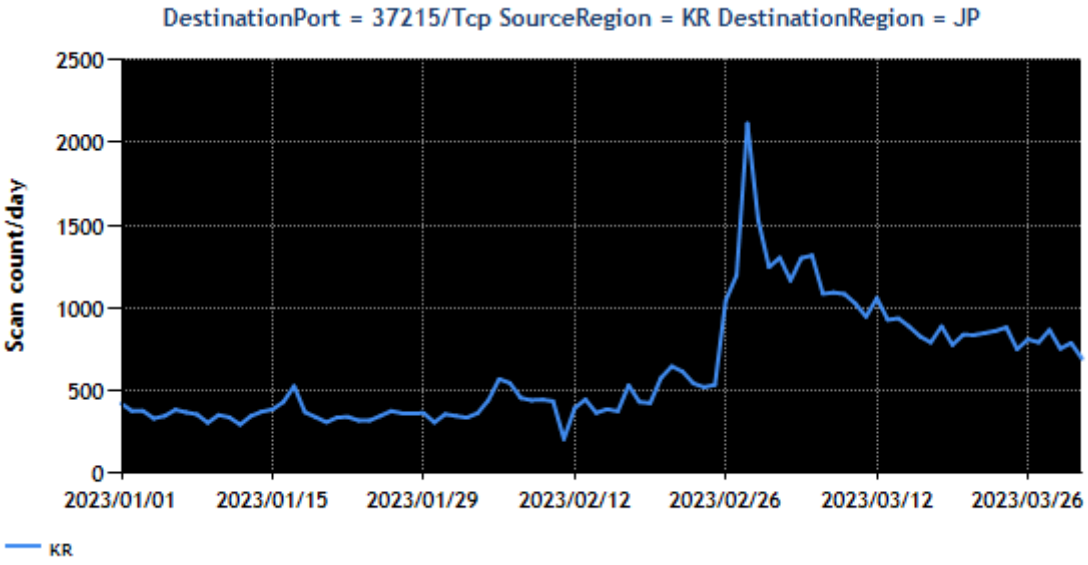


[Figure 4: Packets targeted to port 23/TCP originating in Japan]

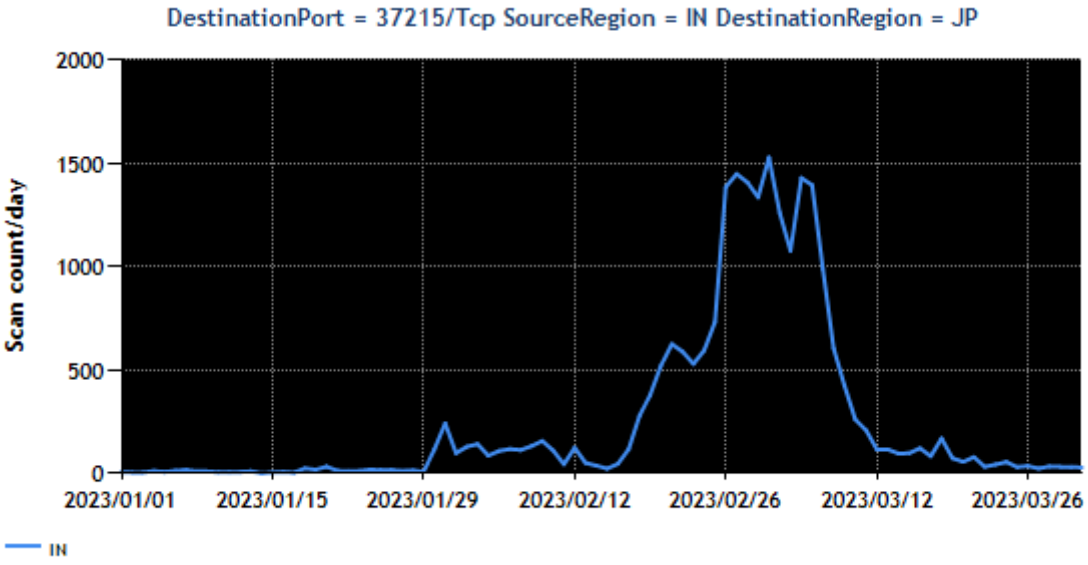
Temporary increases were observed in packets targeted to port 37215/TCP sent from various regions. [Figure 5] through [Figure 11] show the patterns of increase for some of the regions.



