JPCERT/CC Incident Handling Report

October 1, 2022 - December 31, 2022

JPCERT Coordination Center

January 19, 2023

JPCERT CC®

Table of Contents

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 October 1, 2022 through December 31, 2022.

(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 preventthe 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

[Chart1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1: Number of incident reports]

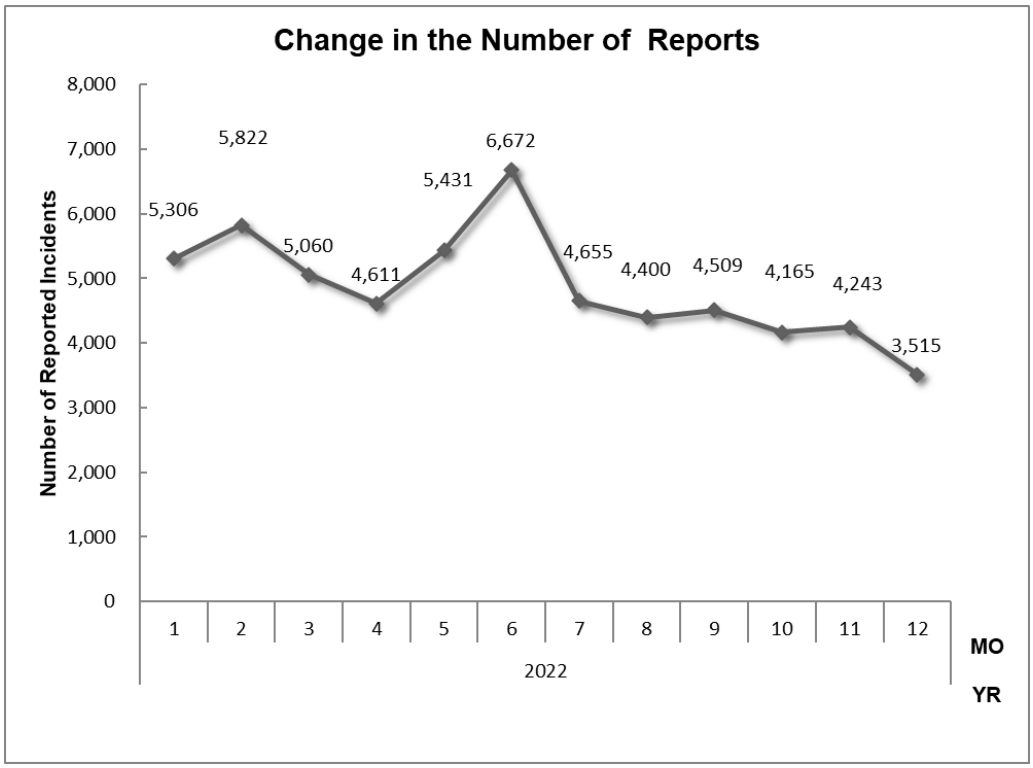
	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports[(2)]	4,165	4,243	3,515	11,923	13,564
Number of Incident[(3)]	3,274	2,452	2,699	8,425	10,656
Cases Coordinated[(4)]	2,383	1,624	1,752	5,759	6,444

