JPCERT/CC Incident Handling Report

April 1, 2021 ～ June 30, 2021

JPCERT Coordination Center

July 15, 2021

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 April 1, 2021 through June 30 , 2021

[*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]

	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports *2	3,036	3,149	4,089	10,274	9,629
Number of Incident *3	2,399	2,299	2,279	6,977	7,108
Cases Coordinated *4	1,341	1,068	1,336	3,745	4,005

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

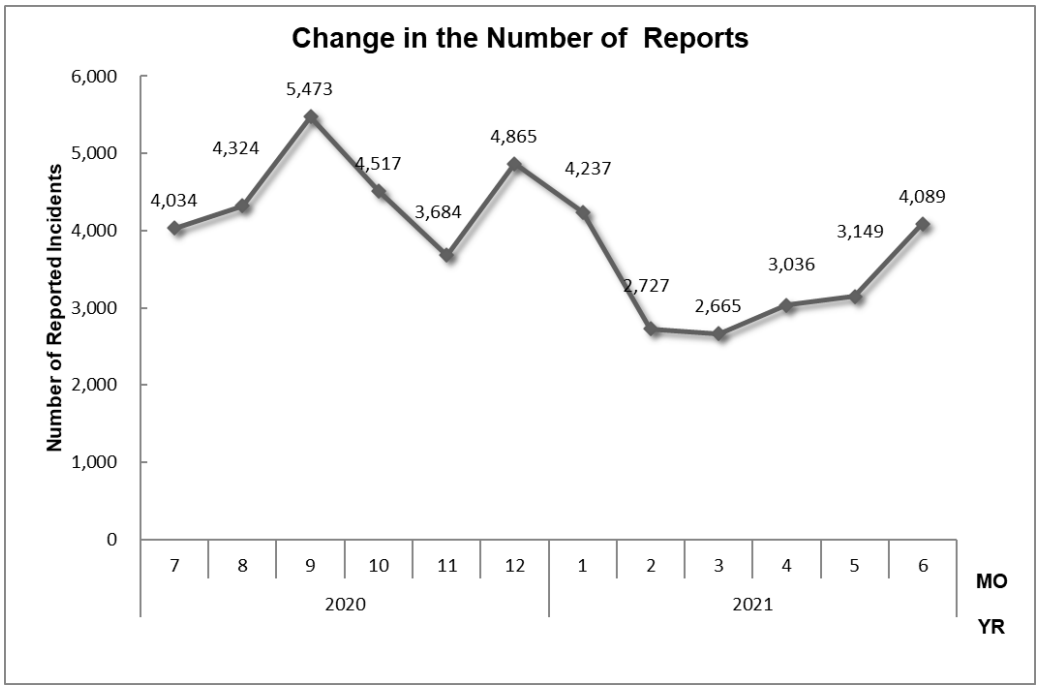
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

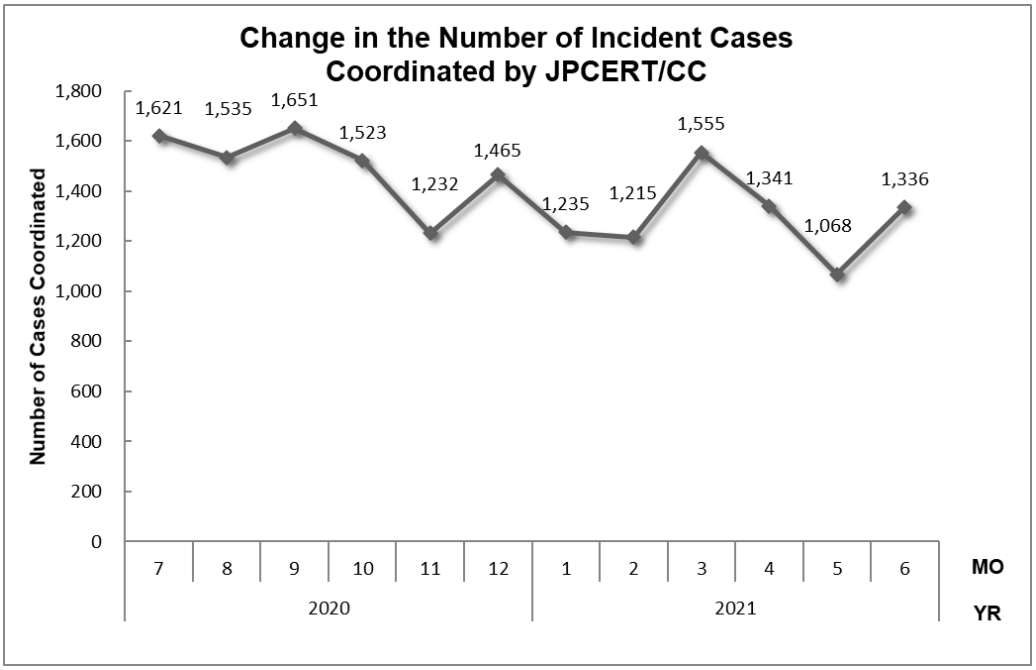
The total number of reports received in this quarter was 10,274. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 3,745. When compared with the previous quarter, the total number of reports increased by 7%, and the number of cases coordinated decreased by 6%. Year on year, the number of reports decreased by 1.4%, and the number of cases coordinated decreased by

