JPCERT/CC Incident Handling Report

April 1, 2020 ～ June 30 , 2020

JPCERT Coordination Center

July 14, 2020

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, 2020 through June 30 , 2020

.

[*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	3,105	3,256	4,055	10,416	6,361
Number of Incident *3	2,221	2,277	2,625	7,123	5,509
Cases Coordinated *4	1,480	1,173	1,548	4,201	4,107

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

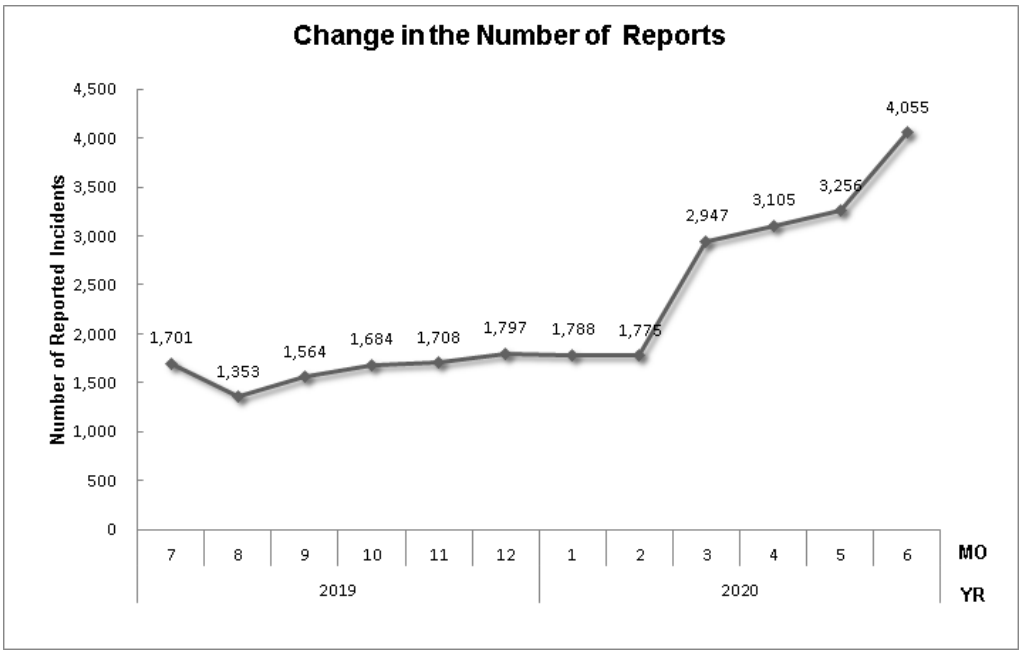
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

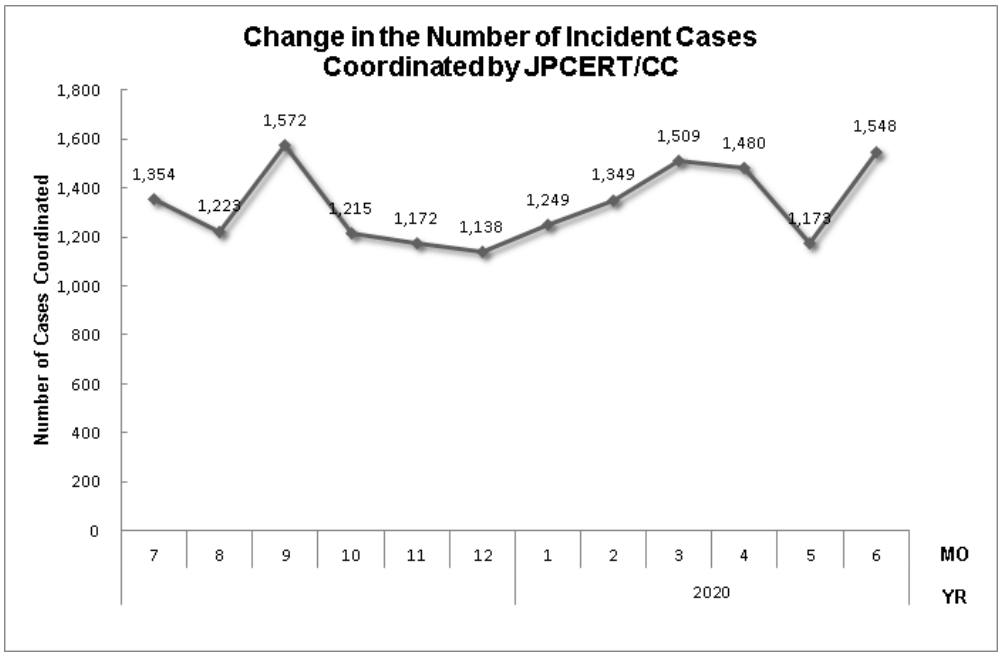
The total number of reports received in this quarter was 10,416. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,201. When compared with the previous quarter, the total number of reports increased by 60%, and the number of cases coordinated increased by 2%.