(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

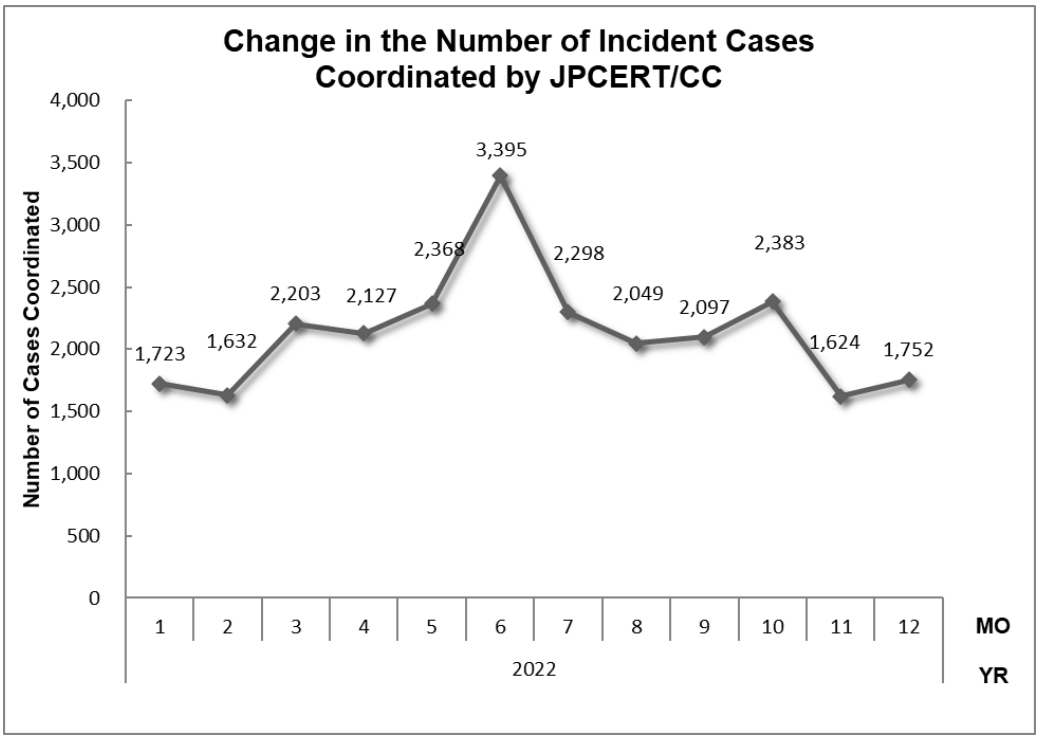
(3) "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

(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 11,923. Of these, the number of cases that JPCERT/CC coordinated was 5,759. When compared with the previous quarter, the total number of reports decreased by 12%, and the number of cases coordinated decreased by 11%. Year on year, the number of reports was roughly the same, and the number of cases coordinated decreased by 12%.
[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]