11%.

[Figure 1] and [Figure 2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC.



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

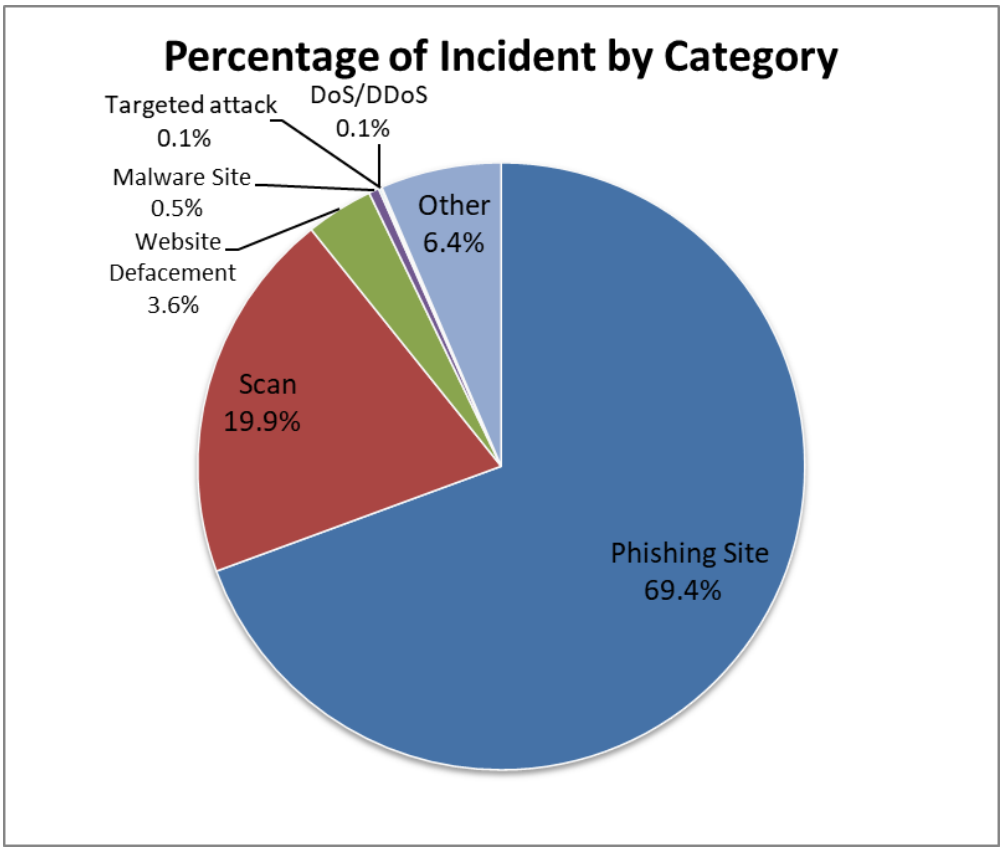


[Figure 2 : Change in the number of incident cases coordinated]

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 the number of incidents received per category in this quarter. The breakdown in percentage is shown in [Figure 3].

