JPCERT Coordination Center

JPCERT/CC Internet Threat Monitoring Report

October 1, 2023 - December 31, 2023

JPCERT Coordination Center

February 15, 2024

JPCERT CC®

Table of Contents

1. Overview

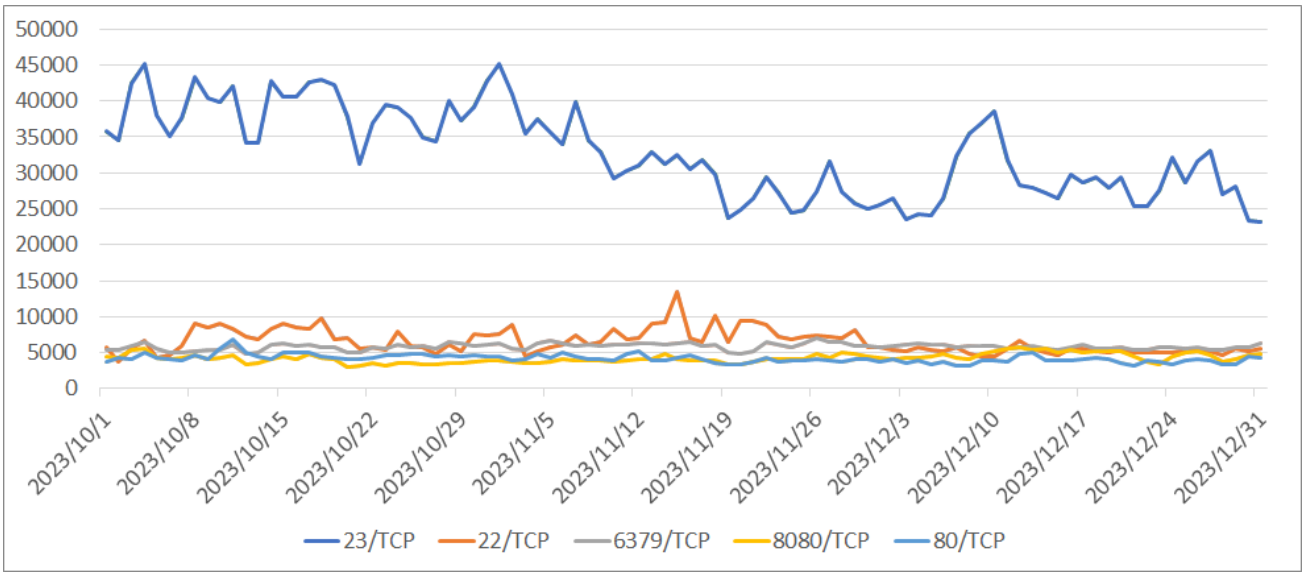
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that are observed by the sensors, and 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 parties who may be able to solve the problem and asks them to take appropriate steps.
This report will provide an overview of the results of monitoring activities by JPCERT/CC's Internet threat monitoring system (TSUBAME) during this quarter and their analysis.
The top 5 services scanned in Japan during this quarter are shown in [Table 1].

[Table 1: Top 5 services frequently scanned in Japan]

Rank	Destination Port Numbers	Previous Quarter
1	telnet (23/TCP)	1
2	ssh (22/TCP)	2
3	redis (6379/TCP)	5
4	http-alt (8080/TCP)	3
5	http (80/TCP)	10

*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 numbers of packets observed for the top 5 services scanned listed in [Table 1] are shown in [Figure 1].