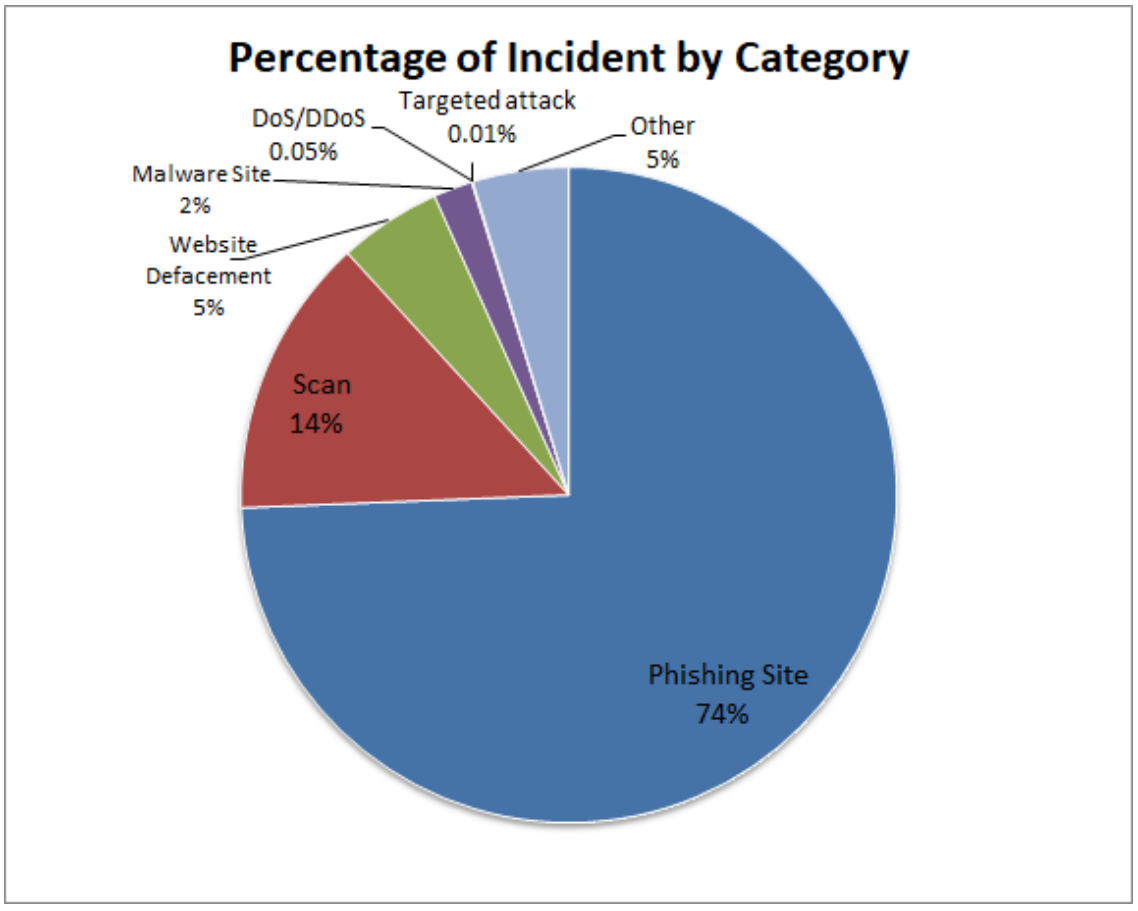


[Figure 2: Change in the number of incident cases coordinated]

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]

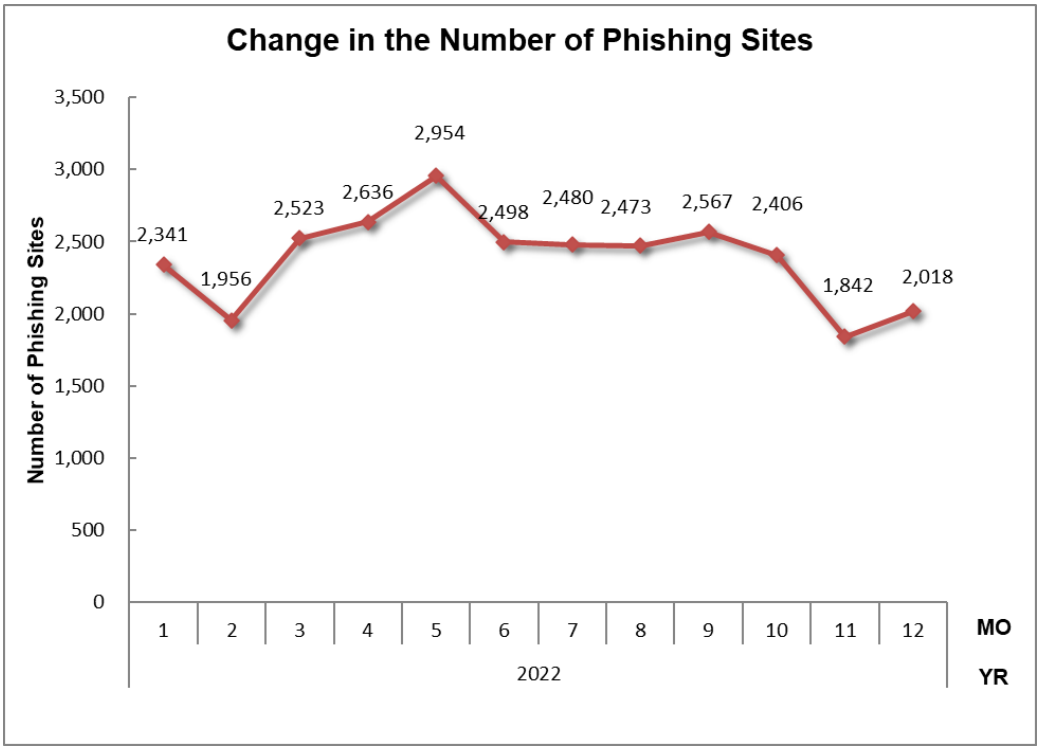
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	2,406	1,842	2,018	6,266	7,520
Website Defacement	253	94	80	427	695
Malware Site	83	36	43	162	199
Scan	443	339	384	1,166	1,917
DoS/DDoS	0	4	0	4	8
ICS Related	0	0	0	0	0
Targeted attack	0	0	1	1	2
Other	89	137	173	399	315