[Chart 2 : Number of incidents by category]

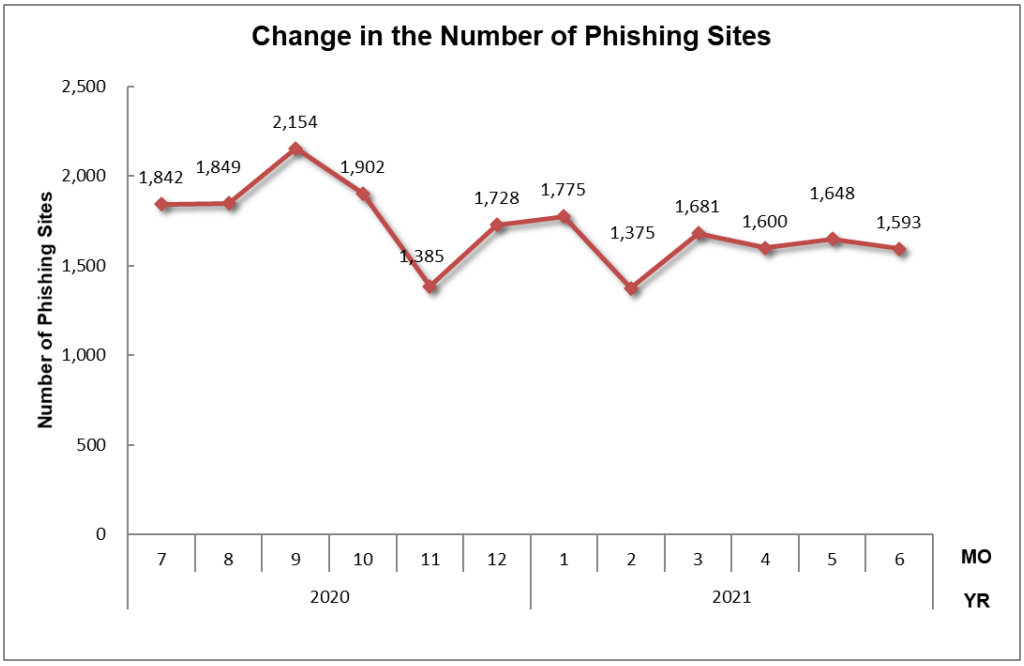
Incident Category	Apr	May	Jun	Total	Last Qtr.Total
Phishing Site	1,600	1,651	1,593	4,841	4,831
Website Defacement	65	79	107	251	282
Malware Site	12	8	18	38	138
Scan	561	430	394	1,385	1,085
DoS/DDoS	3	4	1	8	2
ICS Related	0	0	0	0	0
Targeted attack	4	1	0	5	7
Other	154	126	166	449	763



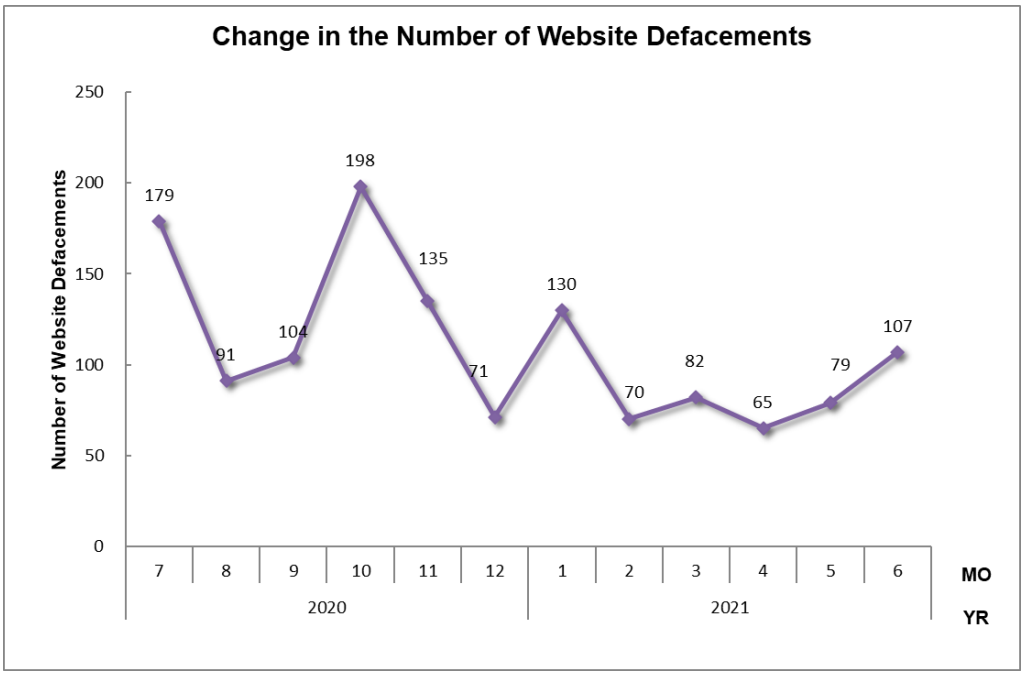
[Figure 3 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 69.4%, and those categorized as scans, which search for vulnerabilities in systems, made up 19.9%.

