JPCERT/CC Internet Threat Monitoring Report

July 1, 2023 - September 30, 2023

JPCERT Coordination Center

October 31, 2023

JPCERT CC®

Table of Contents

1. Overview

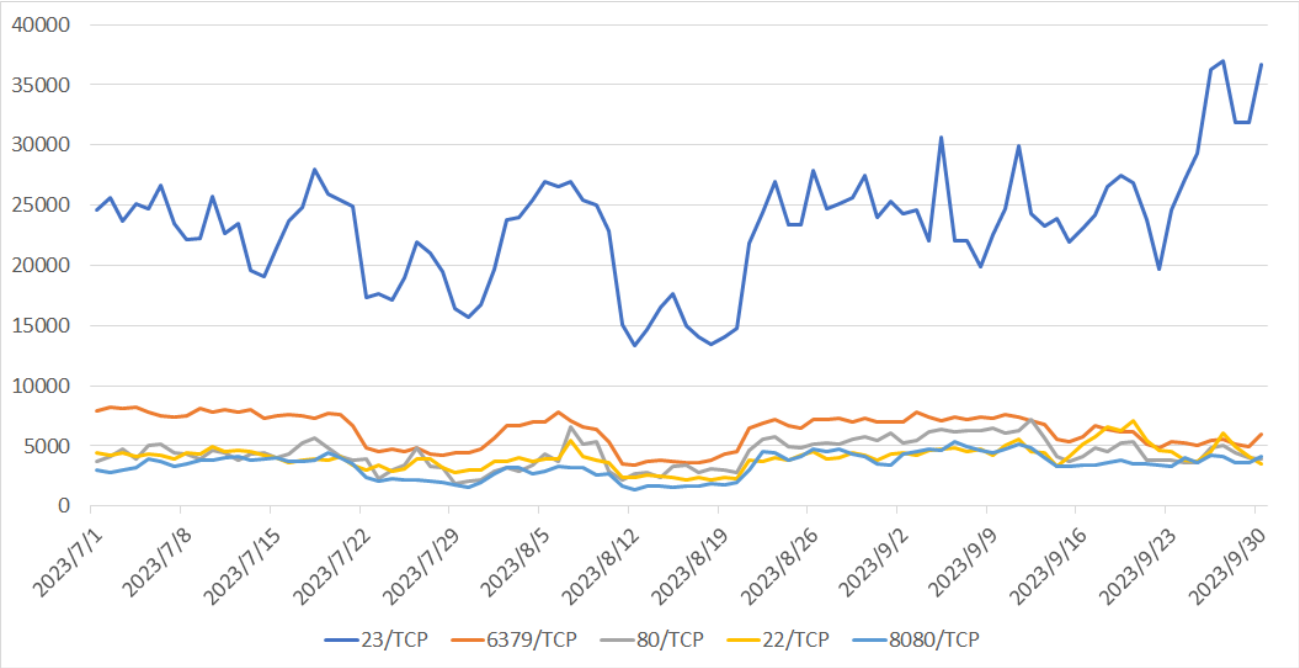
JPCERT/CC has placed multiple monitoring sensors across the Internet to monitor packets that are transmitted exhaustively to certain IP address ranges. It can be assumed that these packets are intended to scan for certain devices or service functions. Also, JPCERT/CC continuously gathers packets that 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	redis (6379/TCP)	2
3	http (80/TCP)	5
4	ssh (22/TCP)	3
5	http-alt (8080/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].