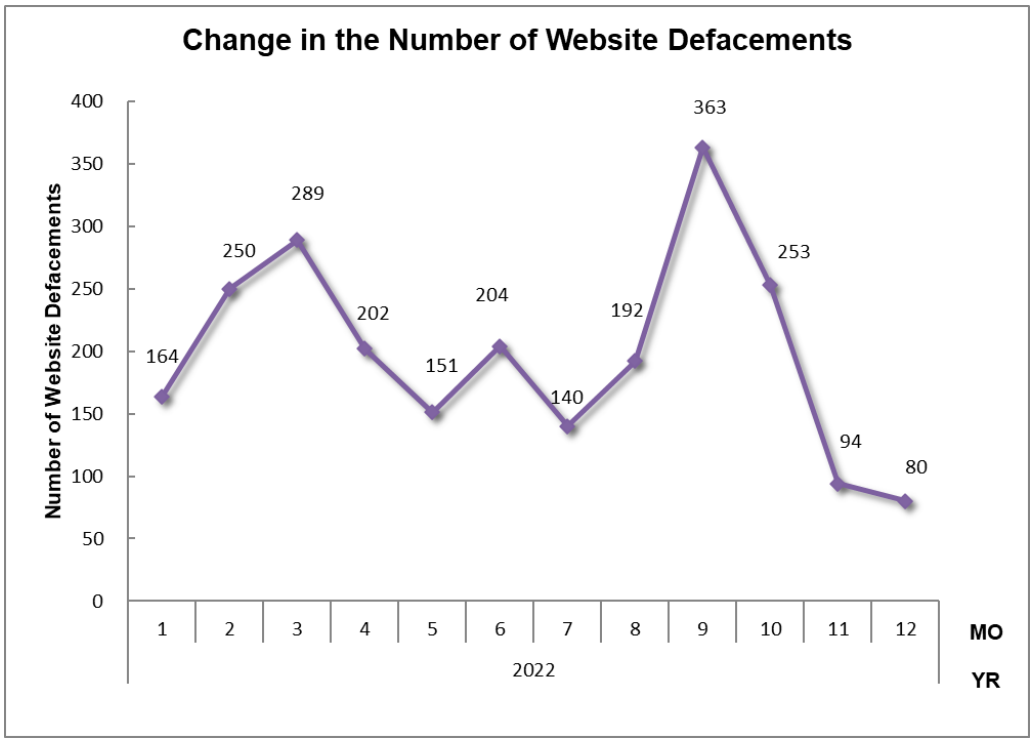
[Figure 3：Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 74%, and those categorized as scans, which search for vulnerabilities in systems, made up 14%.

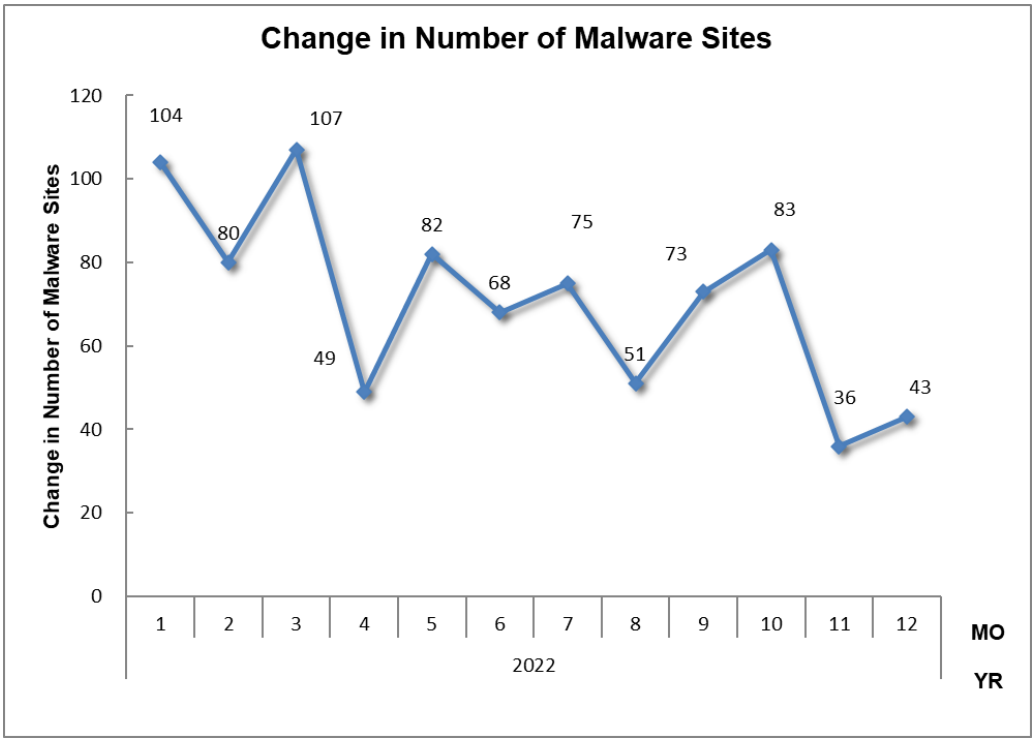
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