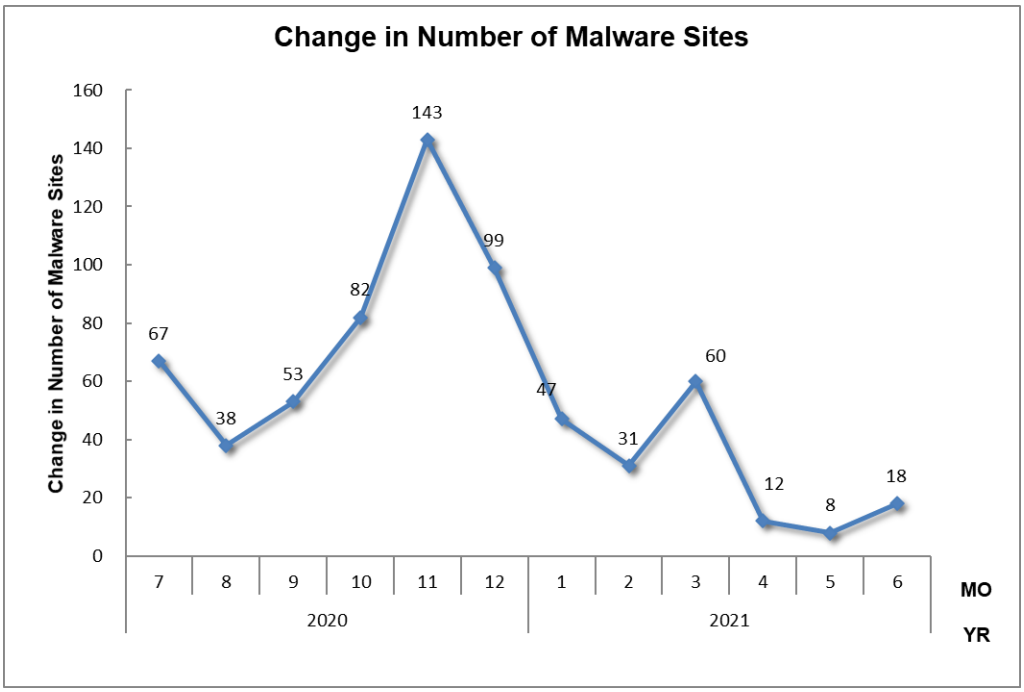
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



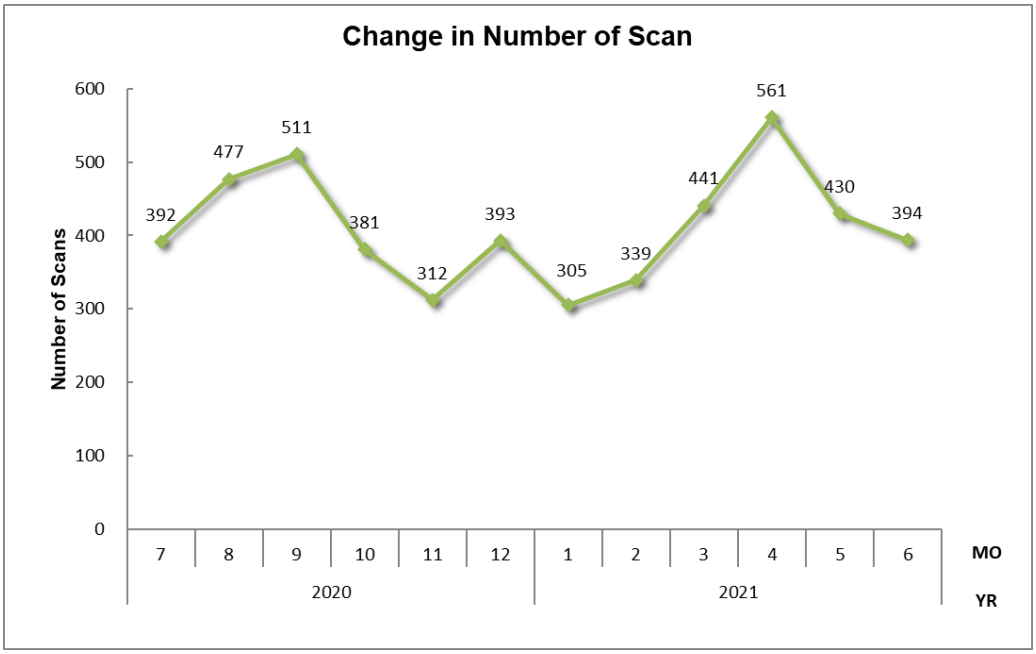
[Figure 4 : Change in the number of phishing sites]



