JPCERT/CC Incident Handling Report

July 1, 2023 - September 30, 2023

JPCERT Coordination Center

October 17, 2023

JPCERT CC®

Table of Contents

1. About the Incident Handling Report 3
2. Quarterly Statistics 3
3. Incident Trends 10
3.1. Phishing Site Trends 10
3.2. Website Defacement Trends 11
3.3. Targeted Attack Trends 12
3.4. Other Incident Trends 13
4. Incident Handling Case Examples 13
Request from JPCERT/CC 16
Appendix-1. Classification of Incidents 17

1. About the Incident Handling Report

JPCERT Coordination Center (herein, JPCERT/CC) receives reports on computer security incidents (herein, incidents) that occur inside and outside Japan [(1)]. This report will introduce statistics and case examples for incident reports received during the period from July 1, 2023 through September 30, 2023.

[(1)] JPCERT/CC refers to all events that may occur in the management of information systems, which include events that may be considered security issues and any case related to computer security, as an incident.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to prevent the spreading of damages from incidents. For incidents that require global coordination and assistance, JPCERT/CC acts as the point of contact for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.).

2. Quarterly Statistics

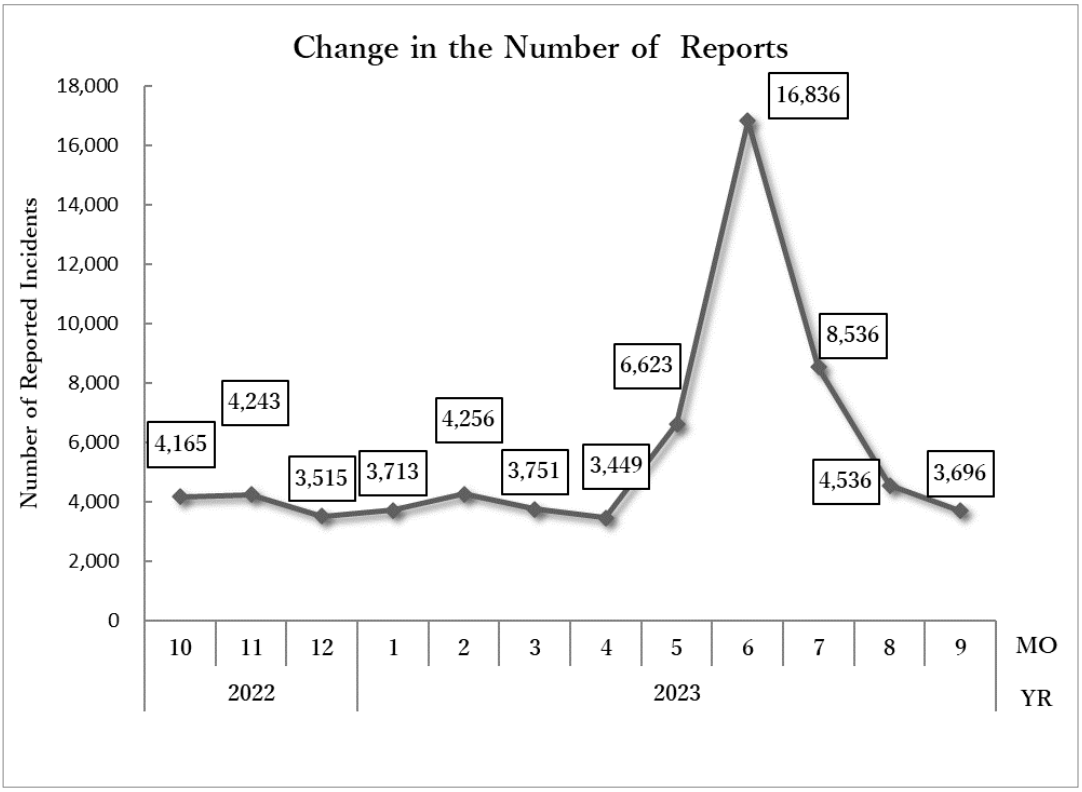
[Chart 1]shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1: Number of incident reports]

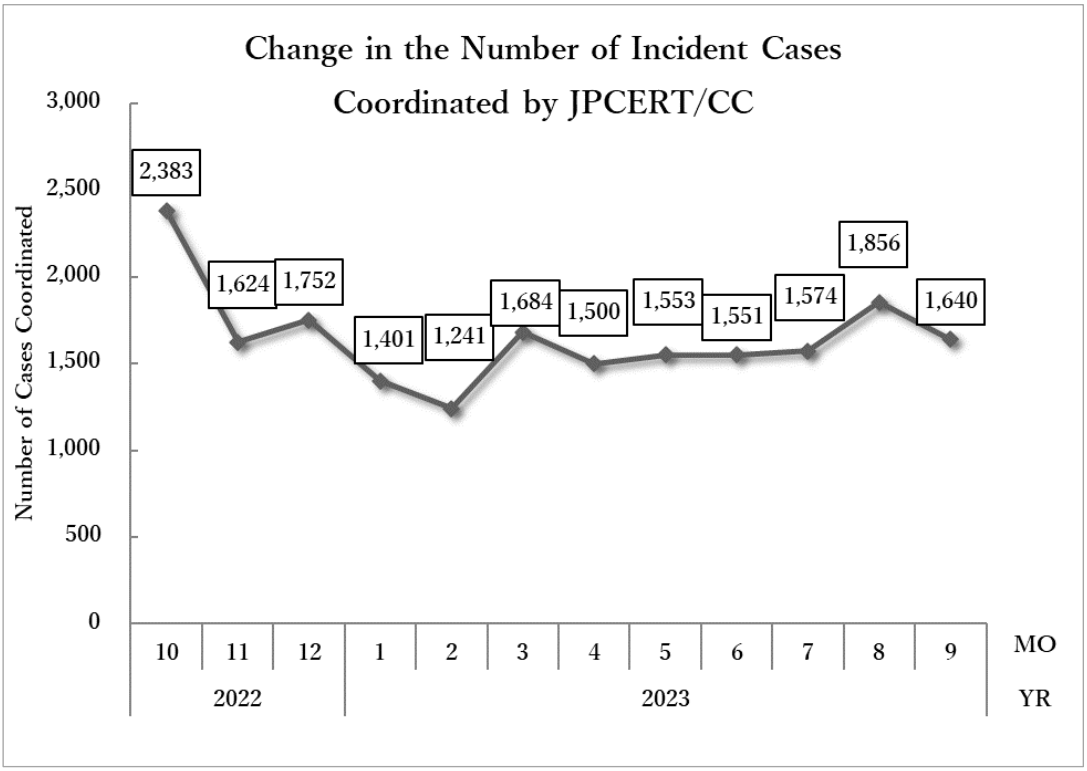
	Jul	Aug	Sept	Total	Last Qtr. Total
Number of Reports [(2)]	8,536	4,536	3,696	16,768	26,908
Number of Incident [(3)]	2,157	1,952	1,794	5,903	7,925
Cases Coordinated [(4)]	1,574	1,856	1,640	5,070	4,604