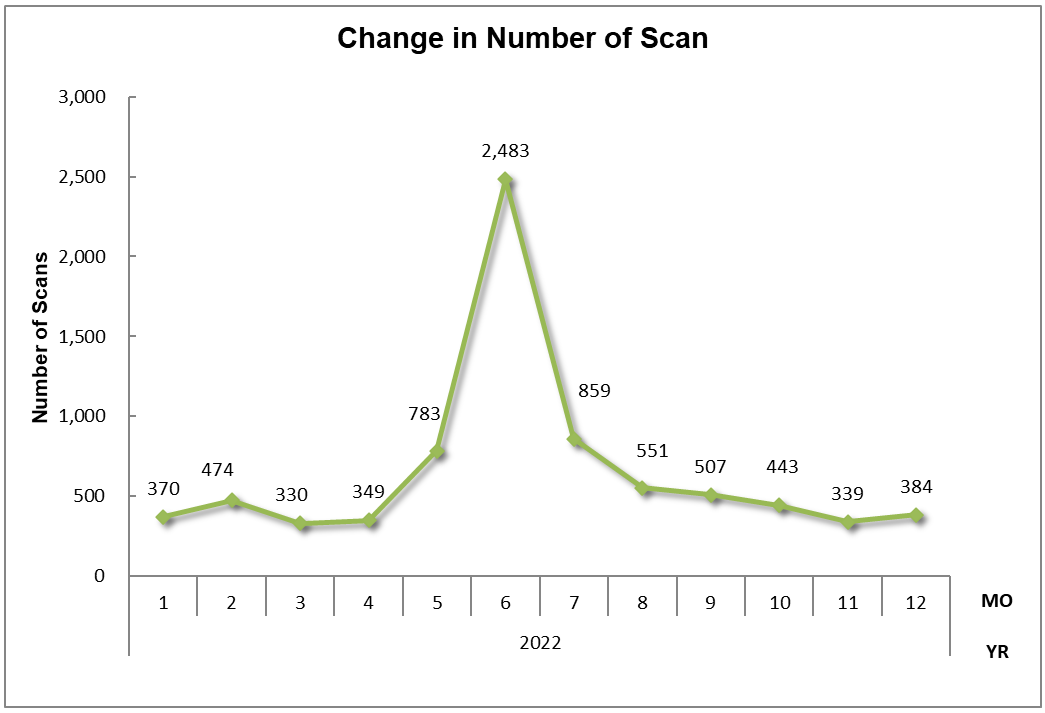
[Figure 4：Change in the number of phishing sites]