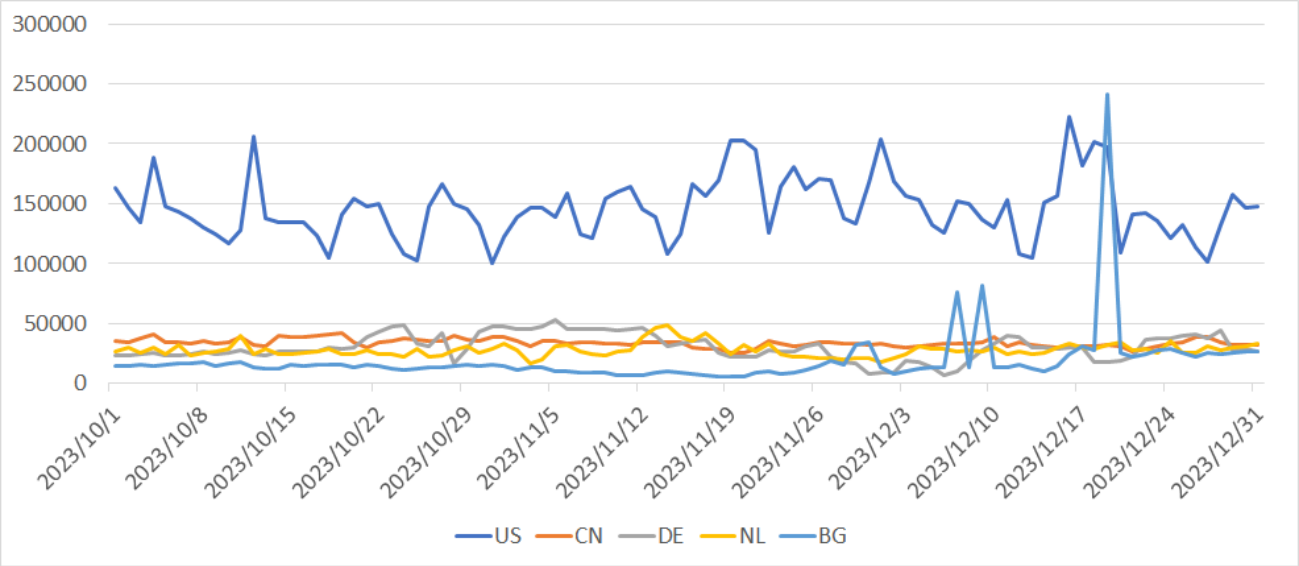
[Figure 1: Number of packets observed at top 5 destination ports from October through December 2023]

The service most frequently scanned this quarter was telnet (23/TCP). The frequency of scans increased for ssh (22/TCP) between October 8 and the end of November, and it moved up to second place in the ranking, replacing redis (6379/TCP). Around late November, http-alt (8080/TCP) and http (80/TCP) changed places in the ranking of scan frequency, with http-alt being constantly scanned more often than http. Next, the top 5 source regions where scanning activities targeting Japan were seen most frequently during this quarter are shown in [Table 2].

[Table 2: Top 5 source regions]

Rank	Source Regions	Previous Quarter
1	USA	1
2	China	4
3	Germany	6
4	Netherlands	2
5	Bulgaria	3

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

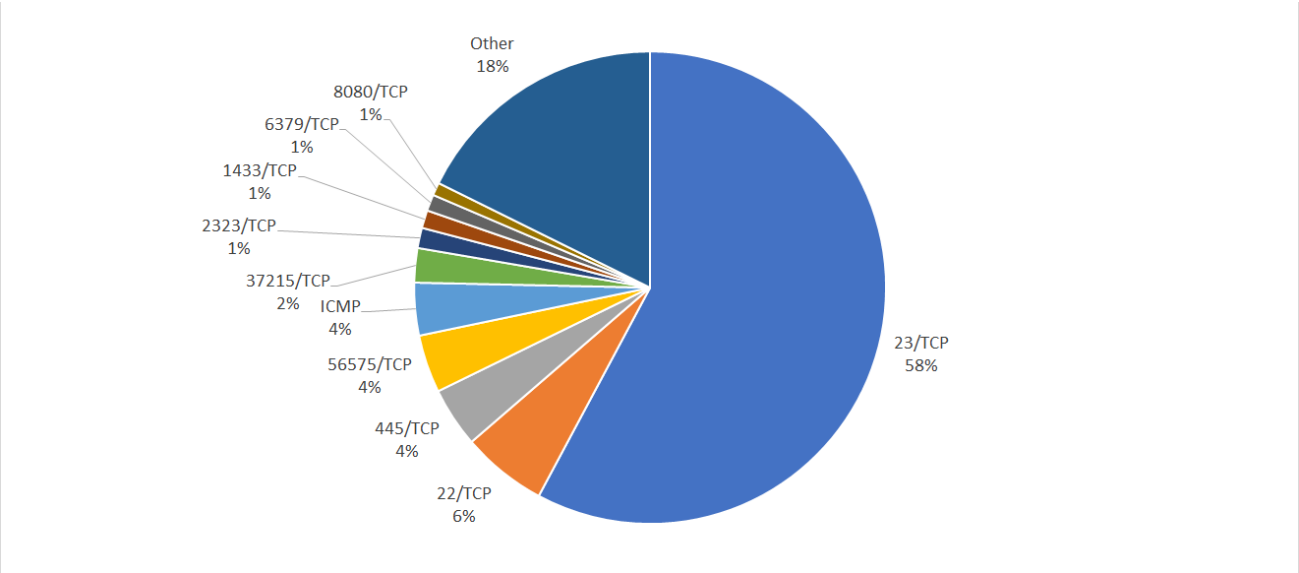


[Figure 2: Number of observed packets of the top 5 source regions from October through December 2023]