(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.
(3) "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incidents are counted as 1 incident.
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 16,768. Of these, the number of cases that JPCERT/CC coordinated was 5,070. When compared with the previous quarter, the number of reports decreased by 38%, and the number of cases coordinated increased by 10%. Year on year, the number of reports increased by 24%, and the number of cases coordinated decreased by 21%.
[Figure 1] and [Figure 2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.



[Figure 1: Change in the number of incident reports]

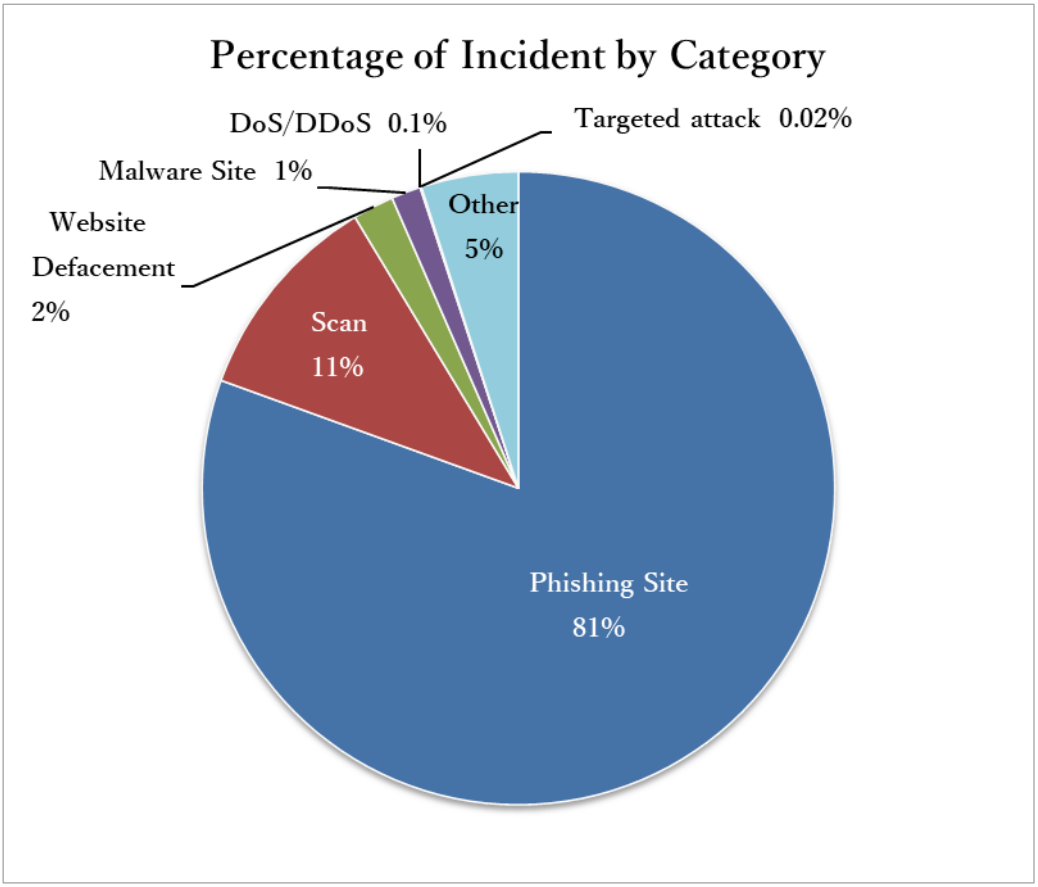


[Figure 2: Change in the number of incident cases coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of each incident category, please see "Appendix 1 - Incident Categories".[Chart 2] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in[Figure 3].

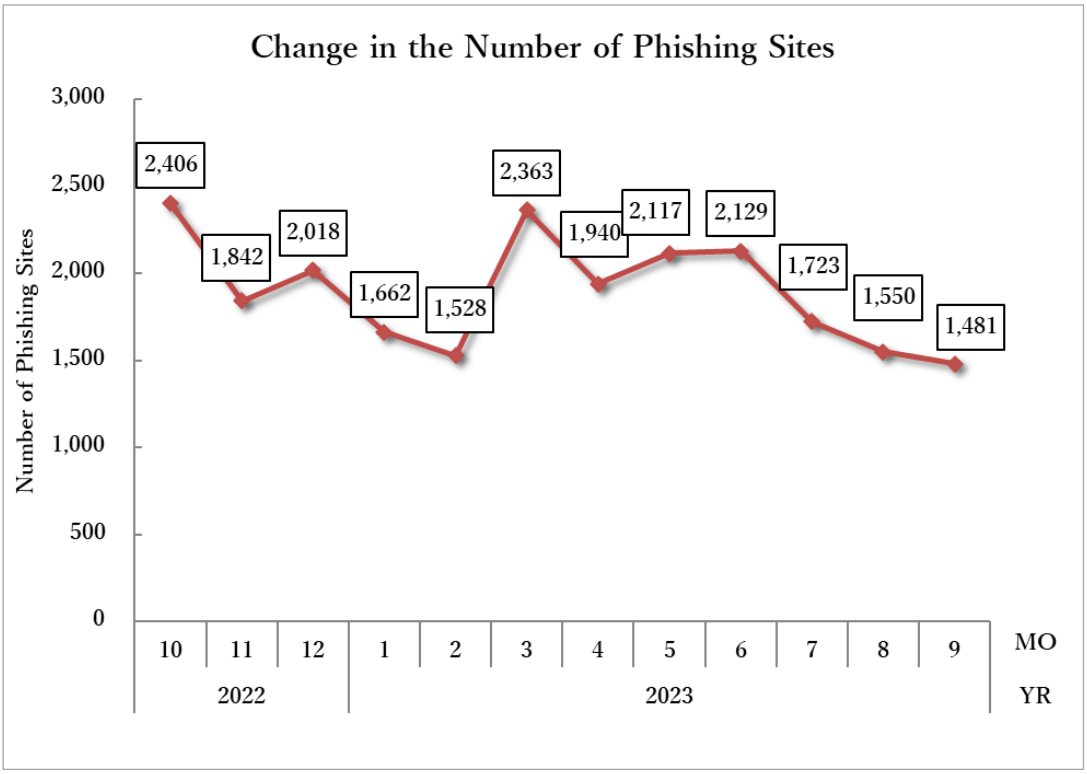
[Chart 2: Number of incidents by category]

