JPCERT/CC Internet Threat Monitoring Report

April 1, 2020 ～ June 30 , 2020

JPCERT Coordination Center
July 30, 2020

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 aboutvulnerabilities, 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 mainly works with overseas National CSIRTs to deploy sensors and 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 during this quarter by sensors located in Japan.

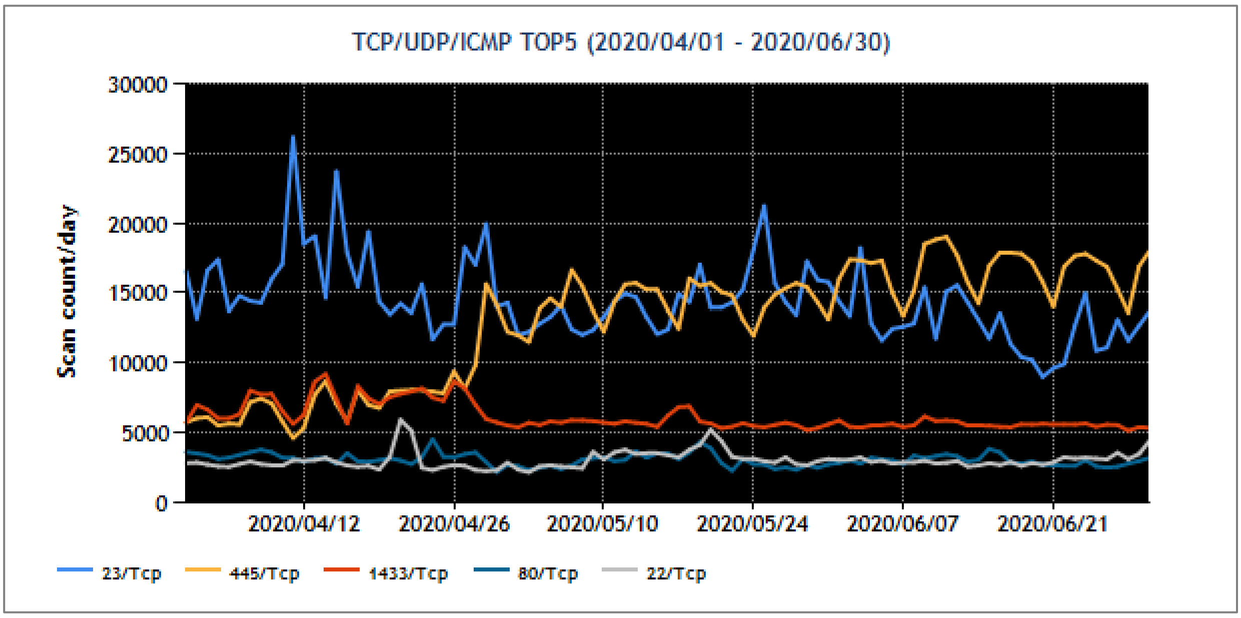
The top 5 destination port numbers for which packets were observed in Japan are listed in [Chart 1].

[Chart 1 : Top 5 destination port numbers]

Rank	Destination Port Numbers	Previous Quarter
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	3
3	1433/TCP (ms-sql)	2
4	80/TCP(http)	4
5	22/TCP	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[Figure 1].



[Figure 1: Number of packets observed at top 5 destination ports from April through June 2020]

