デジタル署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=JPCERT Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2023.03.08 09:39:31 +09'00'

JPCERT/CC Internet Threat Monitoring Report

October 1, 2022 - December 31, 2022

JPCERT Coordination Center
January 31, 2023

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 JPCERT/CC's Internet threat monitoring system (TSUBAME) during this quarter.

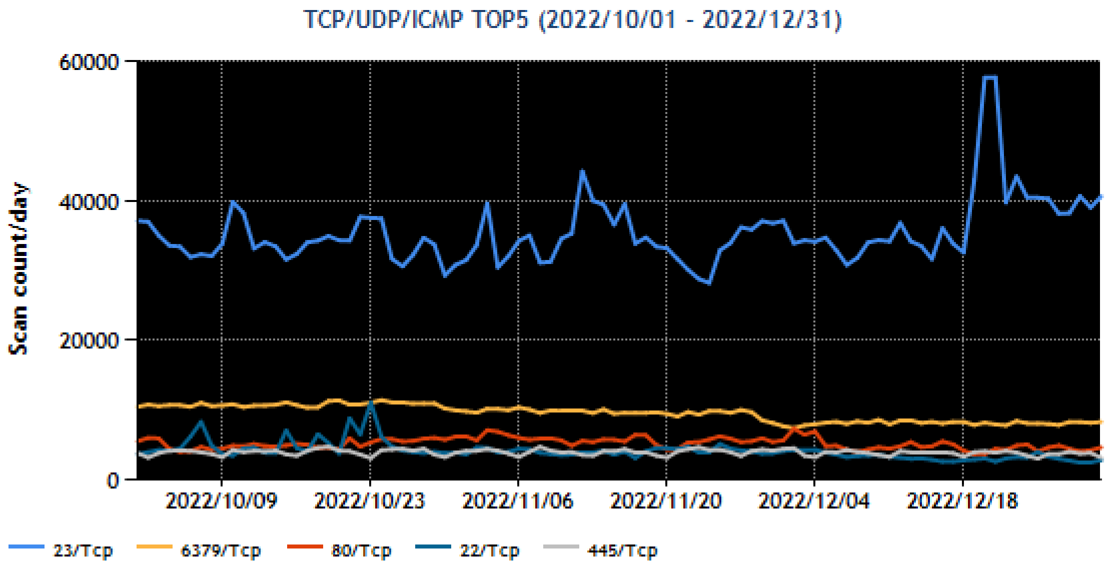
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1: Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	6379/TCP (redis)	2
3	80/TCP (http)	4
4	22/TCP (ssh)	3
5	445/TCP (Microsoft-ds)	6

*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].



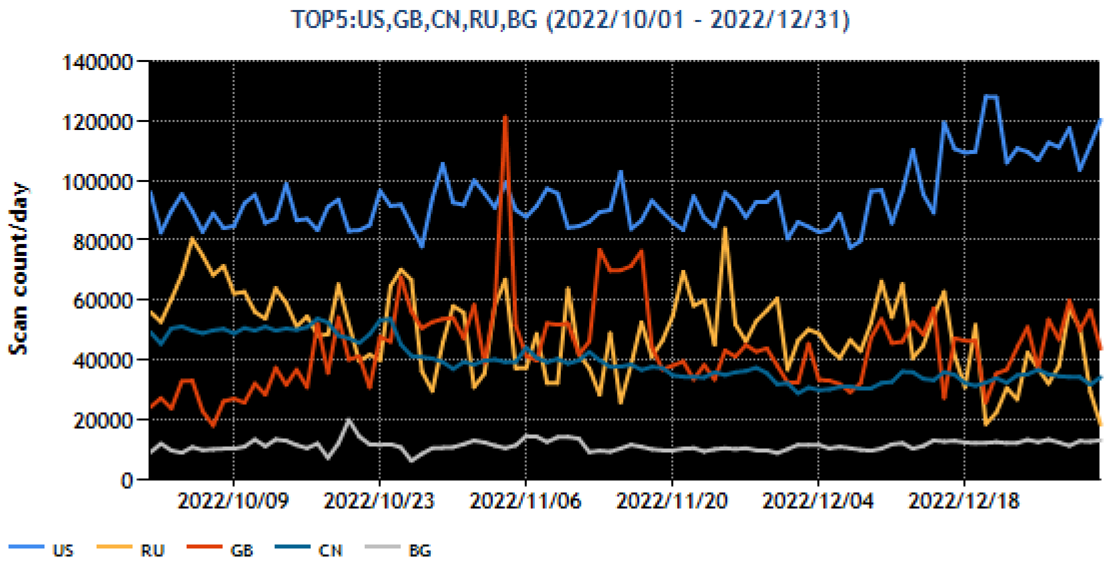
[Figure 1: Number of packets observed at top 5 destination ports from October through December 2022]