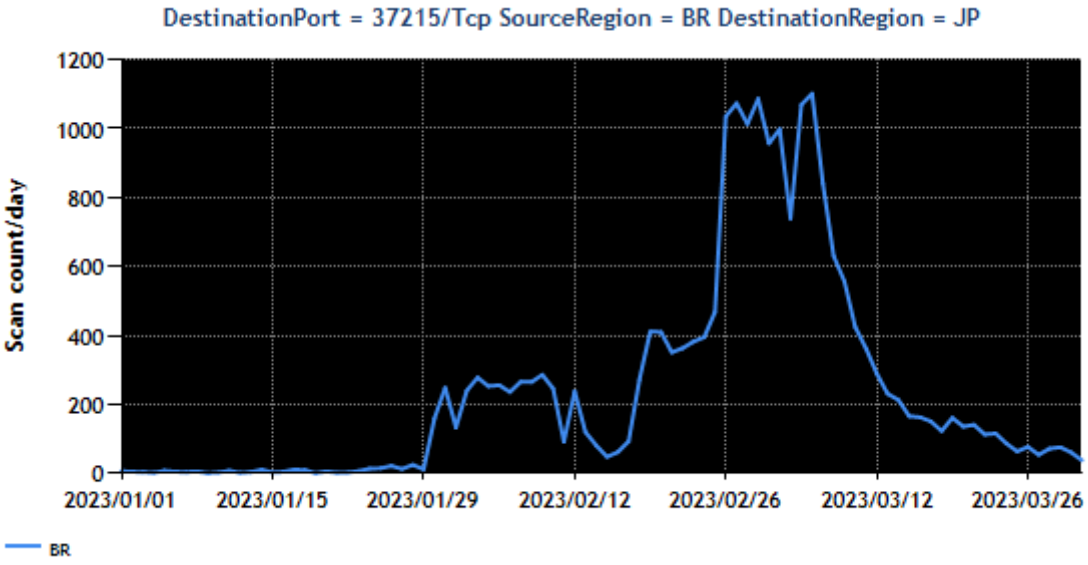
[Figure 5: Packets targeted to port 37215/TCP originating in the United States]



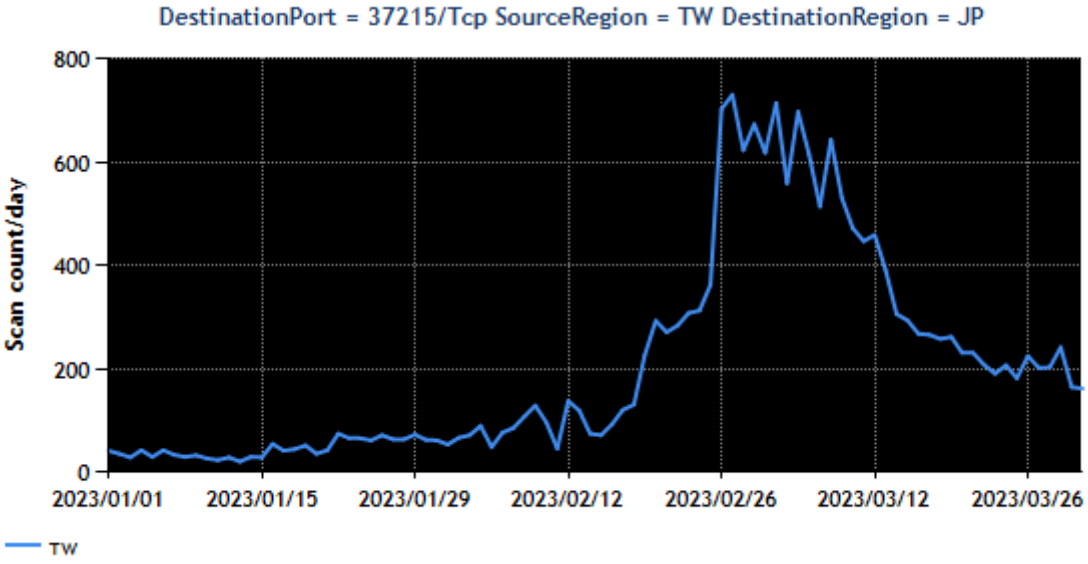
[Figure 6: Packets targeted to port 37215/TCP originating in South Korea]