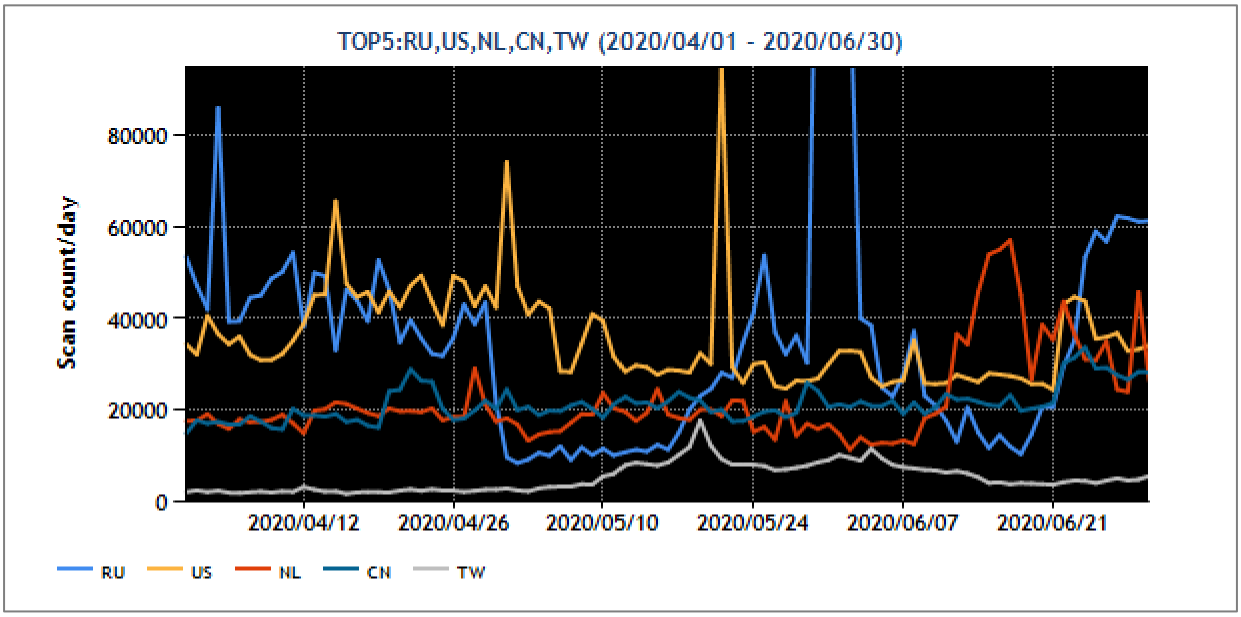
During this quarter, port 23/TCP (telnet) continued to receive the greatest number of packets. Port 445/TCP received the second most number of packets due to an increase seen from late April. Meanwhile, the number of packets targeted to port 1433/TCP decreased around the same time. Since these ports are both used in Windows environments, JPCERT/CC is investigating whether there is any relation between these changes.

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	Russia	1
2	USA	3
3	Netherlands	2
4	China	4
5	Taiwan	9

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



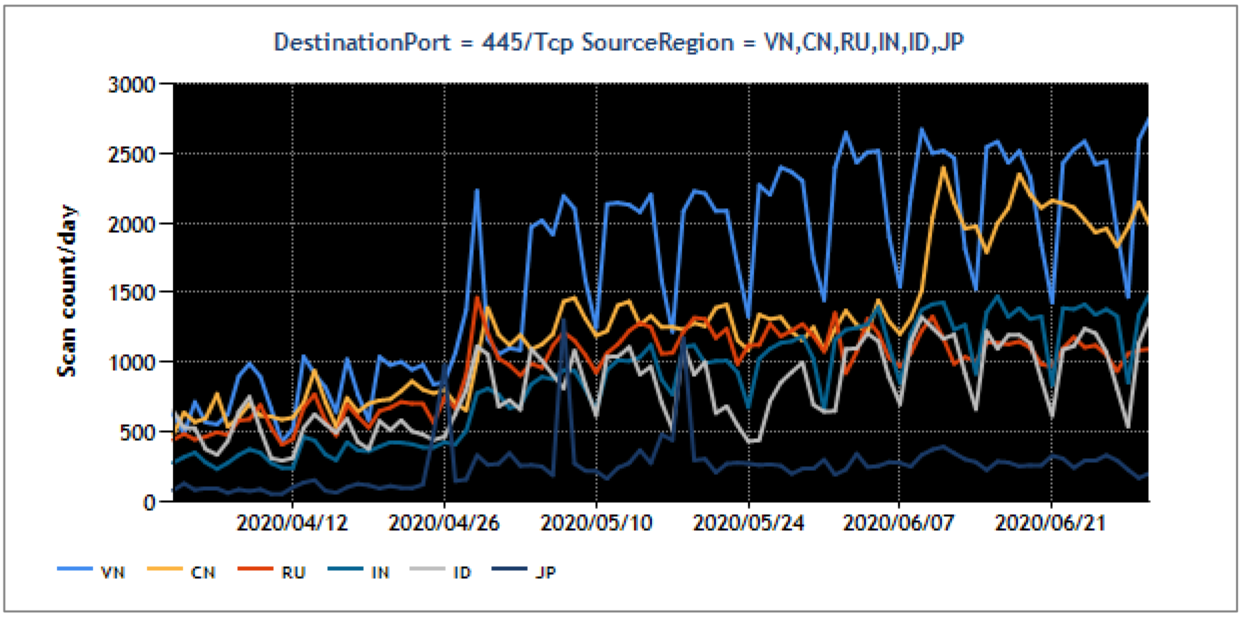
[Figure 2: Number of observed packets of the top 5 source regions from April through June 2020]