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

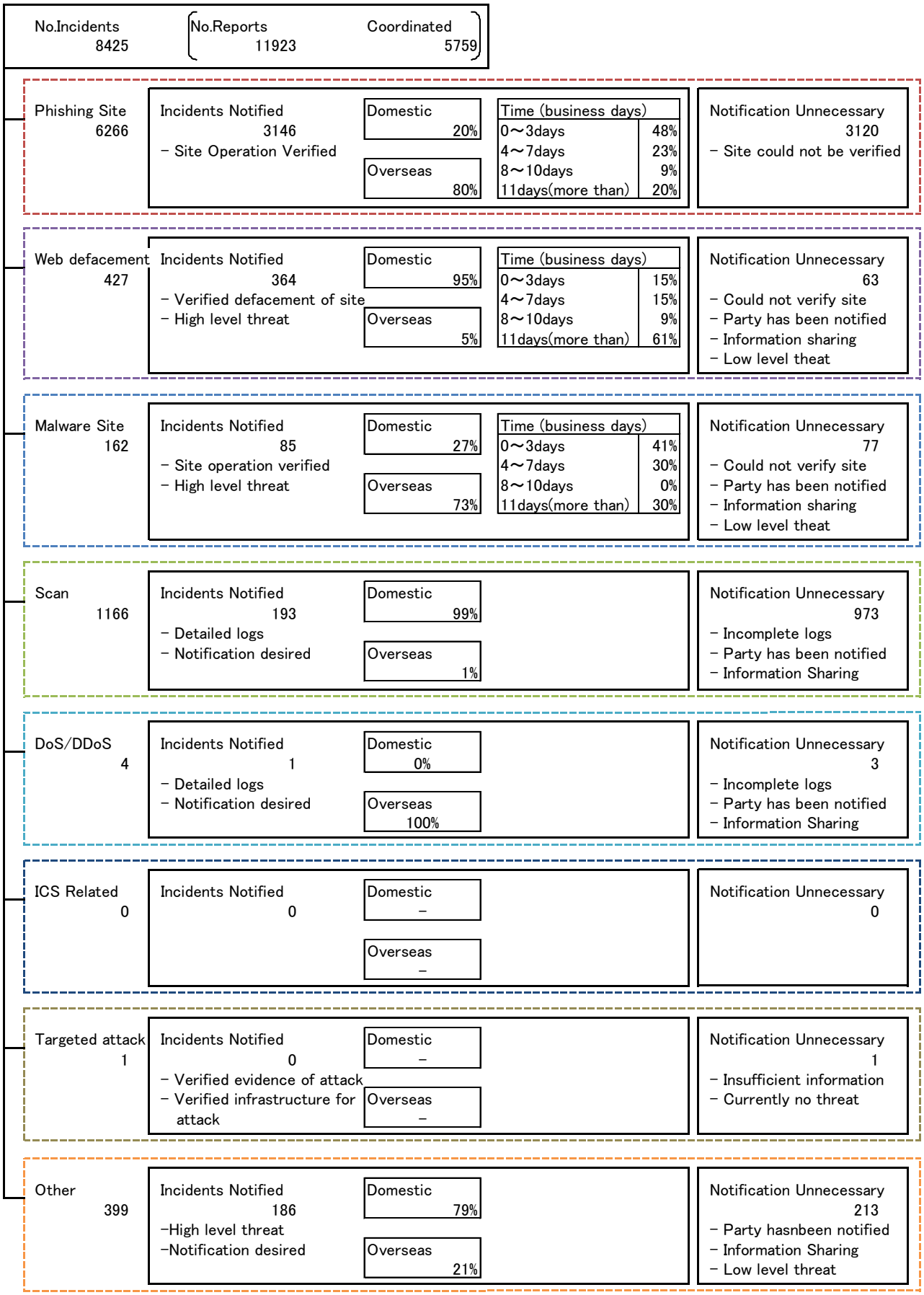


[Figure 6：Change in the number of malware sites]



[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

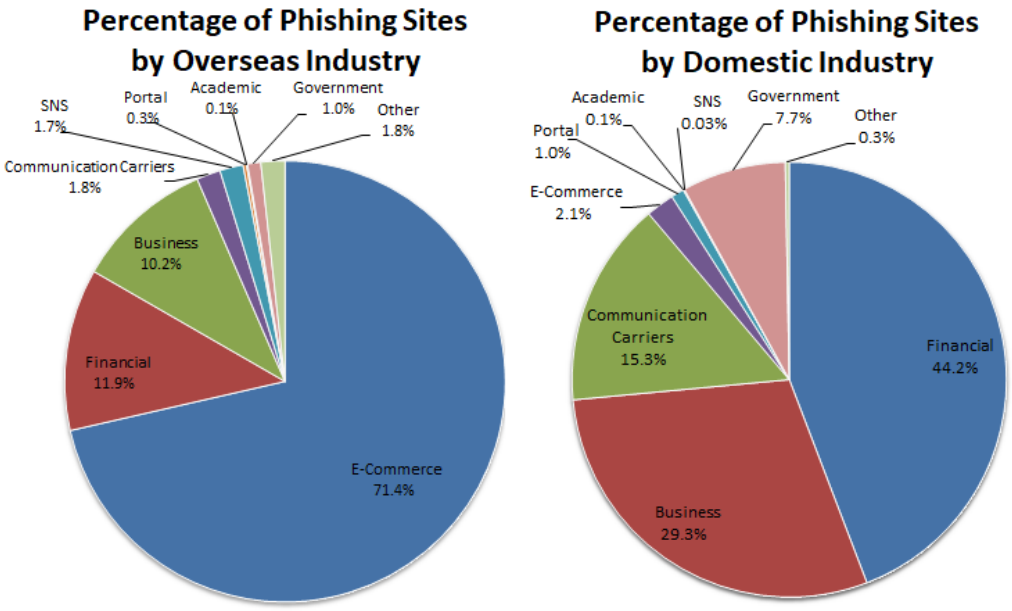
During this quarter, 6,266 reports on phishing sites were received, representing a 17% decrease from 7,520 in the previous quarter. This marks a 12% decrease from the same quarter last year (7,125).