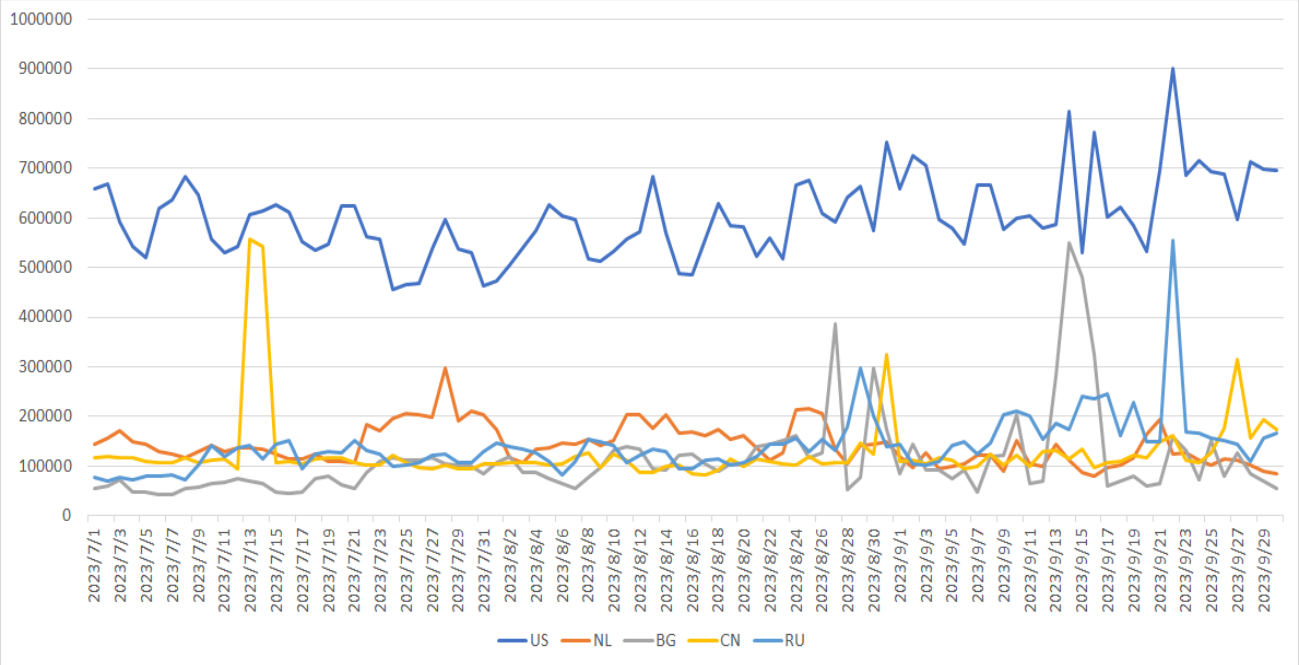
[Figure 1: Number of packets observed at top 5 destination ports from July through September 2023]

The service most frequently scanned this quarter was telnet (23/TCP), followed by redis (6379/TCP). During this quarter, the frequency of scans remained constantly high for http (80/TCP), overtaking ssh (22/TCP) in the ranking. 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	Netherlands	3
3	Bulgaria	4
4	China	2
5	Russia	5