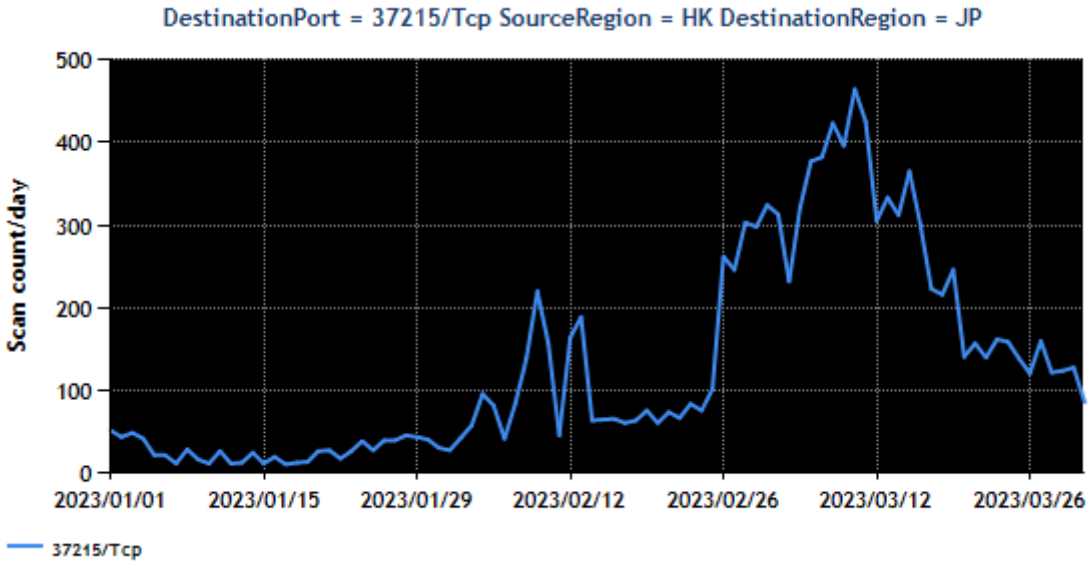
[Figure 7: Packets targeted to port 37215/TCP originating in India]



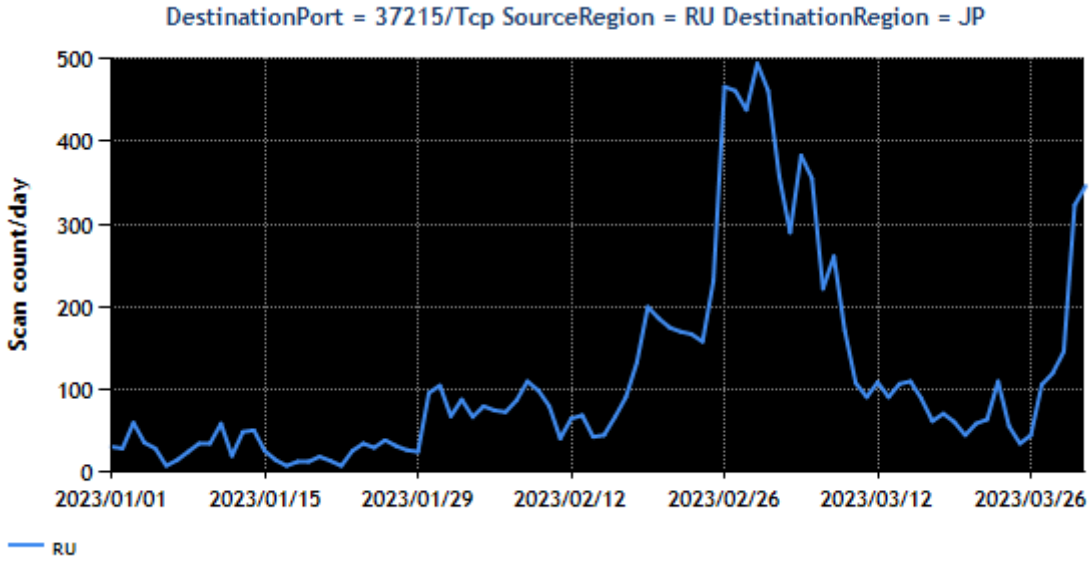
[Figure 8: Packets targeted to port 37215/TCP originating in Brazil]



[Figure 9: Packets targeted to port 37215/TCP originating in Taiwan]



[Figure 10: Packets targeted to port 37215/TCP originating in Hong Kong]



[Figure 11: Packets targeted to port 37215/TCP originating in Russia]

Temporary increases were seen in other regions as well, although their timing varies. The changes in the number of packets targeted to port 37215/TCP shown in [Figure 1] probably reflect these temporary fluctuations.

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) National Institute of Information and Communications Technology (NICT) @nicter_jp
https://twitter.com/nicter_jp/status/1633309683778994181

(3) National Institute of Information and Communications Technology (NICT) @nicter_jp
https://twitter.com/nicter_jp/status/1633310985074397184

(4) National Institute of Information and Communications Technology (NICT)@nicter_jp
https://twitter.com/nicter_jp/status/1645981342499475457

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.