During this quarter, there were 3,413 phishing sites that spoofed domestic brands, decreasing 19% from 4,191 in the previous quarter. There were 2,390 phishing sites that spoofed overseas brands, decreasing 10% from 2,662 in the previous quarter. A breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 3], and a breakdown by industry for domestic and overseas brands is shown in [Figure 9].

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

Phishing Site	Oct	Nov	Dec	Domestic/Overseas Total (%)
Domestic Brand	1,413	888	1,112	3,413(54%)
Overseas Brand	850	773	767	2,390(38%)
Unknown Brand(5)	143	181	139	463(7%)
Monthly Total	2,406	1,842	2,018	6,266

(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, 71.4% spoofed e-commerce websites for overseas brands and 11.9% spoofed financial institution 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, there were numerous phishing sites spoofing East Japan Railway Company's Eki-Net website and the National Tax Agency of Japan, and phishing sites spoofing Electronic Toll Collection (ETC) system usage inquiry services and Rakuten/Rakuten Card continued to be reported in large numbers.

JPCERT/CC confirmed that Rebrandly, a URL shortening service, was being used to redirect users to phishing sites spoofing Amazon, Sumitomo Mitsui Card, and Aeon Card.

The websites that JPCERT/CC coordinated with to take down phishing sites were 20% domestic and 80% overseas for this quarter, indicating an increase in overseas parties compared to the previous quarter (domestic: 28%, overseas: 72%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 427. This was a 39% decrease from 695 in the previous quarter.

This quarter, there were a number of cases in which legitimate websites using CMS were compromised. JPCERT/CC confirmed that obfuscated JavaScript as shown in [Figure 10] were inserted in the compromised websites. This script is designed to steal credit card information, etc. entered on the website.

```
eval(function(p,a,c,k,e,r)
{e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String))
```

[Figure 10: Part of an obfuscated script]

The defacement of the compromised websites was carried out by the use of stolen CMS administrative user credentials or exploitation of vulnerabilities in plugins, etc.

3.3. Targeted Attack Trends

There was 1 incident categorized as a targeted attack. The incident identified is described below.

(1) Attacks attempting to lure targets into downloading a malicious help file via LinkedIn

This quarter, JPCERT/CC received reports of attacks apparently targeting the employees of cryptocurrency exchanges. The confirmed method involved contacting target employees via LinkedIn, exchanging a few chat messages, and finally sending an archive file containing malware. This archive file contains a help file (.chm) that, when executed, causes an MSI file to be downloaded from an external server and executed. JPCERT/CC confirmed that the downloaded MSI file contains functions for collecting information about the infected device.

Similar cases of targeted attacks via LinkedIn were seen in the last fiscal year as well, so similar attacks may continue to be seen in the future.

Quarterly Report of JPCERT/CC Activities [January 1, 2022 – March 31, 2022] (Japanese)
https://www.jpcert.or.jp/pr/2022/PR_Report2021Q4.pdf

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 162. This was a 19% decrease from 199 in the previous quarter.

The number of scans reported in this quarter was 1,166. This was a 39% decrease from 1,917 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), 5060/UDP, Telnet (23/TCP) and IMAP (143/TCP).

[Chart 4：Number of scans by port]

Port	Oct	Nov	Dec	Total
22/tcp	191	186	232	609
5060/udp	85	60	24	169
23/tcp	33	25	72	130
143/tcp	74	25	28	127
80/tcp	18	19	20	57
37215/tcp	32	4	3	39
25/tcp	5	17	9	31
443/tcp	4	1	0	5
445/tcp	3	0	1	4
9530/tcp	1	0	0	1
Others	1	2	3	6
Monthly Total	447	339	392	1178

There were 399 incidents categorized as other. This was a 27% increase from 315 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 reports of human-operated ransomware attacks

This quarter, JPCERT/CC continued to receive a number of reports of human-operated ransomware attacks. Cases in which the attacker appears to have exploited vulnerabilities in SSL-VPN products or Log4j to break into an organization's network have been confirmed. In some of the cases where SSL-VPN products were used as an entry point, the products already had a fix (patch) applied to address the vulnerabilities at the time of intrusion, but the attacker used credentials they had stolen before the fix was applied to gain access to the network. Some of the groups reported as carrying out human-operated ransomware attacks include TargetCompany and BianLian.