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

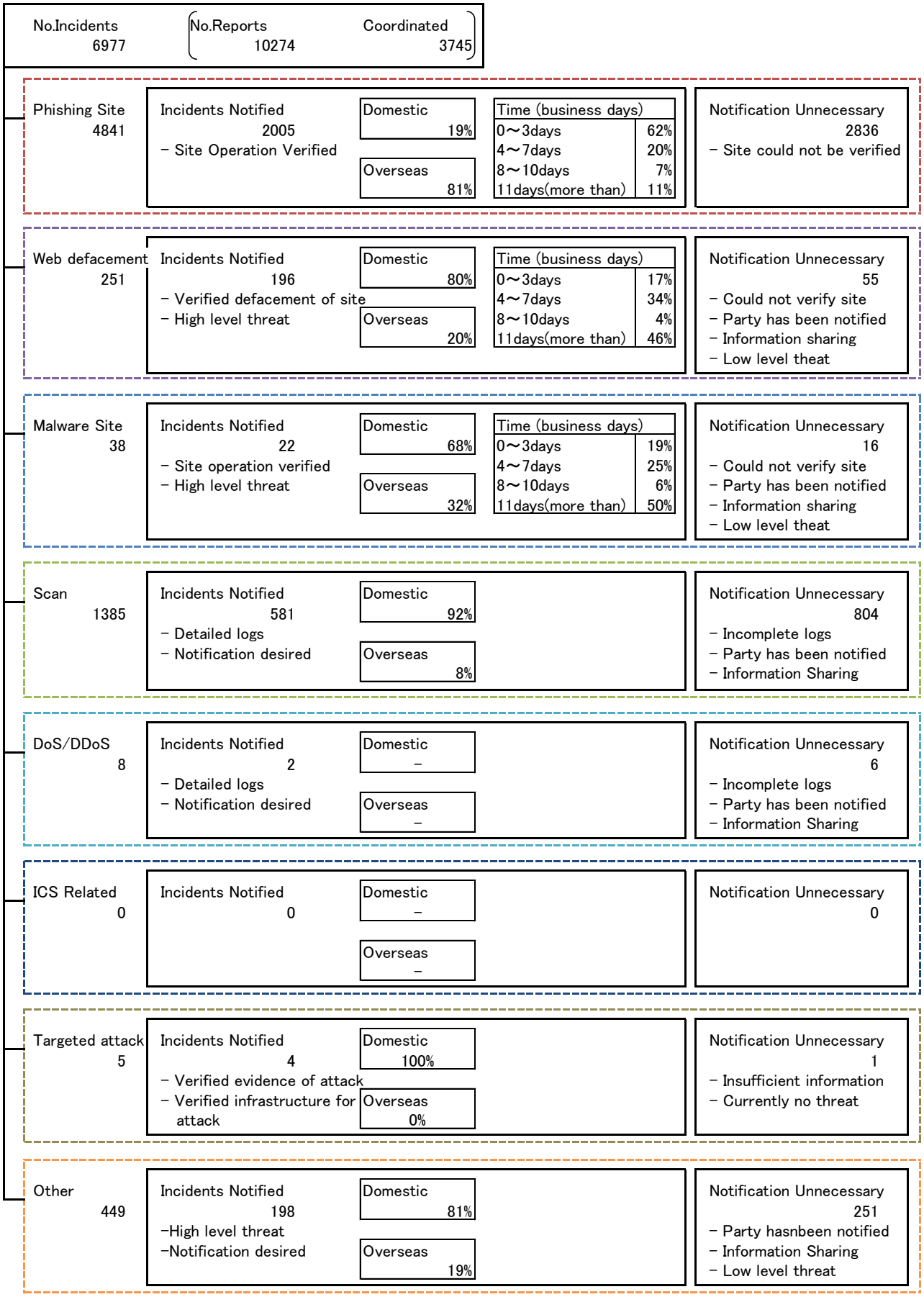


[Figure 6 : Change in the number of malware sites]