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



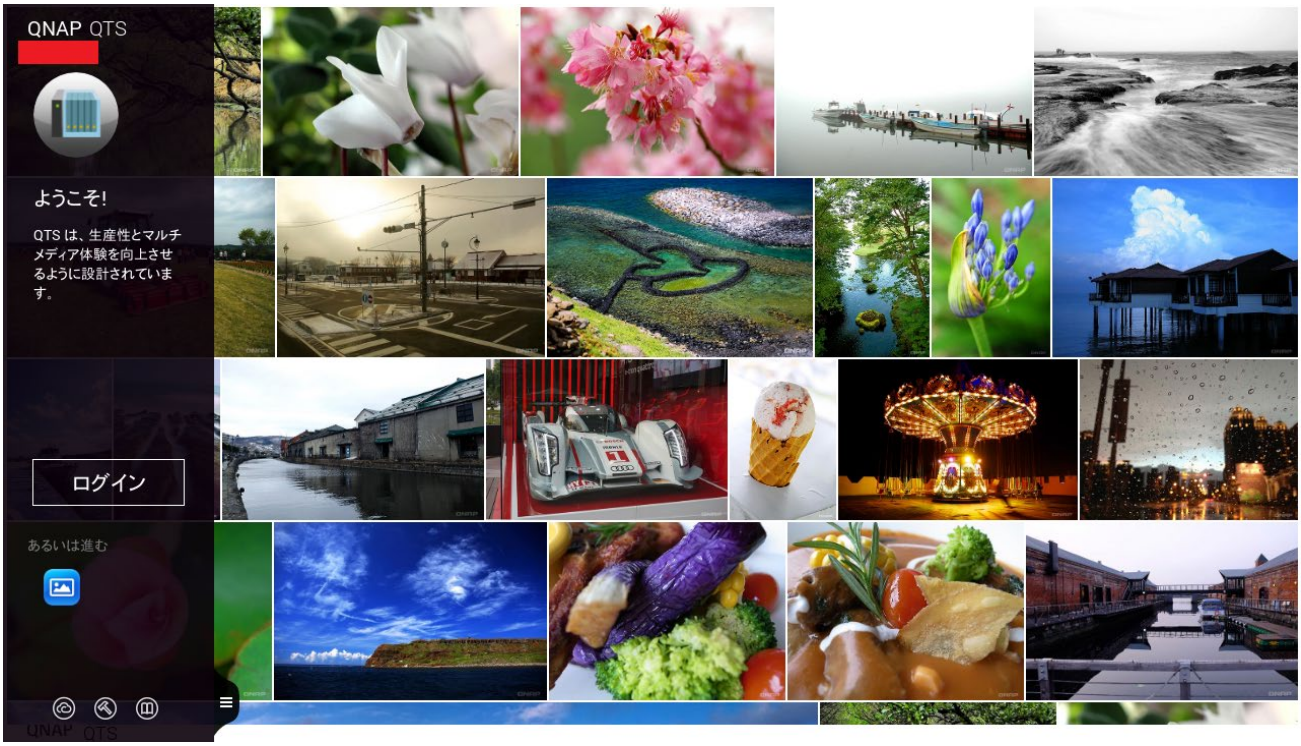
[Figure 2: Number of observed packets of the top 5 source regions from July through September 2023]

Packets originating in Bulgaria temporarily increased from September 8 to 11, and from September 13 to 16. In other regions, no changes were seen from the previous quarter. TSUBAME uses Regional Internet Registry (RIR) allocation data to determine the region of each IP address.