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 decrease during this 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	2
3	Great Britain	3
4	China	4
5	Bulgaria	5

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



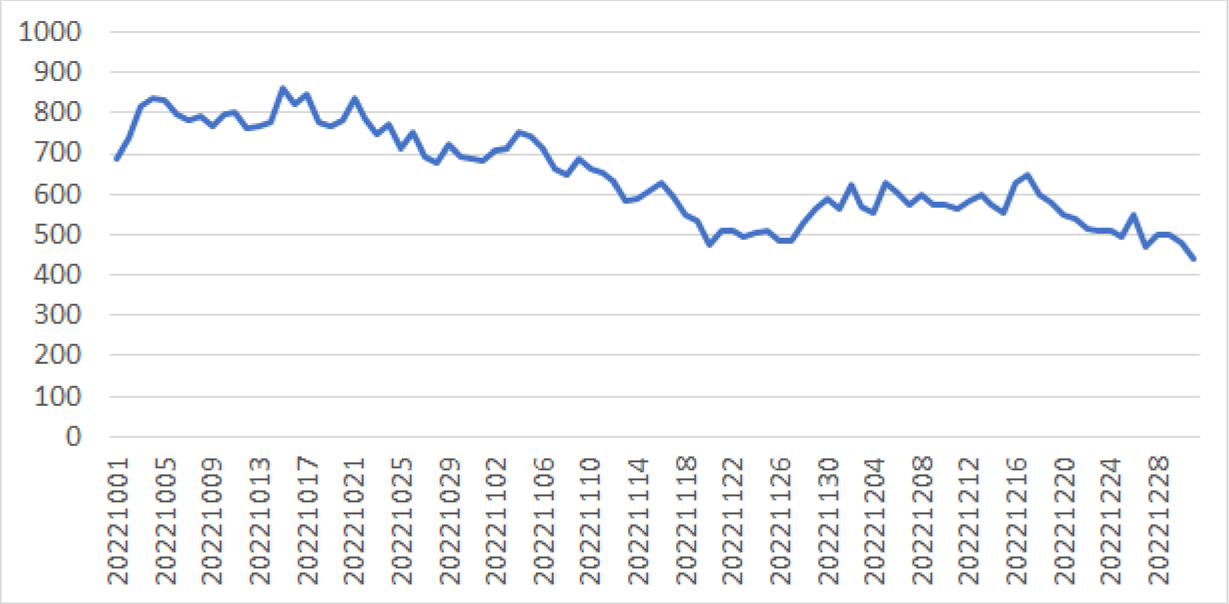
[Figure 2: Number of observed packets of the top 5 source regions from October through December 2022]

While the number of packets originating in the United States increased in December, this was due to the increase in packets targeted to port 81/TCP. Packets from China, fourth in the rankings of source regions, are on a downward trend, falling by approximately 20% (on a 10-day average) over the course of the quarter. As for other regions, while there were sporadic fluctuations in the number of packets, no notable features were seen, and the rankings of source regions were exactly the same as in the previous quarter.