The top source region for the number of packets observed this quarter was Russia. The top 5 destination port numbers for packets originating in Russia are roughly the same as in other regions. However, its total number of packets for the top 5 destination port numbers is less than that of other source regions ranking below. The reason Russia still came out on top in total is the large number of observed packets targeted to other ports. It is assumed that packets were sent to scan for a wide range of open ports[2] instead of a specific port. The Netherlands, which ranked second, showed similar trends as Russia. As for other regions, there were no changes in the rankings.

2. Events of Note

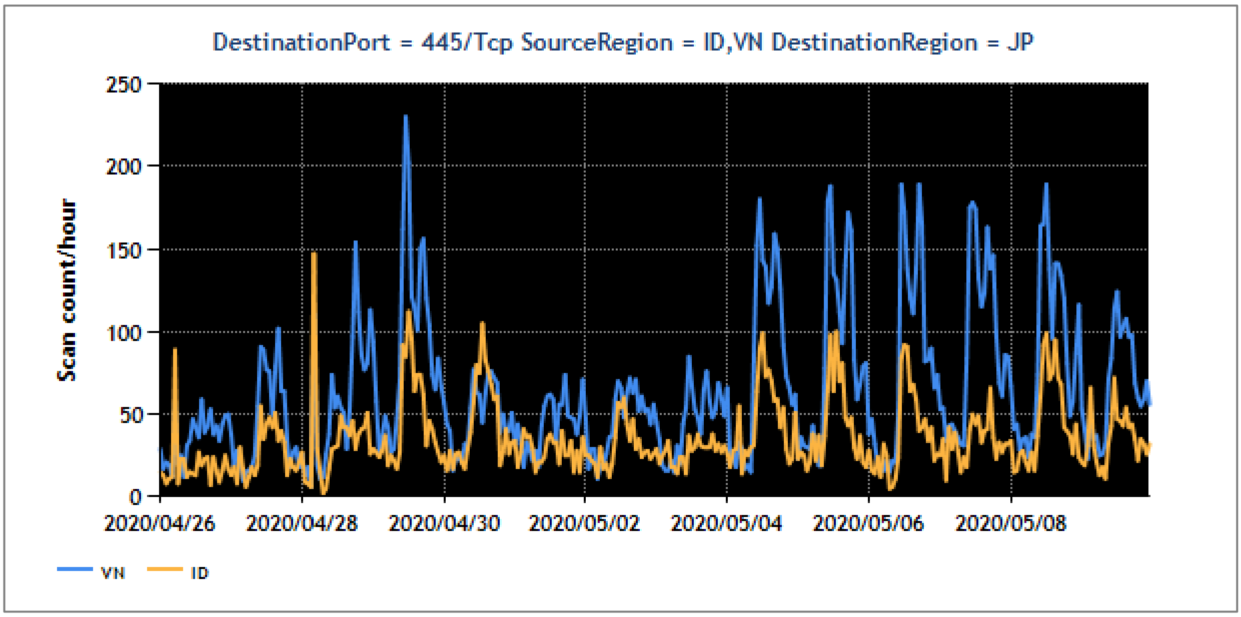
2.1. Increase in the number of packets destined for Port 445/TCP

Since around April 28, 2020, the number of packets sent to port 445/TCP from multiple regions has been increasing. See [Figure 3] for trends in the number of observed packets of the top 5 source regions plus Japan.