Incident Category	Jul	Aug	Sept	Total	Last Qtr. Total
Phishing Site	1,723	1,550	1,481	4,754	6,186
Website Defacement	71	32	21	124	311
Malware Site	13	38	38	89	97
Scan	229	238	172	639	998
DoS/DDoS	0	0	3	3	8
ICS Related	0	0	0	0	1
Targeted attack	1	1	0	2	4
Other	120	93	79	292	320

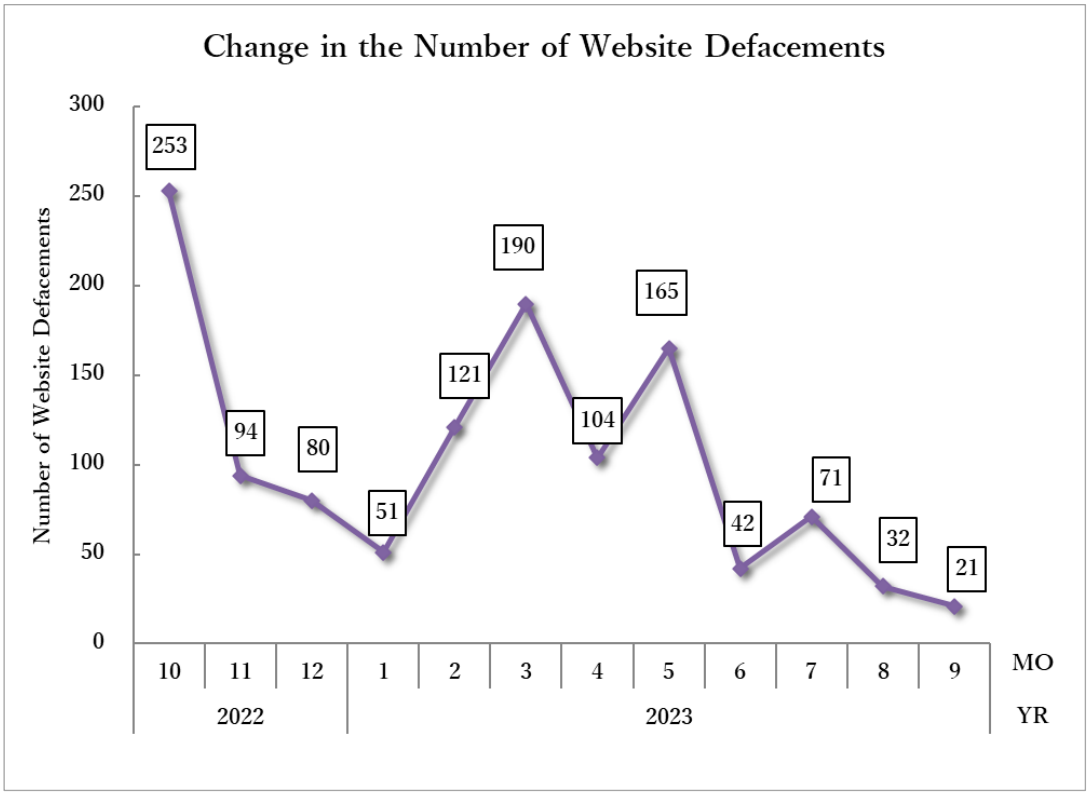


[Figure 3: Percentage of incidents by category]

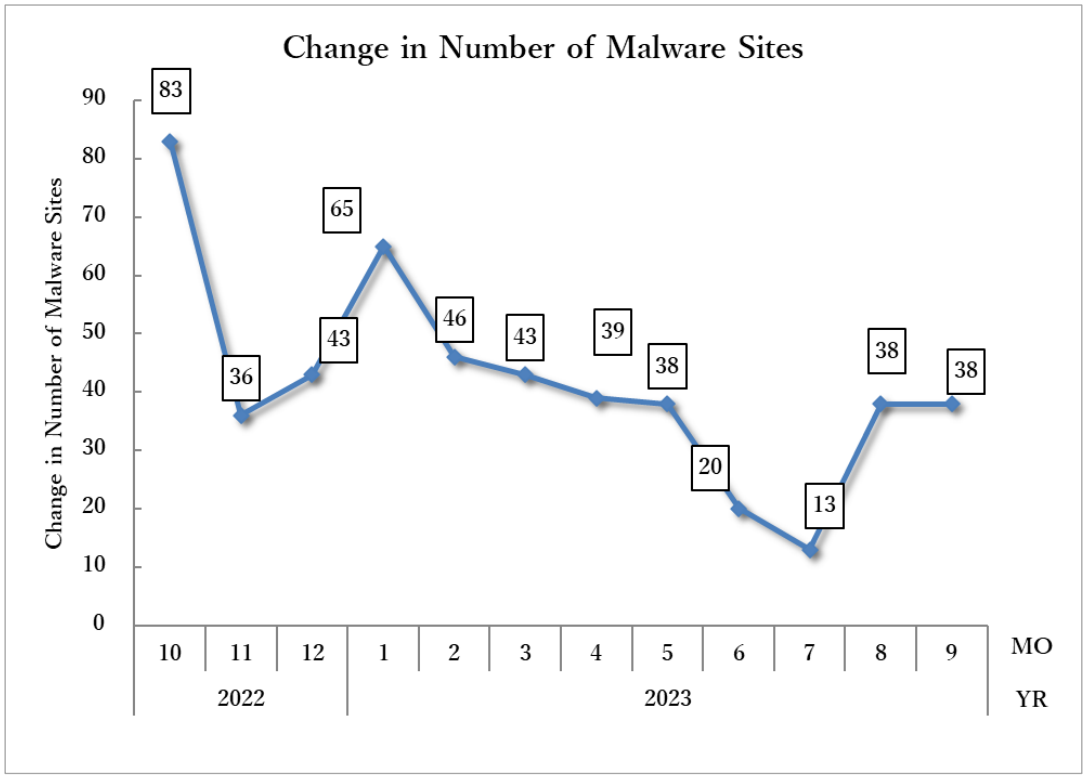
Incidents categorized as phishing sites accounted for 81%, and those categorized as scans, which search for vulnerabilities in systems, made up 11%.
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