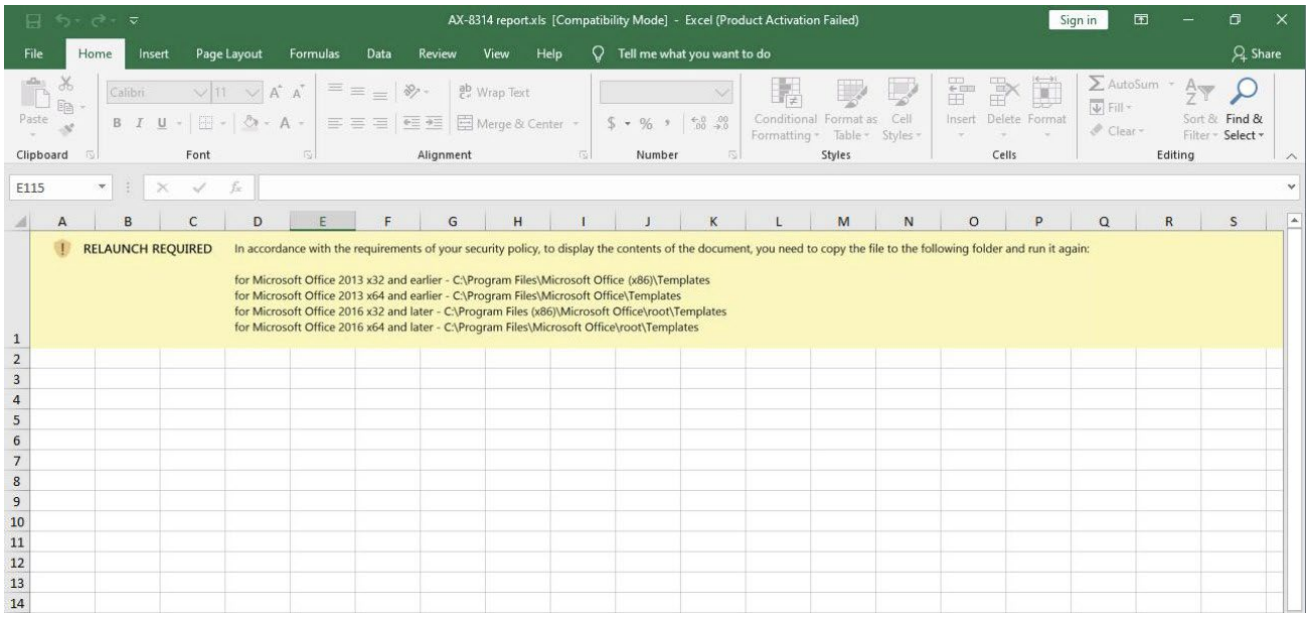
JPCERT/CC has released an FAQ and video summarizing the initial response that should be taken when subjected to a human-operated ransomware attack. Please use these resources for reference when subjected to an attack.

FAQ to read when subjected to a human-operated ransomware attack (Japanese)
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

Key points of initial response to a human-operated ransomware attack (webinar) (Japanese)
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) Coordination involving reports of Emotet malware

JPCERT/CC has confirmed that a malicious e-mail campaign attempting to cause Emotet infections has been resumed since November 2, 2022. As a result, JPCERT/CC received numerous reports related to Emotet this quarter. As shown in [Figure 11], an Excel file attached to a suspicious e-mail contained instructions to copy the file to a specific folder (a trusted location for Office files) and run it. It is assumed that this is intended to ensure malicious macros will be executed even when macros are disabled, since the folder to which the recipient is instructed to copy the file is configured as a "trusted location" by default.



[Figure 11: Excel file instructing the recipient to copy the file to a specific place and run it]

Given the spread of Emotet infections in Japan, JPCERT/CC released the following security alert.

Security alert concerning resumed e-mail campaign leading to Emotet malware infections (Japanese)
https://www.jpcert.or.jp/tips/2022/wr224401.html

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.