2. Suspicious packets observed from NAS, wireless LAN routers, and other devices made in Taiwan

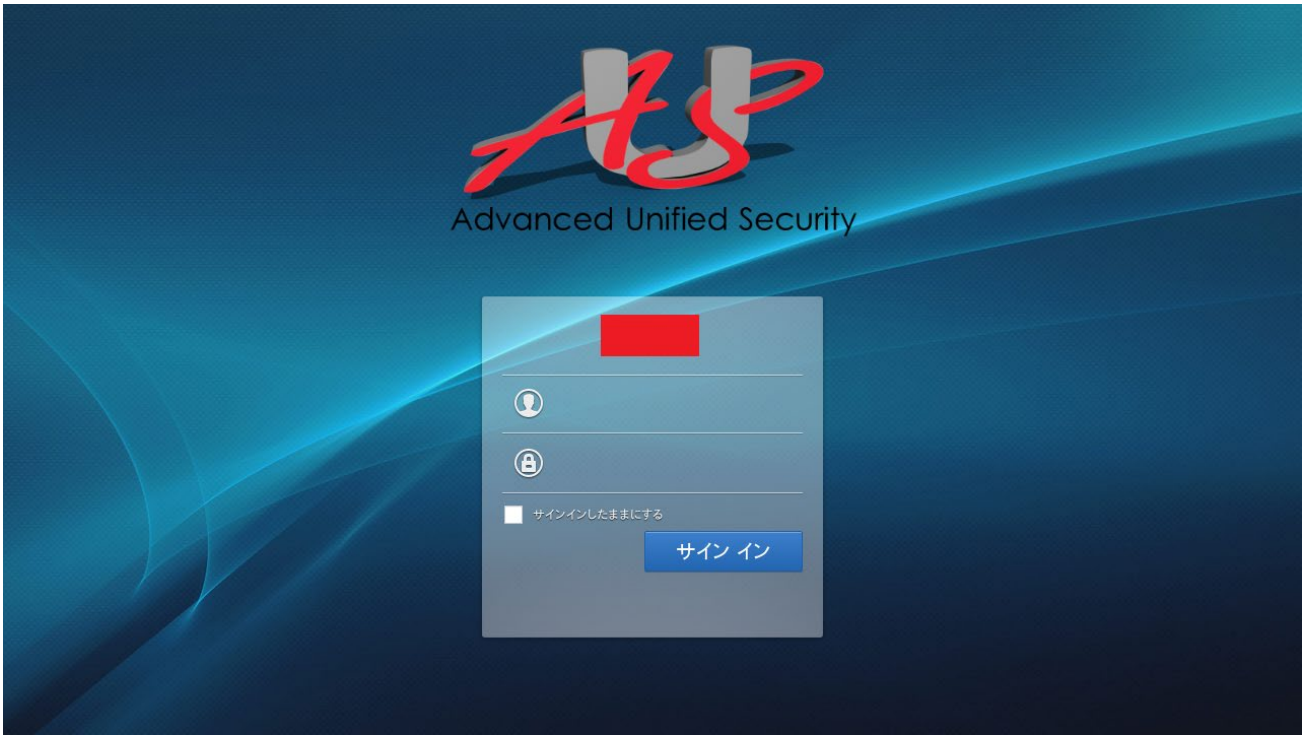
While most scanning activities originating from devices including NAS, wireless LAN routers, and digital video recorders have characteristics suggesting an association with Mirai's infection campaign, a small number of scanning activities without such characteristics have also been observed. The former type of activities will be referred to as Mirai-type scans, and the latter type non-Mirai-type scans. The following analysis focuses on non-Mirai-type scans. Both types of scans widely differed in the services they scanned. Non-Mirai-type scans targeted a wide range of services including ftp, http, https, mongodb, ms-sql-s, pptp, sip, ssc-agent, and imap, as well as ports that are not well-known.

It was hard to identify the products these scans were trying to find based on the targeted services. Therefore, JPCERT/CC sought to identify the source devices based on information found on Shodan.io and elsewhere, and found that the scans originated from NAS, wireless LAN routers, and other devices from manufacturers in Taiwan. In addition, JPCERT/CC was able to confirm that these devices had a number of ports opened to the Internet or had outdated firmware. Assuming that these devices were hacked remotely and have some kind of malware operating on them, JPCERT/CC is conducting further investigations. [Figures 3-1 to 9] show samples of pages that are displayed when the source devices are accessed with a web browser.