[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

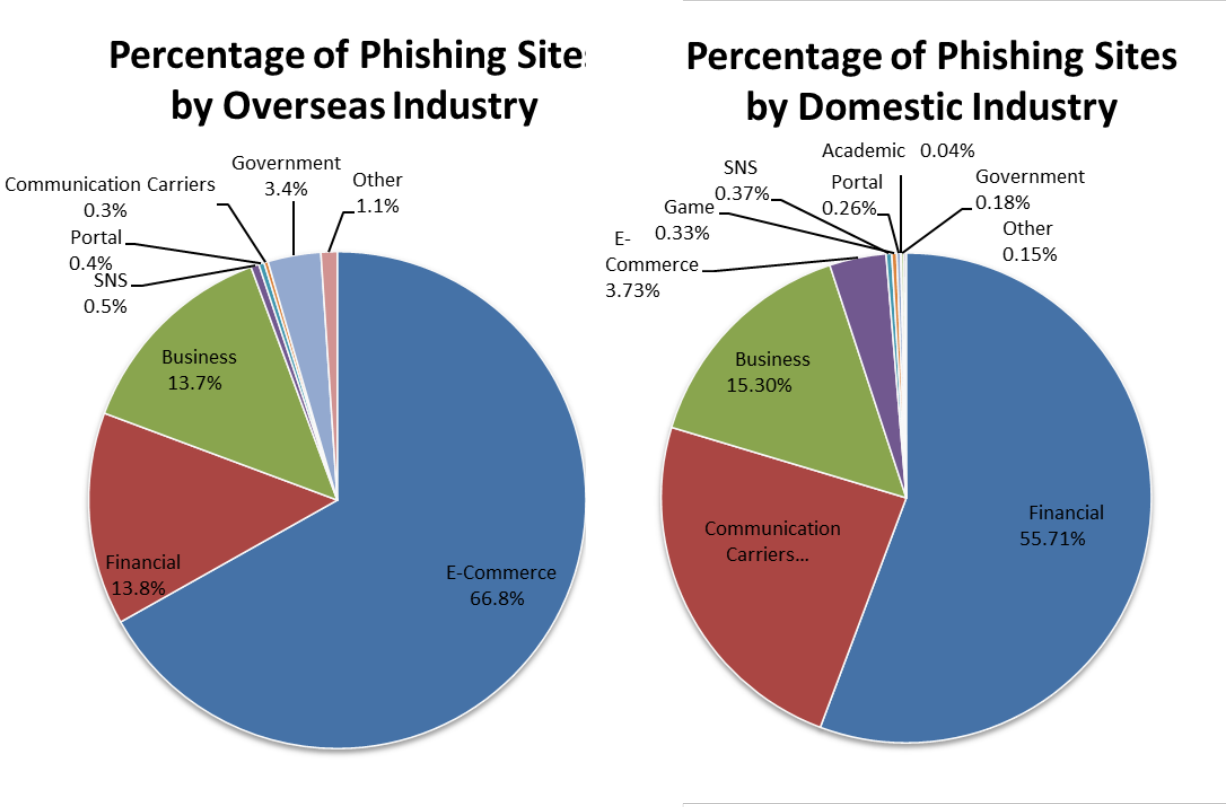
During this quarter, 4,841 reports on phishing sites were received, which is roughly the same as 4,831 in the previous quarter. This marks an 8% decrease from the same quarter last year (5,262).

During this quarter, there were 2,732 phishing sites that spoofed domestic brands, increasing 6% from 2,585 in the previous quarter. And there were 1,134 phishing sites that spoofed overseas brands, decreasing 33% from 1,700 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	Apr	May	Jun	Domestic/Overseas Total (%)
Domestic Brand	894	817	1,021	2,732（56%）
Overseas Brand	479	431	223	1,134（23%）
Unknown Brand [*5]	227	403	349	975（20%）
Monthly Total	1,600	1,651	1,593	4,841

[*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, 66.8% spoofed e-commerce websites for overseas brands and 55.7% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

The number of reports on phishing sites received this quarter was roughly the same as in the previous quarter. For overseas brands, there were many phishing sites spoofing specific online shopping websites and financial institutions. The number of phishing sites spoofing telecommunications carrier websites for members showed an upward trend.

Many of the phishing sites used .com, .cn, .xyz and .top domains containing random strings. There were also cases in which multiple phishing sites spoofing different brands were set up on a single server, with each website containing strings resembling the domains of legitimate sites in the subdomain.