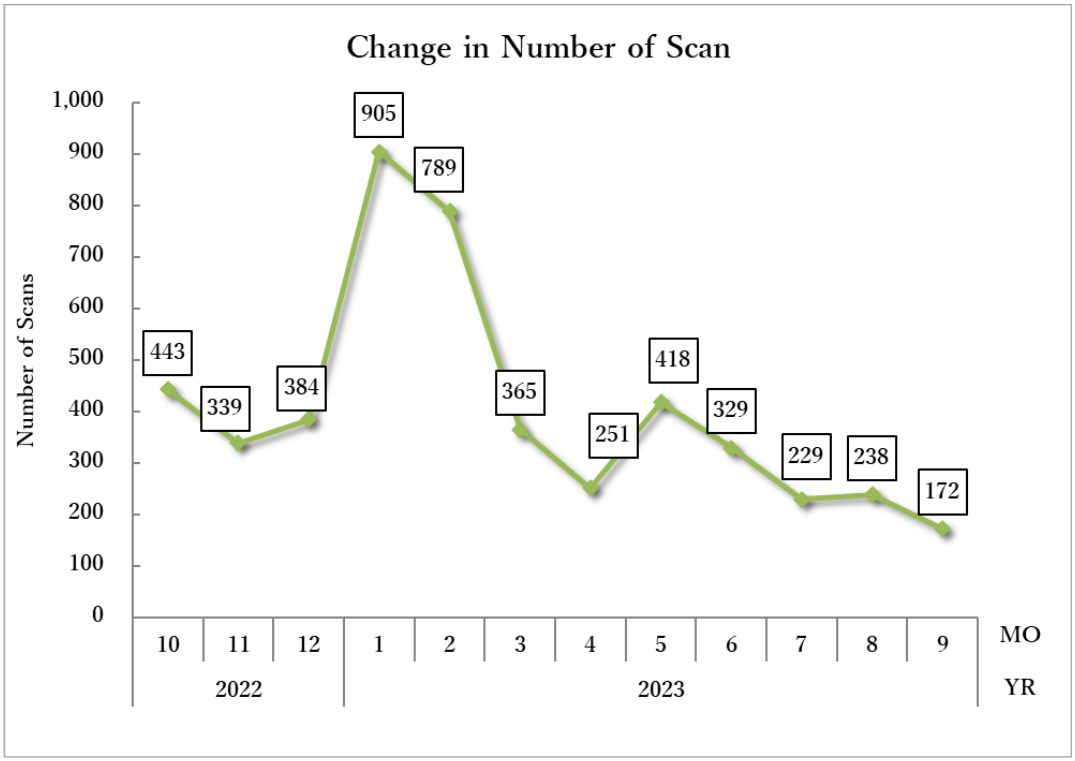
[Figure 4: Change in the number of phishing sites]



[Figure 5: Change in the number of website defacements]