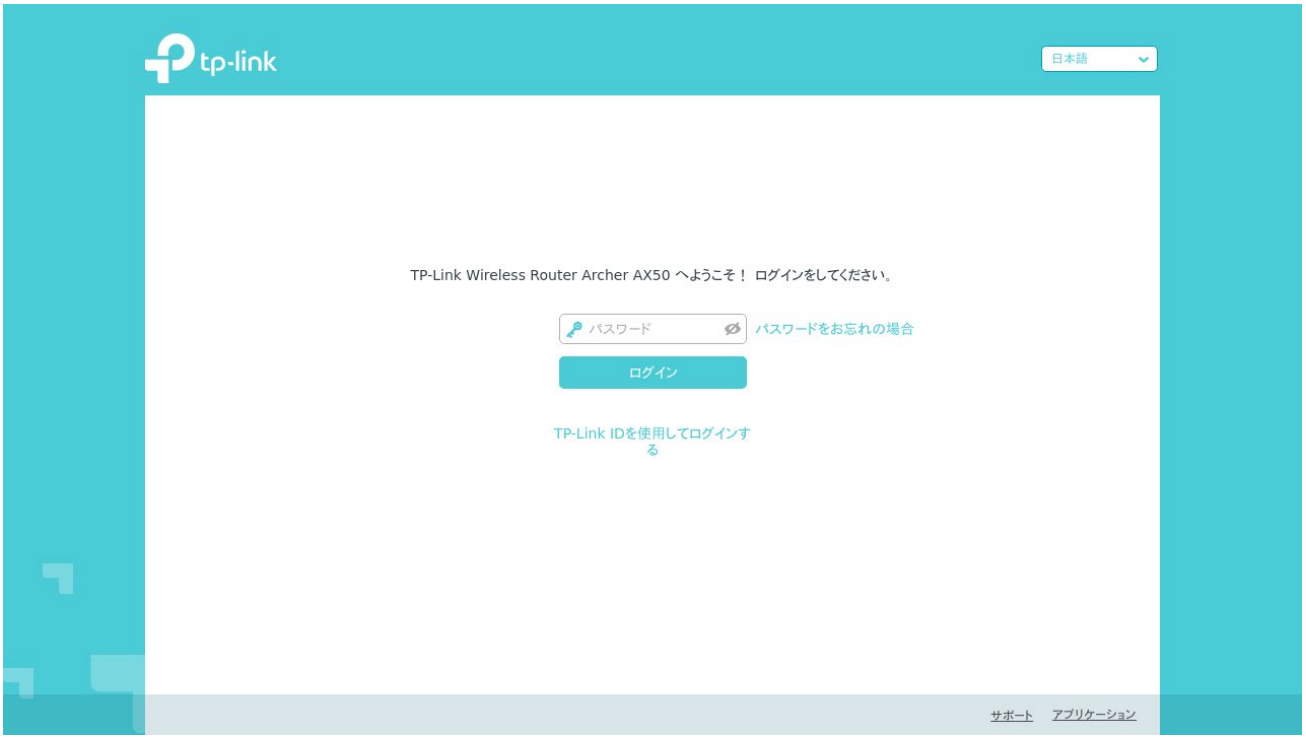
[Figure 3-1: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (1)]

[Figure 4-2: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (2)]