Year on year, the number of reports increased by 172%, and the number of cases coordinated increased by 50%.

[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]

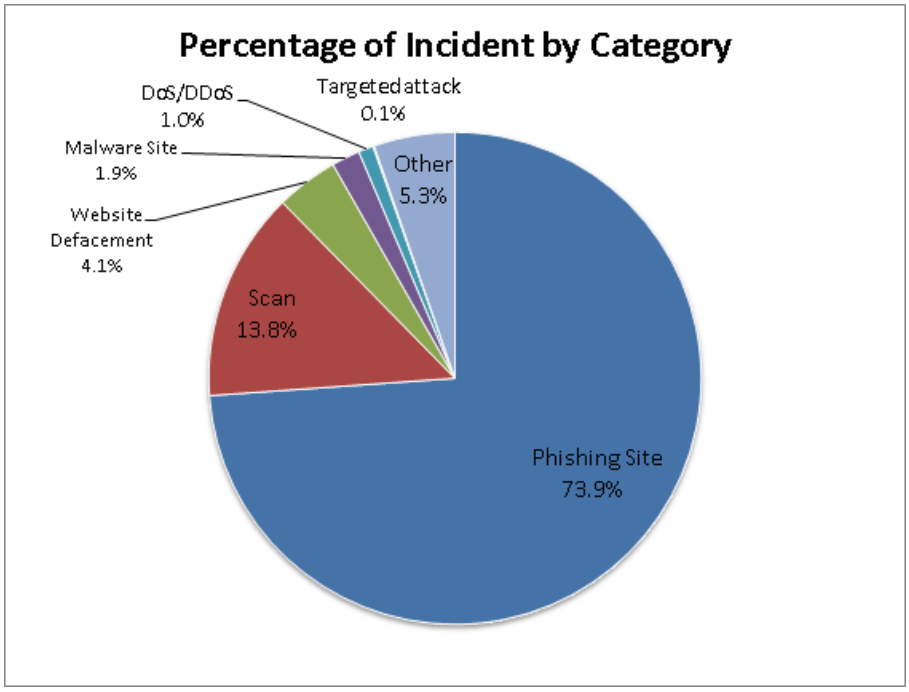


[Figure 2: Change in the number of incident cases coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on each incident category, please see "Appendix 1 - Incident Categories." [Chart 2] shows the number of incidents received per category in this quarter. The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3].

[Chart 2 : Number of incidents by category]