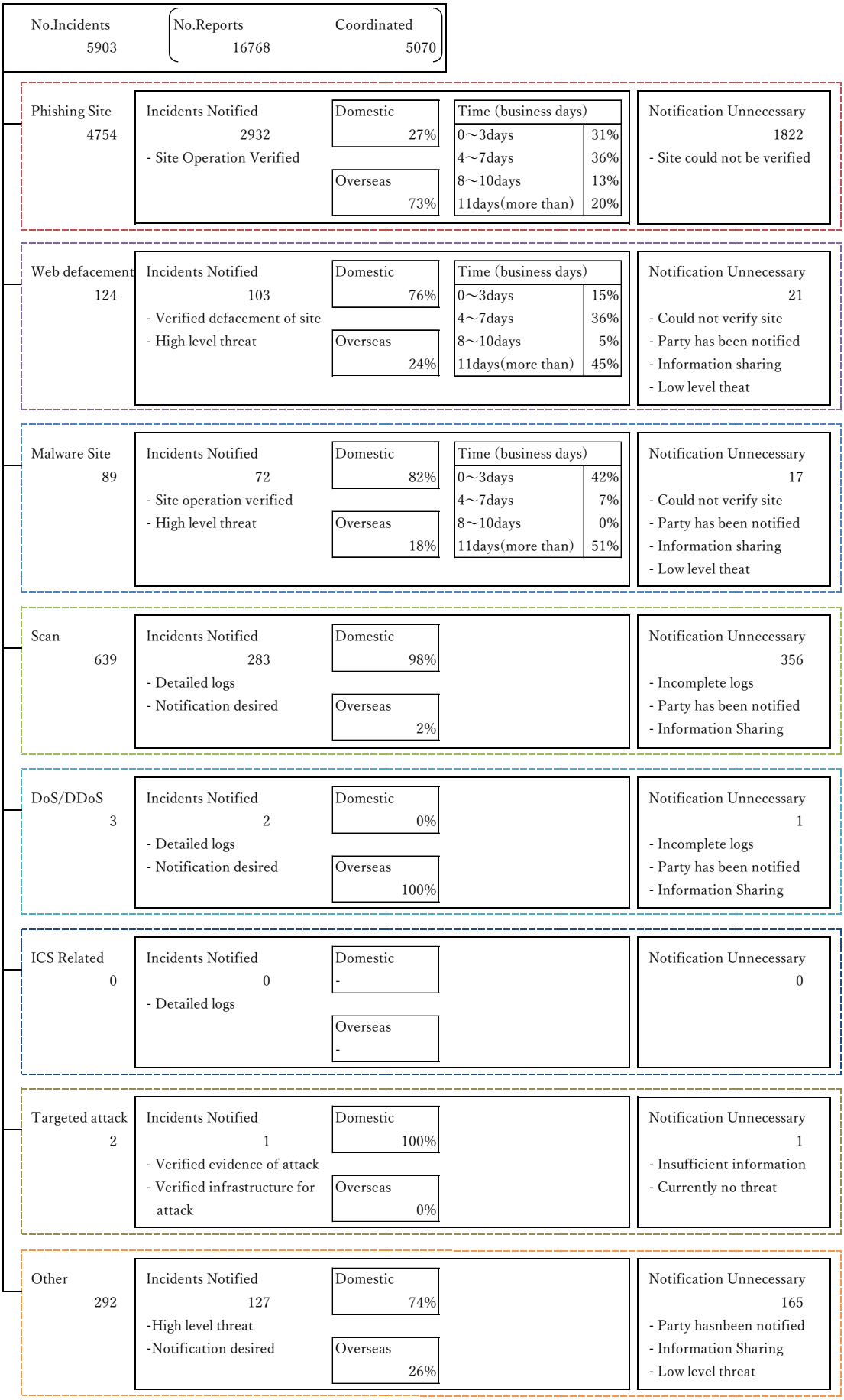


[Figure 6: Change in the number of malware sites]



[Figure 7: Change in the number of scans]

[Figure 8] provides an overview as well as a breakdown of the incidents that were coordinated /Handled.



[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

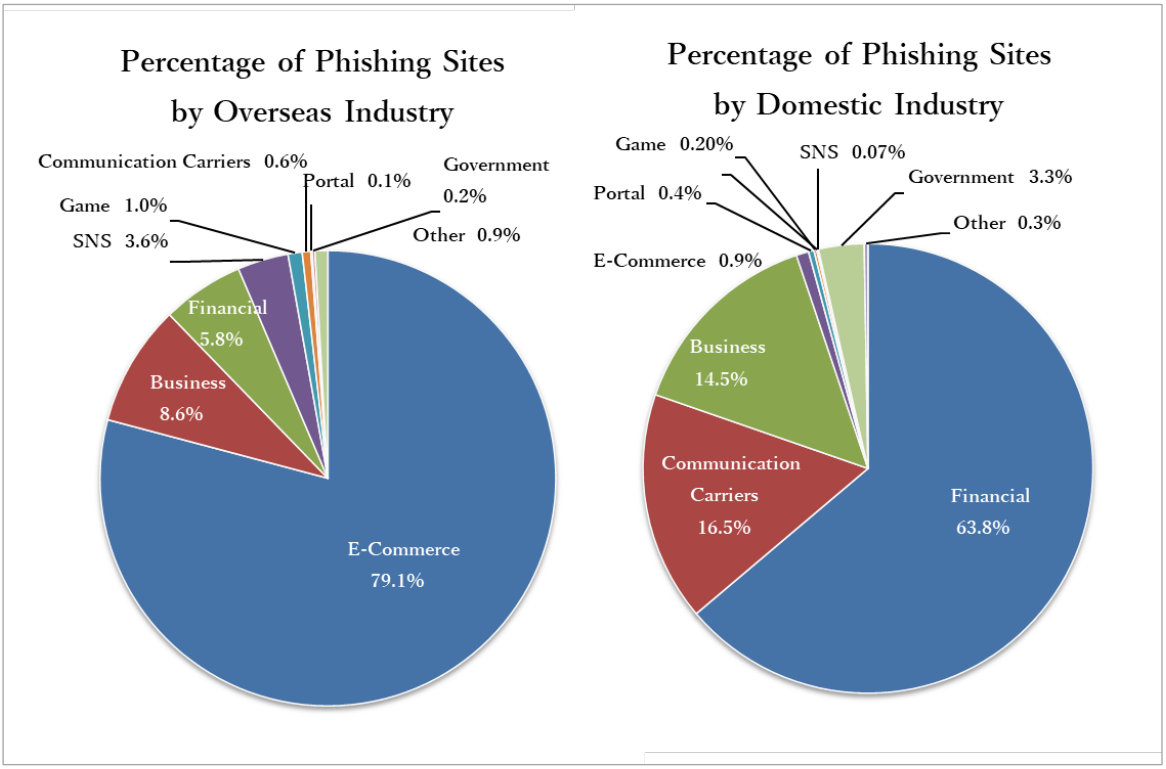
During this quarter, 4,754 reports on phishing sites were received, representing a 23% decrease from 6,186 in the previous quarter. This marks a 37% decrease from the same quarter last year (7,520).

During this quarter, there were 3,029 phishing sites that spoofed domestic brands, decreasing 18% from 3,700 in the previous quarter. There were 997 phishing sites that spoofed overseas brands, decreasing 36% from 1,568 in the previous quarter. The numbers of brands that the phishing sites spoofed in this quarter are shown by brand type (domestic, overseas) in [Chart 3], and the percentages by industry for domestic and overseas brands are shown in [Figure 9].

[Chart 3: Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jul	Aug	Sept	Domestic/Overseas Total (%)
Domestic Brand	1,052	980	997	3,029 (64%)
Overseas Brand	438	310	249	997 (21%)
Unknown Brand (*5)	233	260	235	728 (15%)
Monthly Total	1,723	1,550	1,481	4,754

(*5) "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[Figure 9: Percentage of reported phishing sites by industry (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 79.1% spoofed e-commerce websites for overseas brands and 63.8% spoofed financial websites for domestic brands, both representing the largest share respectively.