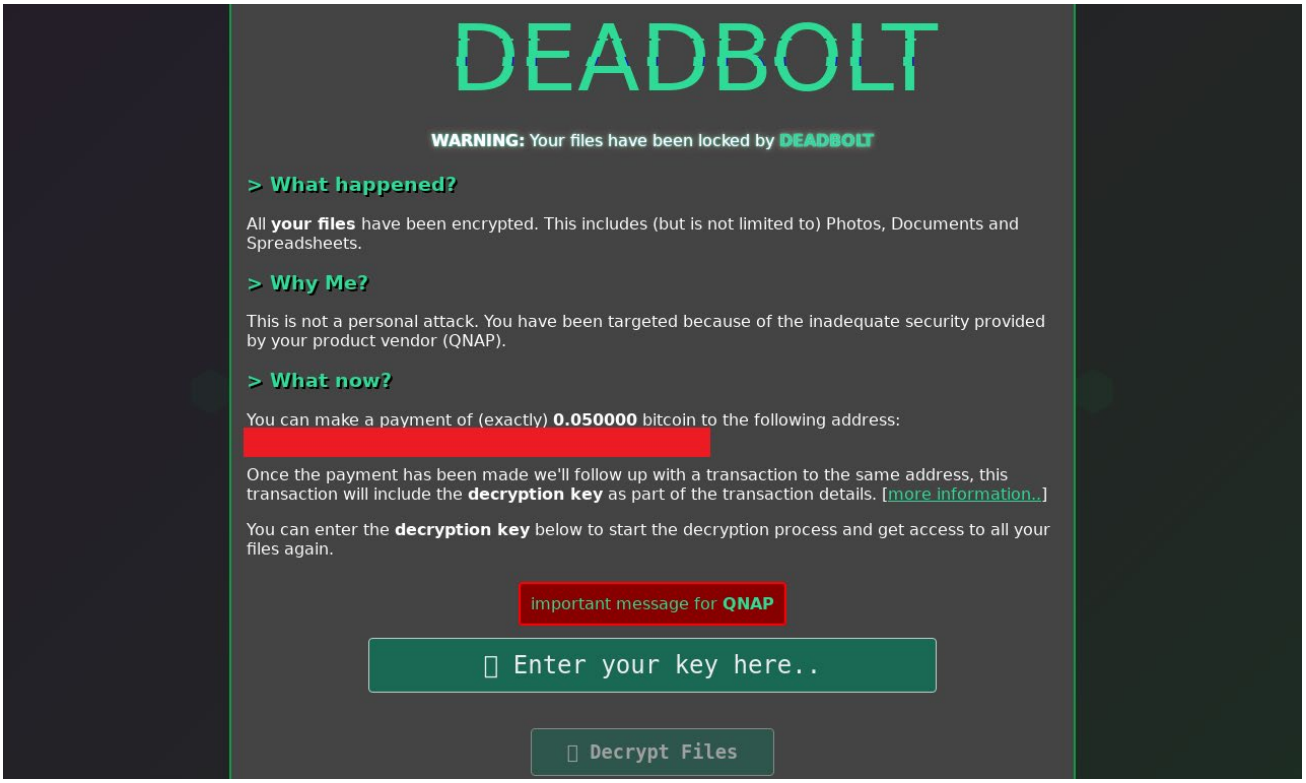


[Figure 5-3: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (3)]

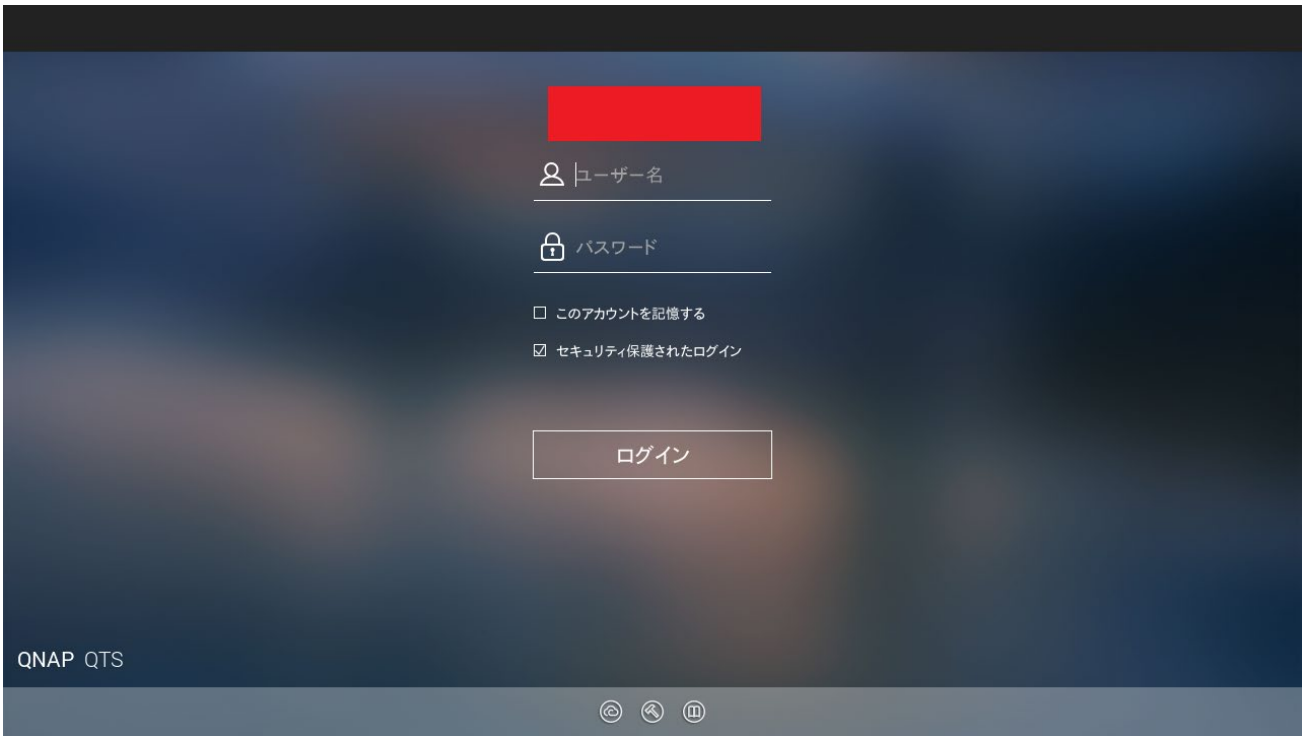
[Figure 6-4: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (4)]