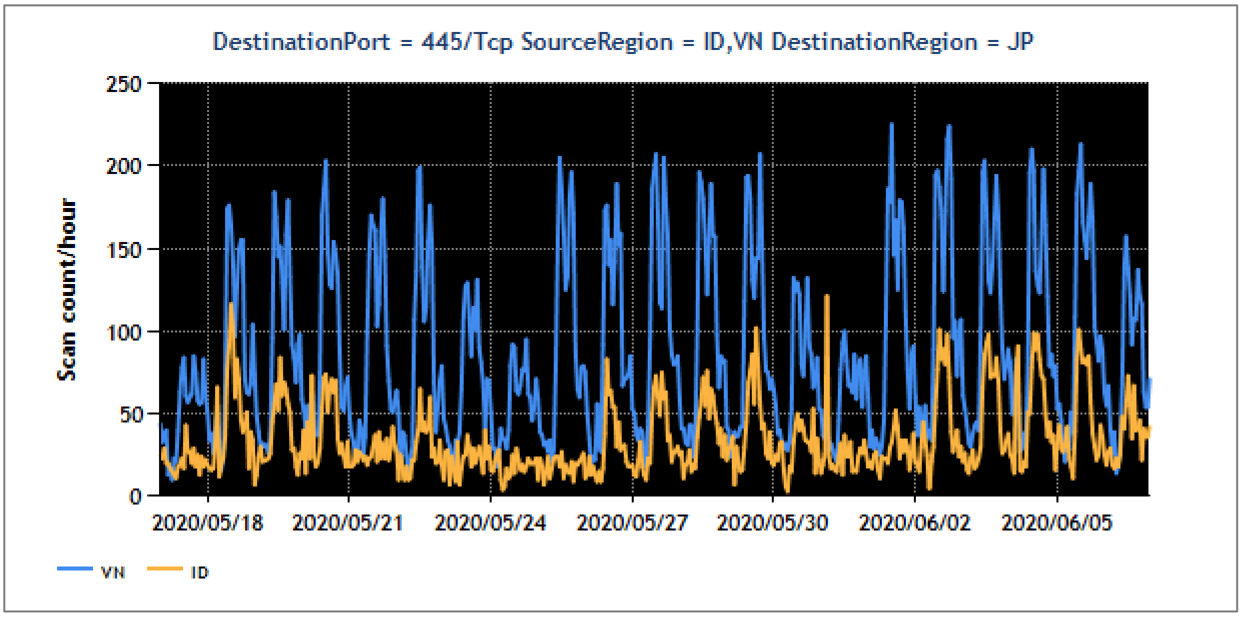


[Figure 3: Number of packets observed at top 5 destination ports from April through June 2020]

JPCERT/CC has observed the greatest number of packets originating in Vietnam. Moreover, it appears that the number of packets observed is changing every week. This trend is particularly evident in observation data for Vietnam and Indonesia [Figure 4,Figure 5].



[Figure 4: Number of packets sent from Vietnam and Indonesia between April 26 and May 9]



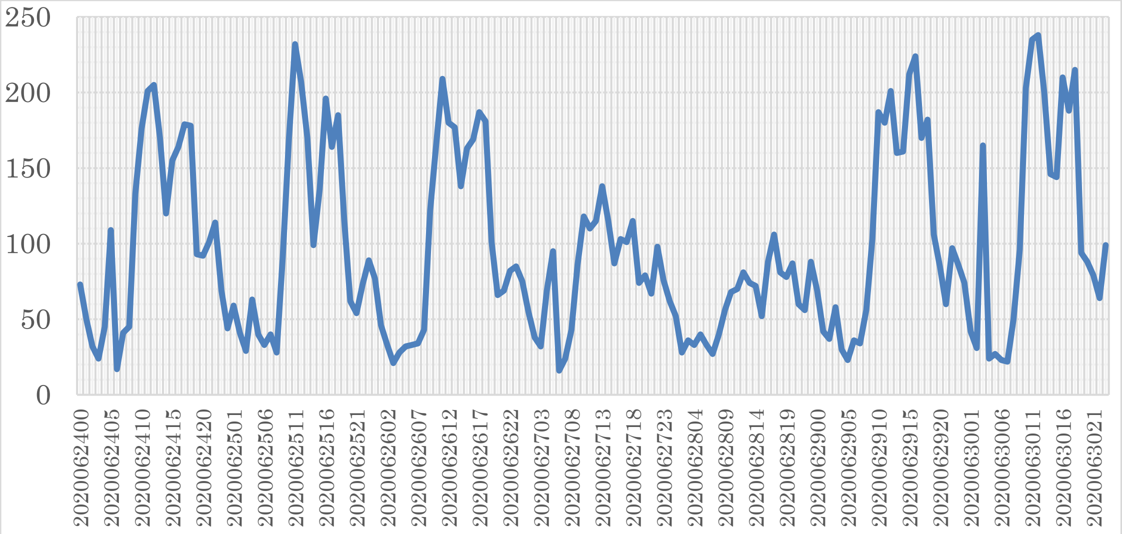
[Figure 5: Number of packets sent from Vietnam and Indonesia between May 17 and June 6]