For overseas brands, phishing sites spoofing Amazon accounted for more than half of the phishing sites reported.
For domestic brands, phishing sites spoofing East Japan Railway Company's Eki-Net website and Electronic Toll Collection (ETC) system usage inquiry services were reported in large numbers. Among domestic financial institutions, phishing sites spoofing EPOS Card, Saison Card, Aeon Card, and Sumitomo Mitsui Card continued to be seen in large numbers as in the previous quarter. Compared with the previous quarter, there were marked declines in the numbers of phishing sites spoofing TEPCO, Mobile Suica, the Bank of Yokohama, the Ministry of Health, Labour and Welfare, and au Jibun Bank.

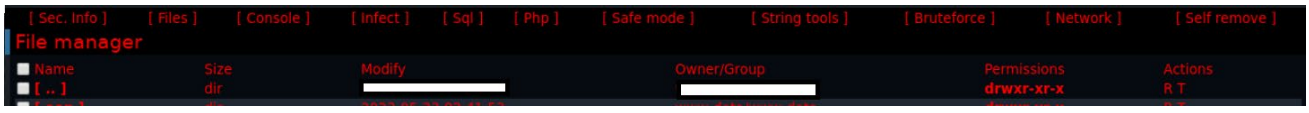
The websites that JPCERT/CC coordinated with to take down phishing sites were 27% domestic and 78% overseas for this quarter, which are roughly the same as the previous quarter (domestic: 25%, overseas: 75%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 124. This was a 60% decrease from 311 in the previous quarter.

During this quarter, JPCERT/CC confirmed various attacks on legitimate websites, including those that inject a script for redirecting the user to a suspicious website ([Figure 10]), those that install a phishing kit, and those that set up an e-mail sending program. Compromised websites were planted with a WebShell as shown in [Figure 11], allowing files in the server to be viewed, files to be uploaded to or downloaded from the server, and any command to be executed from outside.

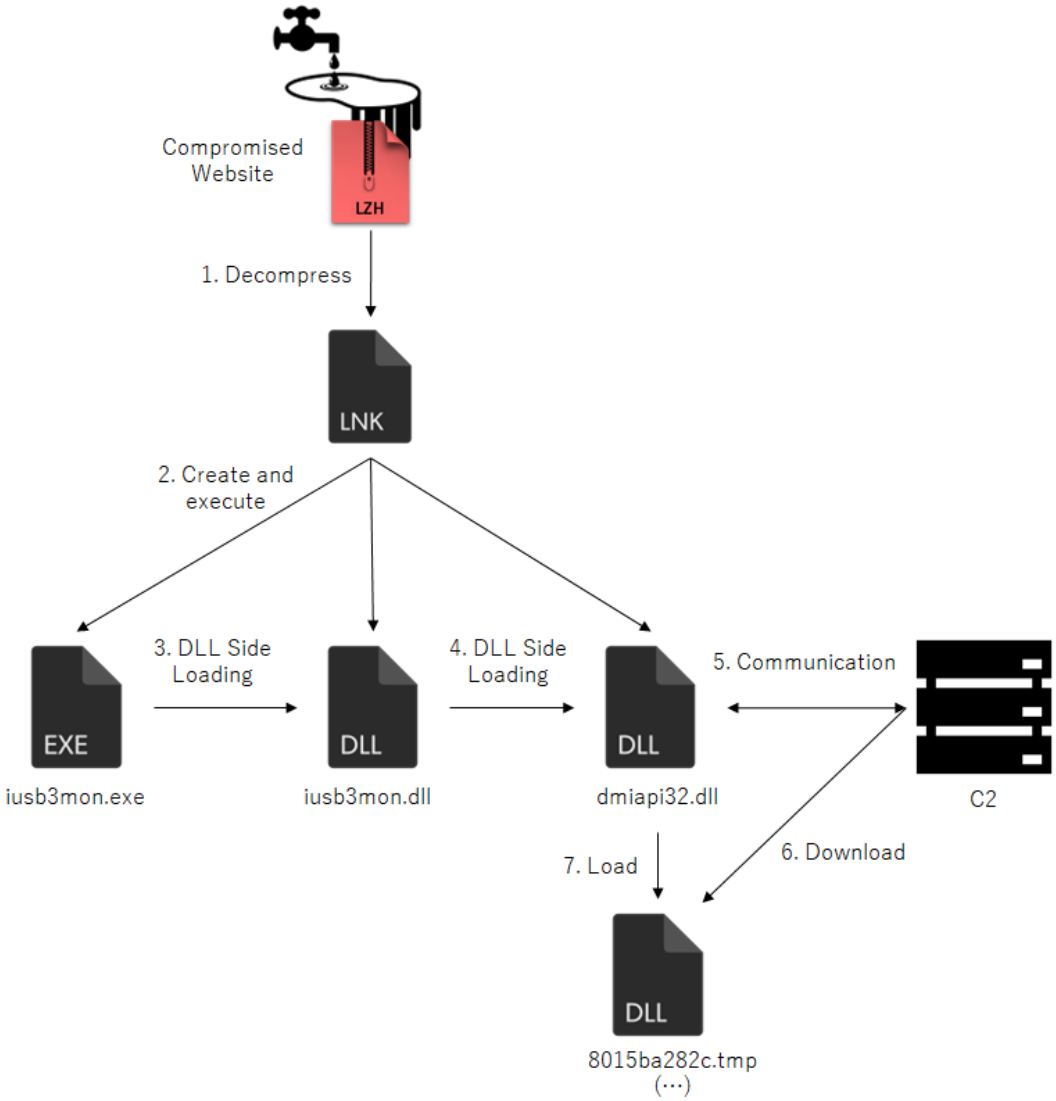
[Figure 10: Example of a maliciously injected]



[Figure 11: Example of a maliciously planted WebShell]

3.3. Targeted Attack Trends

There were 2 incidents categorized as a targeted attack, one of which was identified and is described below. This quarter, JPCERT/CC received reports on the defacement of a website that provides subscription services to paying members. According to the reports, users who accessed paid content on this website ended up downloading malware planted on the website. When users access the compromised website, an LZH file is downloaded, and when they run a file contained in the compressed file, their devices get infected with malware. The compressed file contains a shortcut file that, when executed, generates a number of files on the device, ultimately communicating with the attacker's server to download additional malware. [Figure 12] illustrates the flow of events after the LZH file is executed, up to infection with the malware.