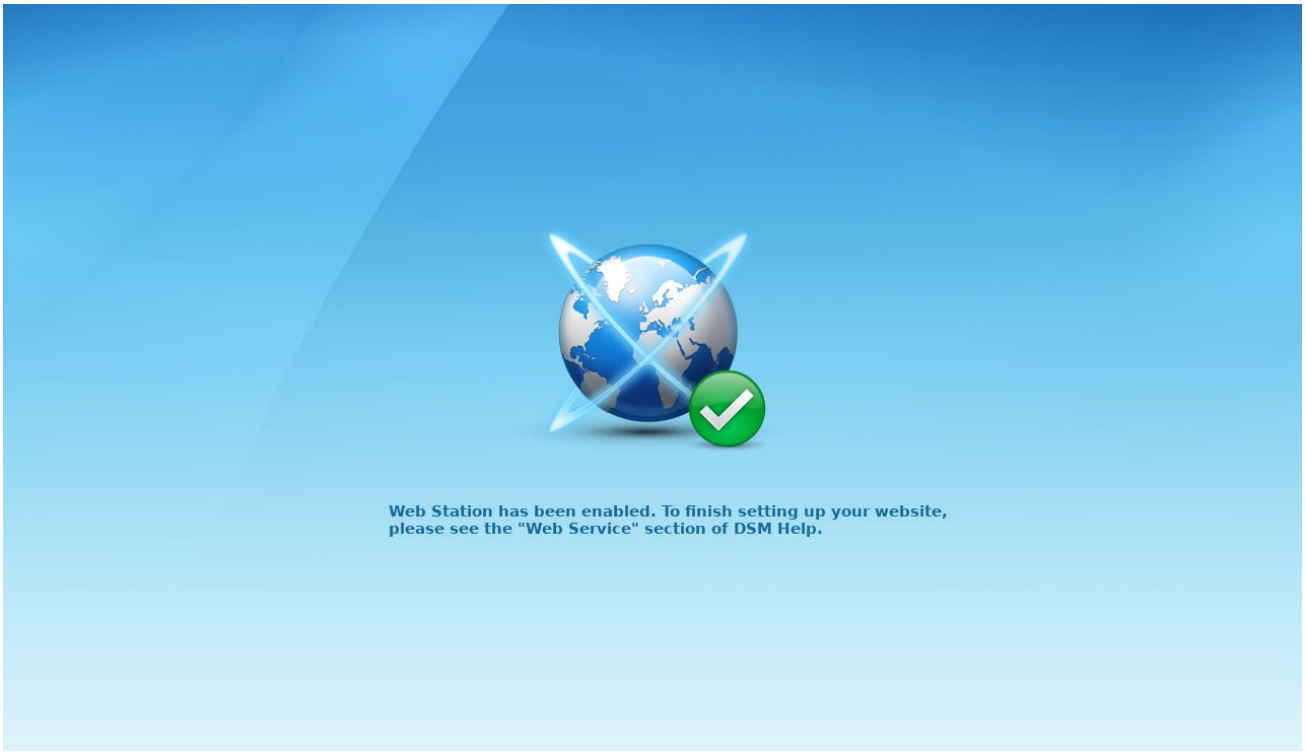
[Figure 7-5: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (5)]