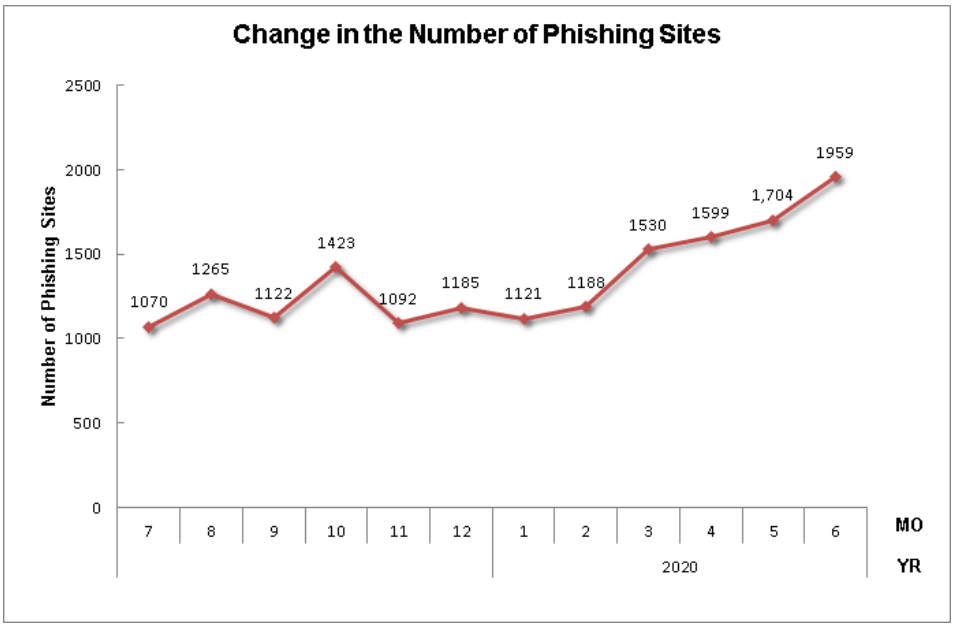
Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	1,599	1,704	1,959	5,262	3,839
Website Defacement	50	95	146	291	192
Malware Site	53	43	37	133	250
Scan	348	286	348	982	713
DoS/DDoS	54	0	16	70	21
ICS Related	0	0	0	0	0
Targeted attack	2	2	2	6	2
Other	115	147	117	379	492



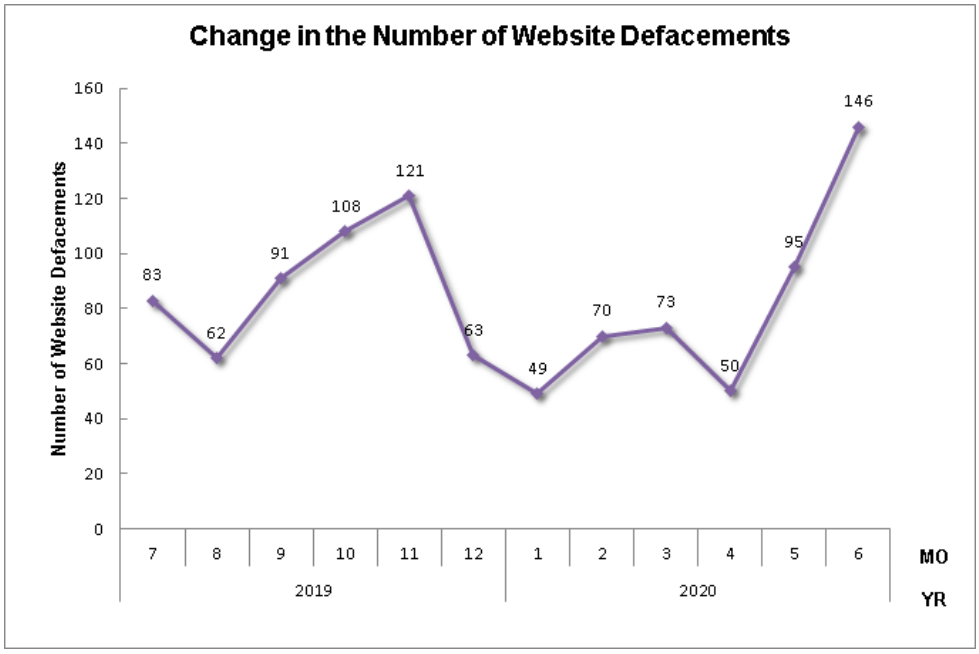
[Figure 3: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 73.9%, and those categorized as scans, which search for vulnerabilities in systems, made up 13.8%.