[Figure 12: Flow of events up to infection with malware from the compromised website]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 89. This was an 8% decrease from 97 in the previous quarter.

The number of scans reported in this quarter was 639. This was a 36% decrease from 998 in the previous quarter. The top 10 ports that the scans targeted are listed in[Chart 4]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP), HTTP (80/TCP), 37215/TCP and 52869/TCP.

[Chart 4: Top 10 ports by number of scans]

Port	Jul	Aug	Sept	Total
22/tcp	112	125	85	322
23/tcp	50	66	55	171
80/tcp	21	12	7	40
37215/tcp	13	20	2	35
52869/tcp	12	5	0	17
445/tcp	1	2	8	11
443/tcp	9	1	1	11
25/tcp	5	1	4	10
8080/tcp	6	0	0	6
5555/tcp	2	0	1	3

There were 292 incidents categorized as other. This was a 9% decrease from 320 in the previous quarter.

4. Incident Handling Case Examples

This section will describe some actual cases that JPCERT/CC handled in this quarter.

(1) Coordination involving a vulnerability (CVE-2023-3519) in Citrix ADC and Citrix Gateway

On July 18, 2023, Citrix released information about multiple vulnerabilities in Citrix ADC and Citrix Gateway. JPCERT/CC released a security alert as well on July 19 since these vulnerabilities may be exploited by unauthenticated third parties to remotely execute arbitrary code.

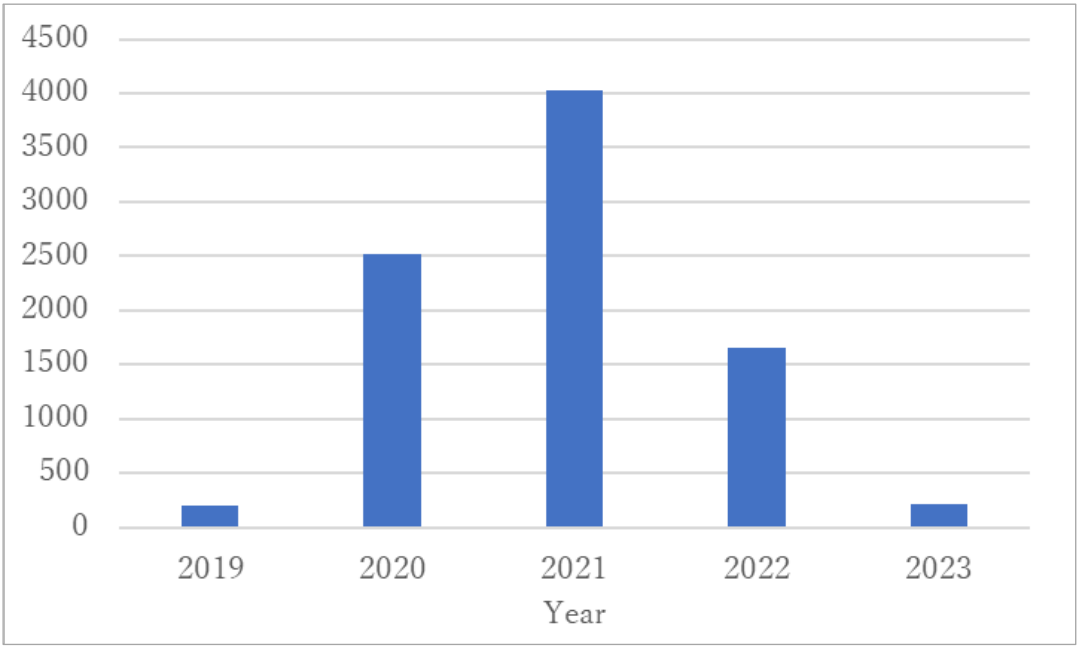
Alert Regarding Vulnerability (CVE-2023-3519) in Citrix ADC and Citrix Gateway
https://www.jpcert.or.jp/english/at/2023/at230013.html

On July 18, 2023, Citrix released information about multiple vulnerabilities in Citrix ADC and Citrix Gateway. JPCERT/CC released a security alert as well on July 19 since these vulnerabilities may be exploited by unauthenticated third parties to remotely execute arbitrary code.

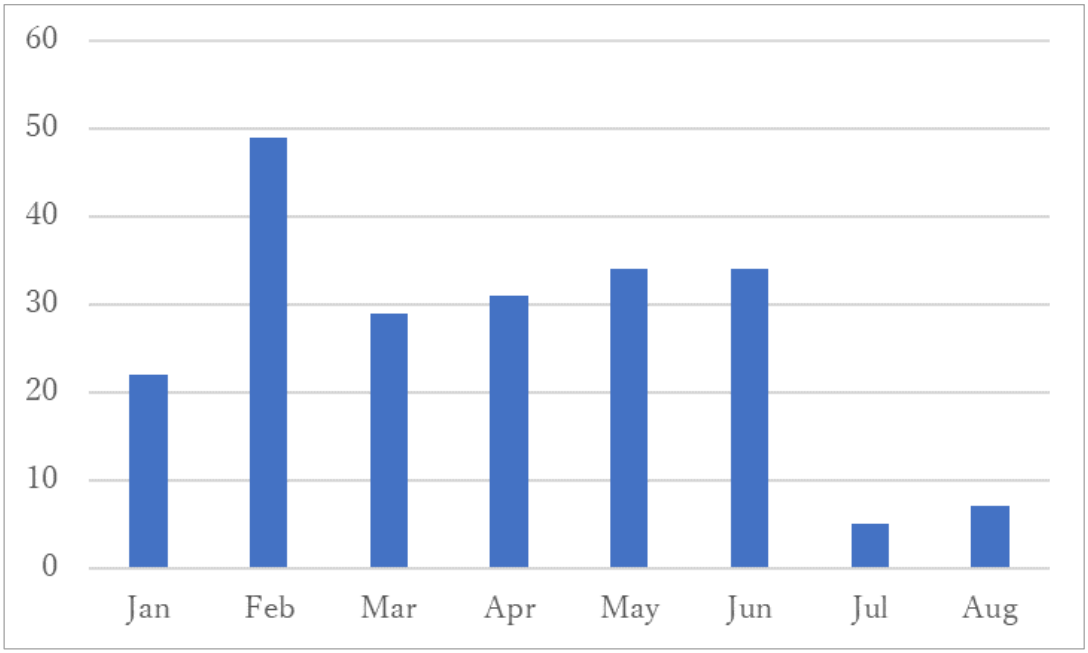
Also, even if a patch for these vulnerabilities has been applied, a backdoor installed by an attacker before the patch was applied may remain. JPCERT/CC has notified the administrators of devices in Japan suspected of such backdoor installation.