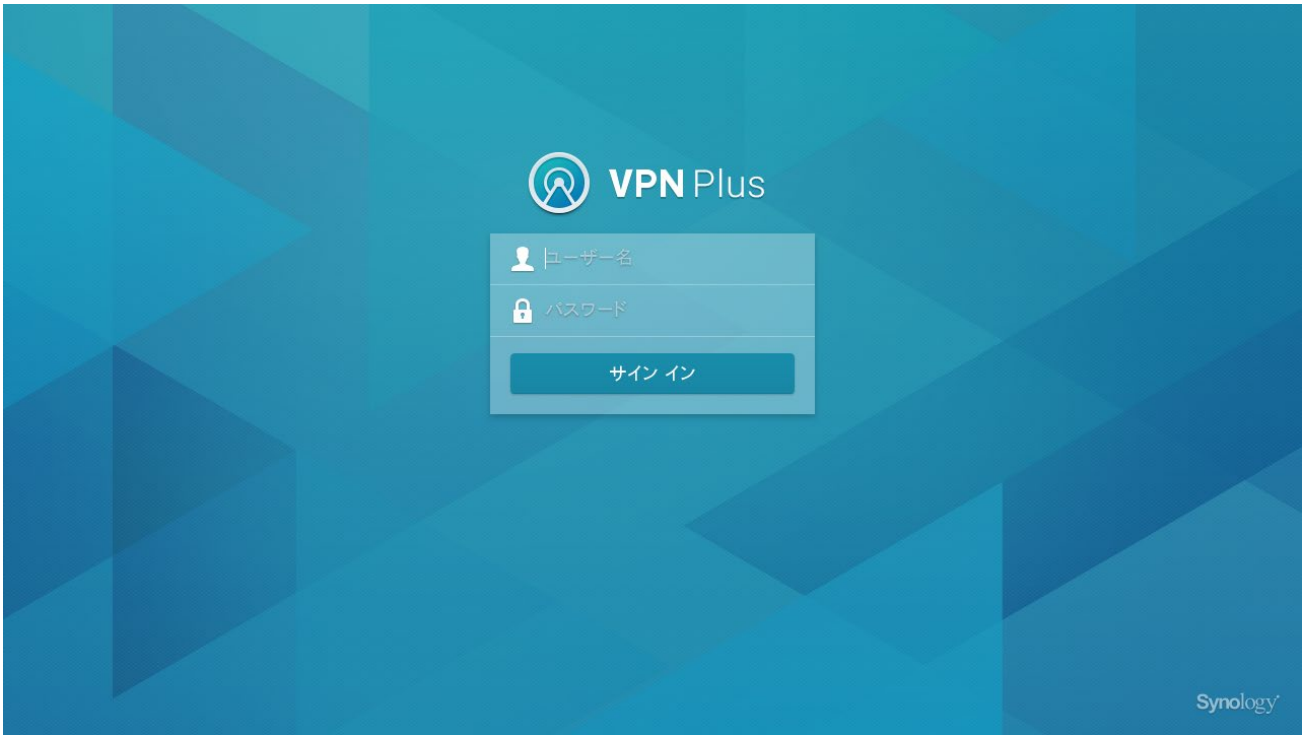
[Figure 8-6: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (6)]



[Figure 9-7: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (7)]



[Figure 10-8: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (8)]



[Figure 11-9: Example of a page displayed when the source of non-Mirai-type packets is accessed with a web browser (9)]

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.