2. Events of Note

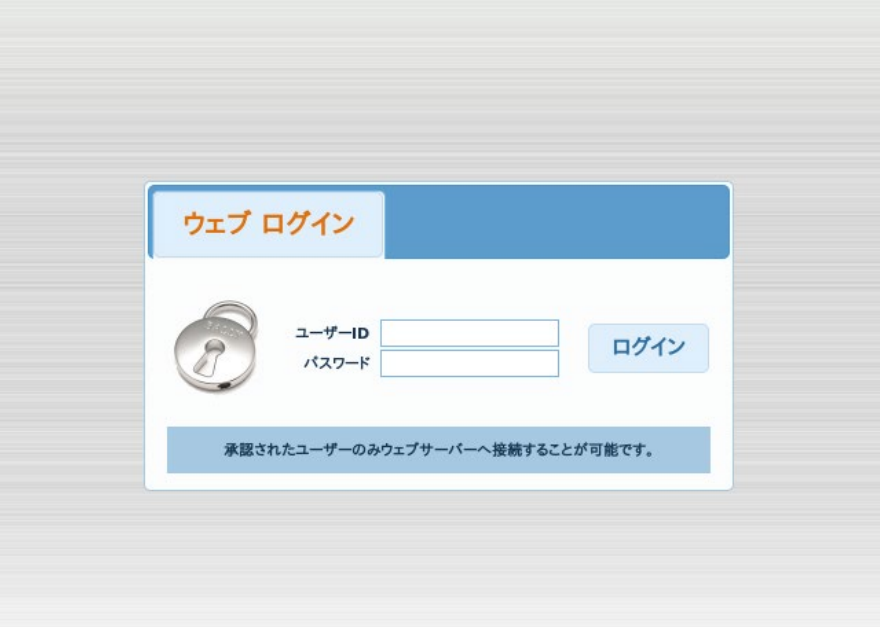
2.1. Trend in the number of packets with a distinctive characteristic of Mirai apparently sent from IoT devices in Japan

Throughout the quarter, packets with a distinctive characteristic of Mirai (i.e., initial sequence number = destination IP address) ("Mirai-type packets") were seen from IP addresses in Japan.[Figure 3]



[Figure 3: Number of observed packets of the top 5 source regions from October through December 2022]

JPCERT/CC examined the characteristics of the source nodes of some of the source IP addresses of these packets using SHODAN. At about 50% of the IP addresses, digital video recorders (DVR), broadband routers, and similar devices were used, and some of the products were models whose vulnerability information was already published. For example, one device displays the login screen shown in [Figure 4].



承認されたユーザーのみウェブサーバーへ接続することが可能です。

[Figure 4: Login screen of DVR product]

The product with this login screen appears to be a DVR manufactured by Focus H&S. Attack activities targeting this product's vulnerabilities to cause malware infection are discussed in NICT's blog article. (2)
Since characteristic Mirai-type packets, such as packets targeted to port 23/TCP or 37215/TCP, are captured by sensors, it is assumed that there are devices infected with Mirai variant malware and conducting scans and attack activities. In Japan, UNIMO Technology, one of the distributors, sells the product, and fixed firmware is available from the company. Please take appropriate steps such as updating the firmware. (3)
Also, please check the status of information, such as whether the Web administration interface is not published on the Internet, whether the initial password has been changed, and whether any security information has been released on the manufacturer's website.

This quarter, suspicious packets were also observed from IP addresses where products that appear to be a Logitec router discussed in the past or Pinetron DVR are installed.
Whenever suspicious packets are observed, JPCERT/CC provides log data to the relevant network administrators. When contacted by an organization that owns relevant IP addresses, please check the status of the devices.

3. References

(1) IANA（Internet Assigned Numbers Authority）
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 Blog
Observation of Attacks Aimed at Infecting DVR Devices (Japanese Only)
https://blog.nicter.jp/2022/10/analysis-of-ddos-bot-targeting-dvrs/

(3) JVN (Japan Vulnerability Notes)
UNIMO Technology digital video recorders vulnerable to missing authentication for critical functions
https://jvn.jp/en/vu/JVNVU90821877/

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.

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). For the latest information, please refer to JPCERT/CC's.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/english/tsubame/

Company names and product names contained in this document are the trademarks or registered trademarks of the respective companies.