(2) Notification to users of devices infected with Qakbot

In August 2023, a multinational team of seven countries led by the United States carried out a takedown operation dubbed Operation Duck Hunt, targeting Qakbot malware. As a result, Qakbot's C2 server was stopped, and Qakbot was removed from infected devices. Subsequently, information about infected devices and relevant account information were identified, and information about infected devices in Japan (infections occurred between 2019 and August 2023) was provided to JPCERT/CC in September. It is assumed that about 80% of the infected devices (40,000) reported to JPCERT/CC were test devices used by researchers. [Figure 13] shows the numbers of infected devices excluding such test devices. Infections have been declining after peaking out in 2021. [Figure 14] shows the numbers for each month in 2023. Currently, it is evident that infected devices have significantly decreased compared to 2021. Based on this data, JPCERT/CC is notifying the users of devices still suspected of Qakbot infection through network operators.



[Figure 13: Numbers of devices infected with Qakbot (by year)]



[Figure 14: Numbers of devices infected with Qakbot in 2023 (by month)]

Request from JPCERT/CC

JPCERT/CC is working to prevent the spread of losses and damages due to incidents and their recurrence through various activities. These include understanding the status and tendency of incidents, and coordination with the aim of suspending or blocking, as the situation requires, attack sources and destination of information transmission, etc. JPCERT/CC also issues alerts and other information to users to make them aware of the need to implement countermeasures.

JPCERT/CC asks for your continued cooperation with information sharing. Please refer to the following web pages for how to report incidents.

Reporting an Incident
https://www.jpcert.or.jp/english/ir/form.html

Reporting an ICS Incident
https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

If you would like to encrypt your report, please use JPCERT/CC's PGP public key. The public key can be obtained at the following web page.

PGP Public Key
https://www.jpcert.or.jp/english/ir/pgp.html

JPCERT/CC provides a mailing list to ensure speedy delivery of the information it issues. If you wish to use the mailing list, please refer to the following information.

Appendix-1. Classification of Incidents

JPCERT/CC classifies incidents contained in reports it receives according to the following definitions.

○ Phishing Site

A "phishing site" refers to a site that spoofs the legitimate site of a bank, auction or other service operators to carry out "phishing fraud" intended to steal user information including IDs, passwords and credit card numbers.

JPCERT/CC classifies the following as "phishing sites".

- Websites made to resemble the site of a financial institution, credit card company, etc.
- Websites set up to guide visitors to a phishing site

○ Website Defacement

"Website defacement" refers to a site whose content has been rewritten by an attacker or malware (including the embedding of a script unintended by the administrator).

JPCERT/CC classifies the following as "website defacement".

- Sites embedded with a malicious script, iframe, etc., by an attacker, malware, etc.
- Sites whose information has been altered by an SQL injection attack

○ Malware Site

A "malware site" refers to a site that infects the computer used to access the site with malware, or a site on which malware used for attack is made publicly available.

JPCERT/CC classifies the following as "malware sites".

- Sites that attempt to infect the visitor's computer with malware
- Sites on which an attacker makes malware publicly available

○ Scan

A "scan" refers to an access made by an attacker (that does not affect the system) to check for the existence of computers, servers and other systems targeted for attack, or to search for vulnerabilities (security holes, etc.) that can be exploited to make unauthorized intrusion into systems. It also includes attempts to infect by malware, etc.

JPCERT/CC classifies the following as "scans".

- Vulnerability searches (checking the program version, service operation status, etc.)
- Attempts to make an intrusion (those that failed)
- Attempts to infect by malware (viruses, bots, worms, etc.) (those that failed)
- Brute force attacks targeting ssh, ftp, telnet, etc. (those that failed)

○ DoS/DDoS

"DoS/DDoS" refers to an attack against servers and/or computers on a network, and network resources including devices and connection lines that make up a network, with an attempt to make a service unavailable.

JPCERT/CC classifies the following as "DoS/DDoS".

- Attacks that exhaust network resources with a large volume of traffic, etc.
- Reduction or suspension of server program responses due to a large access volume
- Service interference by sending a large volume of e-mail (error e-mail, SPAM e-mail, etc.)

○ ICS Related Incident

An "ICS related incident" refers to an incident related to ICS or plants.

JPCERT/CC classifies the following as an "ICS related incident".

- ICSs that are subject to attack via the Internet
- Servers that malware targeting ICSs communicates with
- Attacks that cause abnormal operations of an ICS

○ Targeted attack

A "targeted attack" is a type of attack in which specific organizations, companies, or industries are targeted for malware infection or unauthorized access.

JPCERT/CC categorizes the following as a targeted attack.

- Spoofed e-mail with malware attached sent to a specific organization
- Defacement of a website affected to limited organizations
- A fake website accessible to limited organizations and attempting to infect site visitor's computer
- A command and control server that specially crafted malware communicates with

○ Other

"Other" refers to incidents other than the above.

- The following are examples of incidents that JPCERT/CC classifies as "other".
- Unauthorized intrusion into a system exploiting a vulnerability, etc.
- Unauthorized intrusion by a successful brute force attack targeting ssh, ftp, telnet, etc.
- Stealing of information by malware with a keylogger function
- Infection by malware (viruses, bots, worms, etc.)

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.