During this quarter, there were also many reports of phishing sites using Duck DNS. Duck DNS, a free dynamic DNS service, often causes websites to become inaccessible in a short time. Depending on when the website was accessed, maintenance screens and rooter administration screens were displayed in some cases.

The parties that JPCERT/CC contacted for coordination of phishing sites were 19% domestic and 81% overseas for this quarter, indicating an increase in overseas parties compared to the previous quarter (domestic: 23%, overseas: 77%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 251. This was an 11% decrease from 282 in the previous quarter.

During this quarter, JPCERT/CC received multiple reports of being redirected from compromised websites to scam sites and suspicious websites selling merchandise. Compromised websites were planted with a malicious PHP script, which is used to create numerous fraudulent pages. [Figure 10] shows an example of a lucky visitor scam page that is displayed when one of the fraudulent pages is accessed.

[Figure 10 : Example of a scam site]

[Figure 11] illustrates the flow of events that is triggered by accessing a fraudulent page and ends in the visitor being redirected to a scam site.

[Figure 11：Flow of events]

When a compromised website is accessed, the visitor's information is sent to the attacker's server. Next, the attacker's server returns a redirect URL based on the visitor's information, and the compromised website ultimately redirects the visitor to this URL. Details of this attack are discussed on JPCERT/CC Eyes.

JPCERT/CC Eyes : PHP Malware Used in Lucky Visitor Scam
https://blogs.jpcert.or.jp/en/2021/06/php_malware.html

3.3. Targeted Attack Trends

There were 5 incidents categorized as a targeted attack. This was a 29% decrease from 7 in the previous quarter. The incidents identified are described below.

(1) Attacks using LODEINFO malware

This quarter, JPCERT/CC continued to receive reports of targeted attacks using the LODEINFO malware. The LODEINFO malware infects computers when a Word file attached to a targeted attack e-mail is opened, and the malicious macro contained in the file is executed.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 38. This was a 72% decrease from 138 in the previous quarter.

The number of scans reported in this quarter was 1,385. This was a 28% increase from 1,085 in the previous quarter. A breakdown of the ports that were scanned are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), IMAP (143/TCP) and 9530/TCP.

[Chart 4 : Number of scans by port]

Port	Apr	May	Jun	Last Qtr. Total
22/tcp	97	134	102	333
143/tcp	252	68	11	331
9530/tcp	0	42	135	177
80/tcp	45	50	30	125
23/tcp	60	34	26	120
62223/tcp	26	24	39	89
443/tcp	18	24	23	65
37215/tcp	45	13	1	59
445/tcp	6	9	10	25
2323/tcp	10	10	1	21
25/tcp	1	9	7	17
1433/tcp	5	9	3	17
8080/tcp	4	5	0	9
6379/tcp	1	3	5	9
52869/tcp	4	1	1	6
3389/tcp	3	1	1	5
26/tcp	5	0	0	5
21/tcp	1	3	1	5
8000/tcp	1	3	0	4
Unknown	9	25	11	45
Monthly Total	593	467	407	1467

There were 449 incidents categorized as other. This was a 41% decrease from 763 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 an incident exploiting an XSS vulnerability on a website using EC-CUBE

This quarter, JPCERT/CC received a report concerning information leakage from an e-commerce site using EC-CUBE. As a result of an investigation, it was found that the website had been compromised by exploiting a cross site scripting vulnerability, and suspicious code that steals credentials had been inserted on the administrator screen.

JPCERT/CC confirmed that the compromised website was embedded with malicious code that steals site users' IDs, passwords and credit card information, and a WebShell that manipulates its database.

Based on this report, JPCERT/CC exchanged information with EC-CUBE Co., Ltd. about Indicators of Compromise (IoC), specific details of attack and various logs. Since multiple cases of damage were confirmed in Japan, and the source IP address used to access the WebShell placed by the attacker was identical in all cases, JPCERT/CC issued the following alert on Twitter.