Based on [Figure 4,Figure 5], it can be observed that the number of packets sent from Vietnam and Indonesia drops on Saturdays, Sundays and national holidays (see [Chart 3]).

[Chart 3: List of national holidays in Vietnam and Indonesia]

Observation Date	Region	Holiday
April 30	Vietnam	Reunification Day
May 1	Vietnam, Indonesia	Labor Day
May 7	Indonesia	Waisak
May 21	Indonesia	Ascension of Christ
May 22	Indonesia	Government-decreed holidays
May 24	Indonesia	Ramadan
May 25	Indonesia	Ramadan
June 1	Indonesia	Pancasila Day

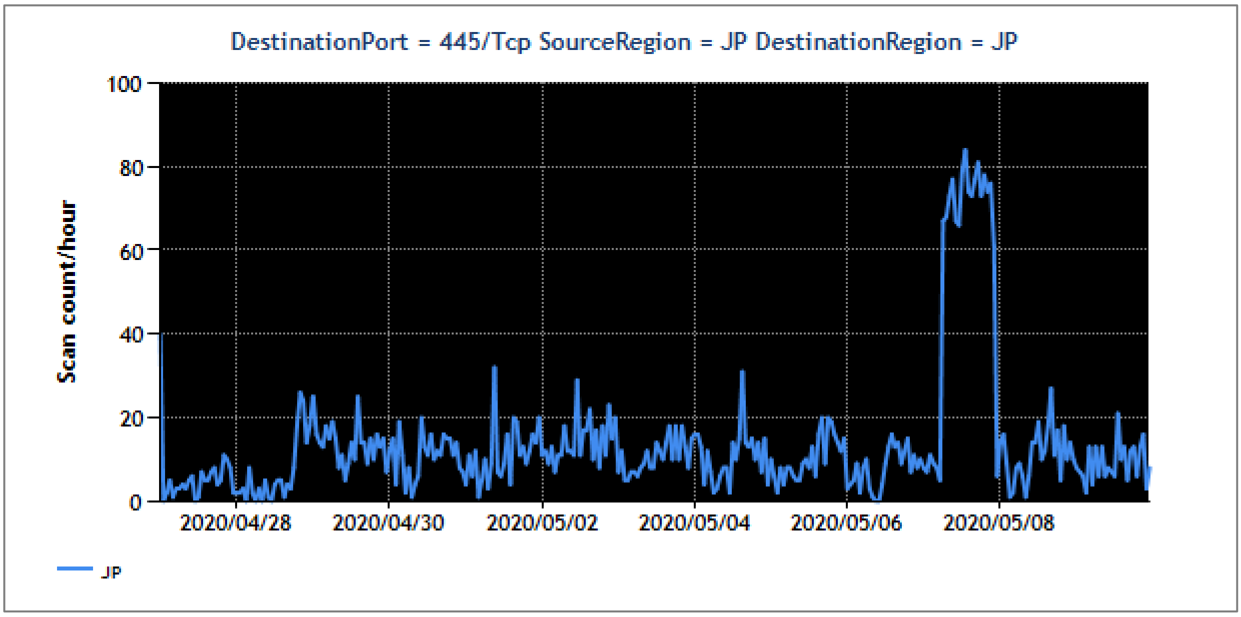
To observe the trend in more detail, hourly changes in the number of packets sent from Vietnam between June 24 and 30 are shown in[Figure 6].