While the rankings of the USA and China remained unchanged, Germany took third place after seeing a rise in scanning activities between mid-October and mid-November. As for other regions, there was nothing in particular to note. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

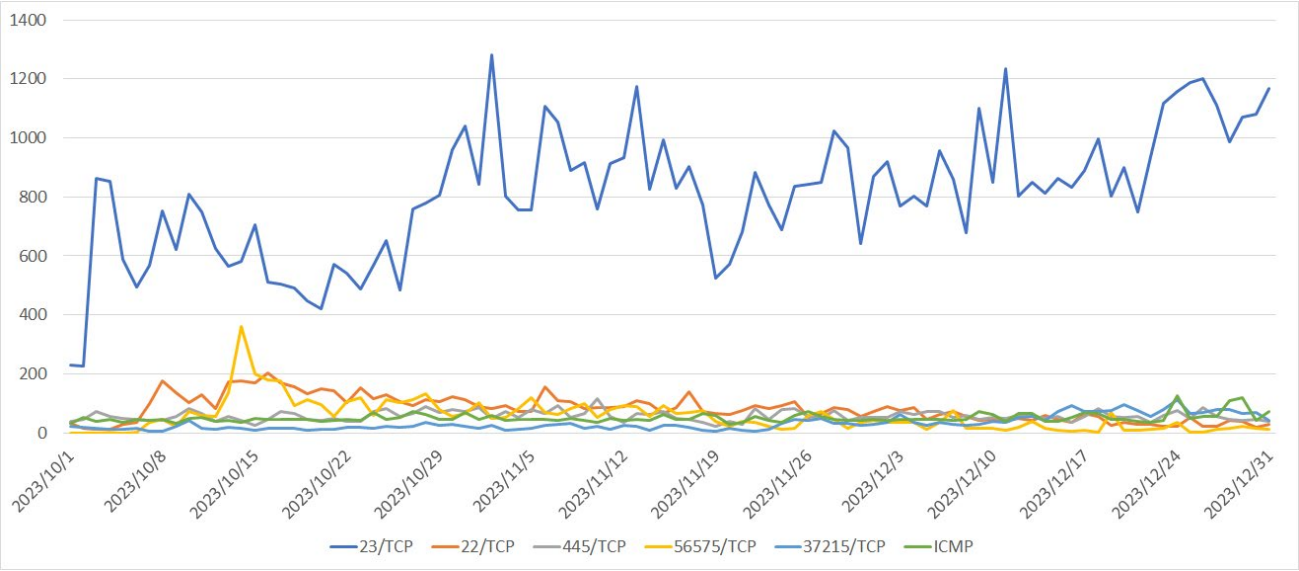
2. Observation of scan packets originating in Japan

This chapter will discuss trends in Japan that were not touched on in the overview. The percentages of services scanned from sources in Japan during this quarter are shown in [Figure 3].



[Figure 3: Percentages of services scanned from sources in Japan between October and December 2023]

Telnet rose in scan frequency, accounting for roughly 60%. It was followed by ssh in second place. Although first and second places mirrored the rankings for scans originating overseas, as shown in Table 1, the rest differed, with Microsoft-ds (445/TCP), 56575/TCP, and 37215/TCP taking third, fourth, and fifth places, respectively. Trends for the top 5 destination ports are shown in [Figure 4].



[Figure 4: Number of packets originating in Japan and observed at top 5 destination ports from October through December 2023]

Telnet (23/TCP) was not scanned at a constant rate throughout the quarter. Its scan frequency in late December was nearly triple the rate in early October. It turned out that some of the scans originated from devices such as NAS, wireless LAN routers, and digital video recorders. On the other hand, those whose sources could not be identified are presumed to be devices with closed ports (i.e., http, https, and other ports) , or devices that could not be tracked as they restarted due to overload caused by malware or other reasons and therefore had a different IP address at the time of investigation.
Meanwhile, scans targeting 56575/TCP started increasing in frequency from around October 7. Since sources that scan 56575/TCP often scan 22/TCP as well, the graphs for these two ports in [Figure 4] show similar changes. JPCERT/CC checked the page that is displayed when the source devices are accessed with a web browser and confirmed that most digital video recorders were sending these scan packets. It is assumed that these digital video recorders were hacked via the Internet and, as a result, have some kind of malware embedded and operating on them.

3. Request from JPCERT/CC

JPCERT/CC may contact users of IP addresses sending suspicious packets and ask them to take certain action via Internet service providers. If you ever receive such requests, we hope you understand the purpose of our investigation activities and, if possible, provide information such as products used, firmware versions, and any evidence of intrusion. There are a number of unknown scanning activities, including those discussed in this report. Your information may offer valuable insights leading to clarification.

4. 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 2023.