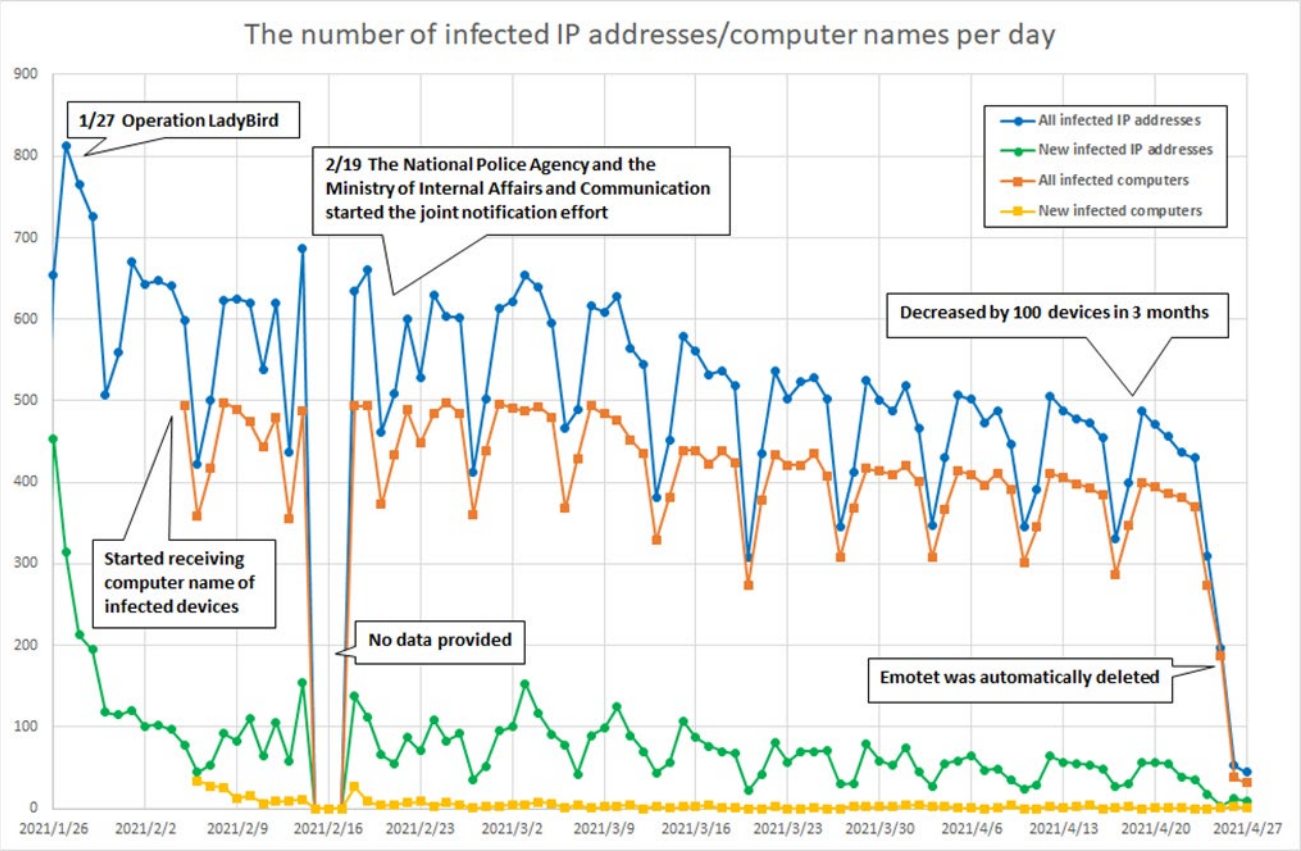
EC-CUBE alert on Twitter (Japanese)
https://twitter.com/jpcert_ac/status/1399604992059744256

These attacks can be countered by updating EC-CUBE and EC-CUBE plugins to the latest version. Users of the EC-CUBE 4.0 series should read the following alert regarding the vulnerability in EC-CUBE and take appropriate steps.

Alert Regarding Cross Site Scripting Vulnerability (CVE-2021-20717) in EC-CUBE
https://www.jpcert.or.jp/english/at/2021/at210022.html

(2) Results of notification to computers infected with Emotet malware

After the Emotet botnet was taken down, JPCERT/CC received information about computers infected with Emotet from related organizations. Since computers infected with Emotet might be infected with another type of malware downloaded by Emotet, JPCERT/CC continued to send notifications in cooperation with ISPs and other parties until April 25, 2021, when Emotet was automatically deleted. As shown in [Figure 12], measures were taken with about 100 computers during a period of roughly 3 months from around February when the notification began until April 25, and very few Emotet infections are observed from April 26 onward.



[Figure 12：Changes in the numbers of computers infected with Emotet in Japan (end of April 2021)]

Results of these notification activities are discussed in detail on JPCERT/CC Eyes.

JPCERT/CC Eyes : Emotet Disruption and Outreach to Affected Users
https://blogs.jpcert.or.jp/en/2021/02/emotet-notice.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 2021 Fiscal Year".