[Figure 6: Number of packets sent from Vietnam between June 24 and June 30, 2020]

The horizontal axis of [Figure 6] shows the hours in Japan time (GMT+9), and the local time is 2 hours behind. According to this figure, the number of packets starts increasing from around 7:00 and 8:00 local time, temporarily drops at 12:00, increases again at 13:00, and drops at 19:00. This pattern roughly coincides with business hours in Vietnam. Although the reason behind the increase in packets is not clear, assuming that malware has something to do with this, it can be inferred that the number of packets observed is changing with the startup and shutdown of infected PCs. As there is a possibility that offices and schools that use PCs during weekdays may be infected with malware, JPCERT/CC provided the observation data to the national CSIRTs of the relevant regions.

Lastly, let’s look at the status of packets sent from Japan. While the number of packets is small compared to the top 5 source regions, JPCERT/CC observed an increase in the number of packets sent from Japan to port 445/TCP from around April 28 (see [Figure 7]).



[Figure 7: Number of packets sent from Japan between April 27 and May 9]

Unlike [Figure 5], however,[Figure 7] does not show any decrease in the number of packets on certain days of the week or on holidays. Moreover, packets are observed over a longer period of time during the day compared to [Figure 6], and the only time packets decrease is during midnight hours.

To collect information regarding this matter, JPCERT/CC is contacting all the entities managing the source IP addresses of these packets that appear to have been sent from a company or other organizations in Japan.

Contacted entities will be asked to conduct an investigation to the extent possible, and share the results if permissible. This information will help obtain a greater understanding of this phenomenon, and also serve as a reference in devising countermeasures in case a similar phenomenon occurs again.

2.2. Increase in packets attempting an attack on QNAP NAS

QNAP announced on June 8(2) that attacks targeting a published vulnerability in QNAP NAS software are on the rise. The targeted vulnerability has already been fixed in an updated version that is already available. In addition, the exploit code of the vulnerability was published on the Internet by researchers on May 25. (3)

Part of the reconnaissance and attack activities against this vulnerability is observed with TSUBAME's sensors as packets targeted to port 8080/TCP and so on. However, TSUBAME's observation results do not indicate the type of attack intended.

JPCERT/CC used a honeypot currently being tested to investigate the type of attack based on data captured since May 1, 2020, when the exploit code was not yet published. As a result, characteristics seen with the published exploit code were found in data observed on May 27 and later (see [Chart 4]).

This suggests that reconnaissance activities scanning for the said vulnerability started immediately after the exploit code was published.

[Chart 4: Honeypot observation trends]

Observation Date	Source Region	Destination Port Number	Request	Count
May 27	Russia	8080	/photo/p/api/album.php	1
May 28	Russia	8080	/photo/p/api/album.php	3
May 29	Russia	5000	/photo/p/api/album.php	1
		5001	/photo/p/api/album.php	4
		8083	/photo/p/api/album.php	4
May 30	Russia	5000	/photo/p/api/album.php	3
May 31	Russia	8080	/photo/p/api/album.php	3

It is also possible that the requests listed in [Chart 4]were performed against focused targets based on information obtained from other sources. However, given that communications from the same source IP addresses were also detected by TSUBAME almost without exception, it appears likely that the scans are being performed widely in an exhaustive fashion, without narrowing down the targets in advance.
JPCERT/CC has received reports of attacks targeting this vulnerability.(4) It is advised that users of the products check their logs to make sure there is no anomaly

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) eCh0raix Ransomware
https://www.qnap.com/ja-jp/security-advisory/QSA-20-02

(3) QNAP QTS and Photo Station 6.0.3 - Remote Command Execution
https://www.exploit-db.com/exploits/48531

(4) Information about ransomware affecting QNAP NAS and Photo Station
https://www.jpcert.or.jp/newsflash/2020060901.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 2020.

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