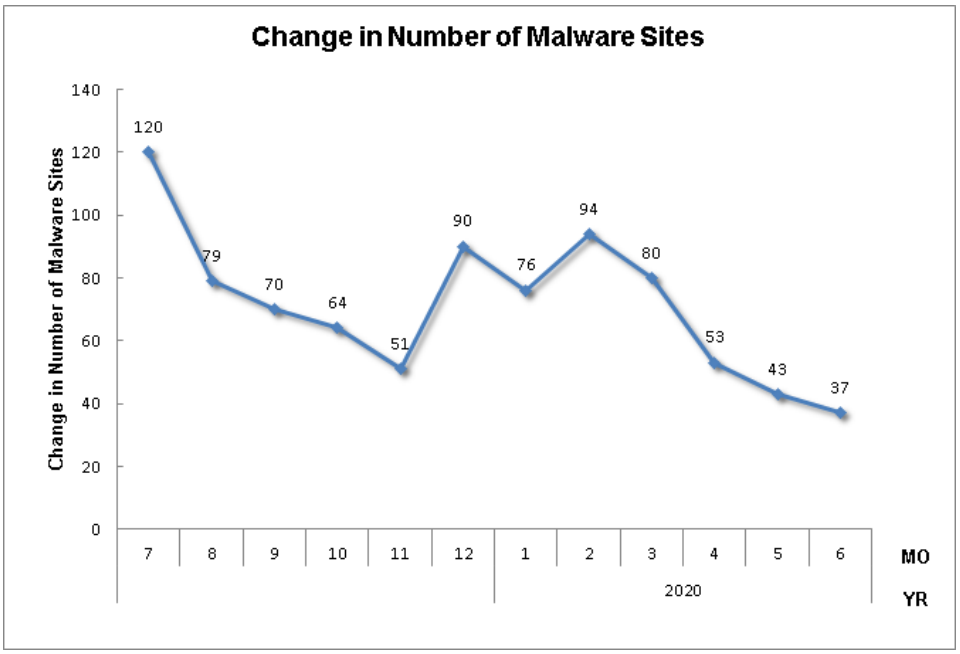
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



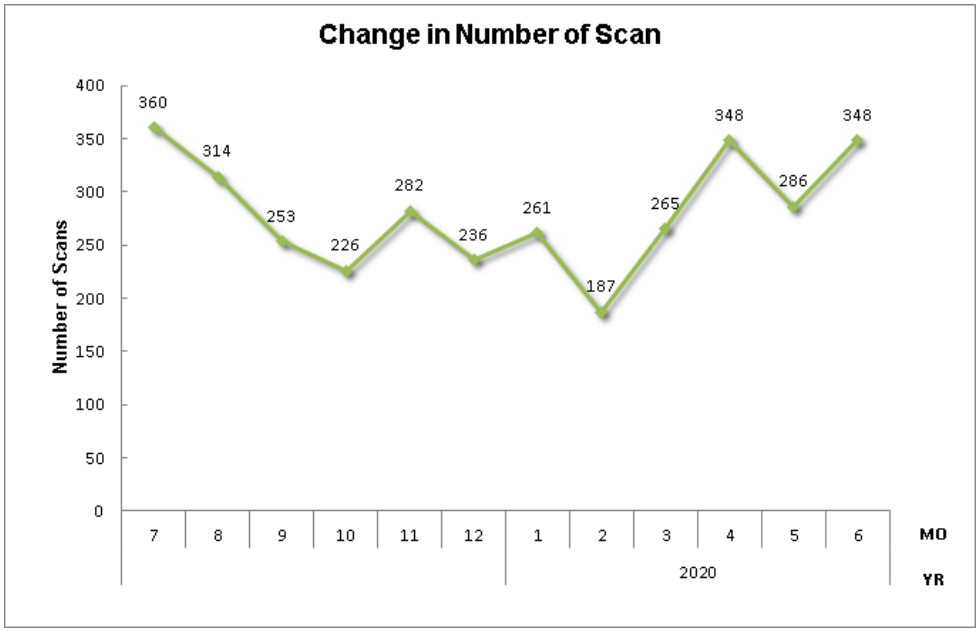
[Figure 4: Change in the number of phishing sites]



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

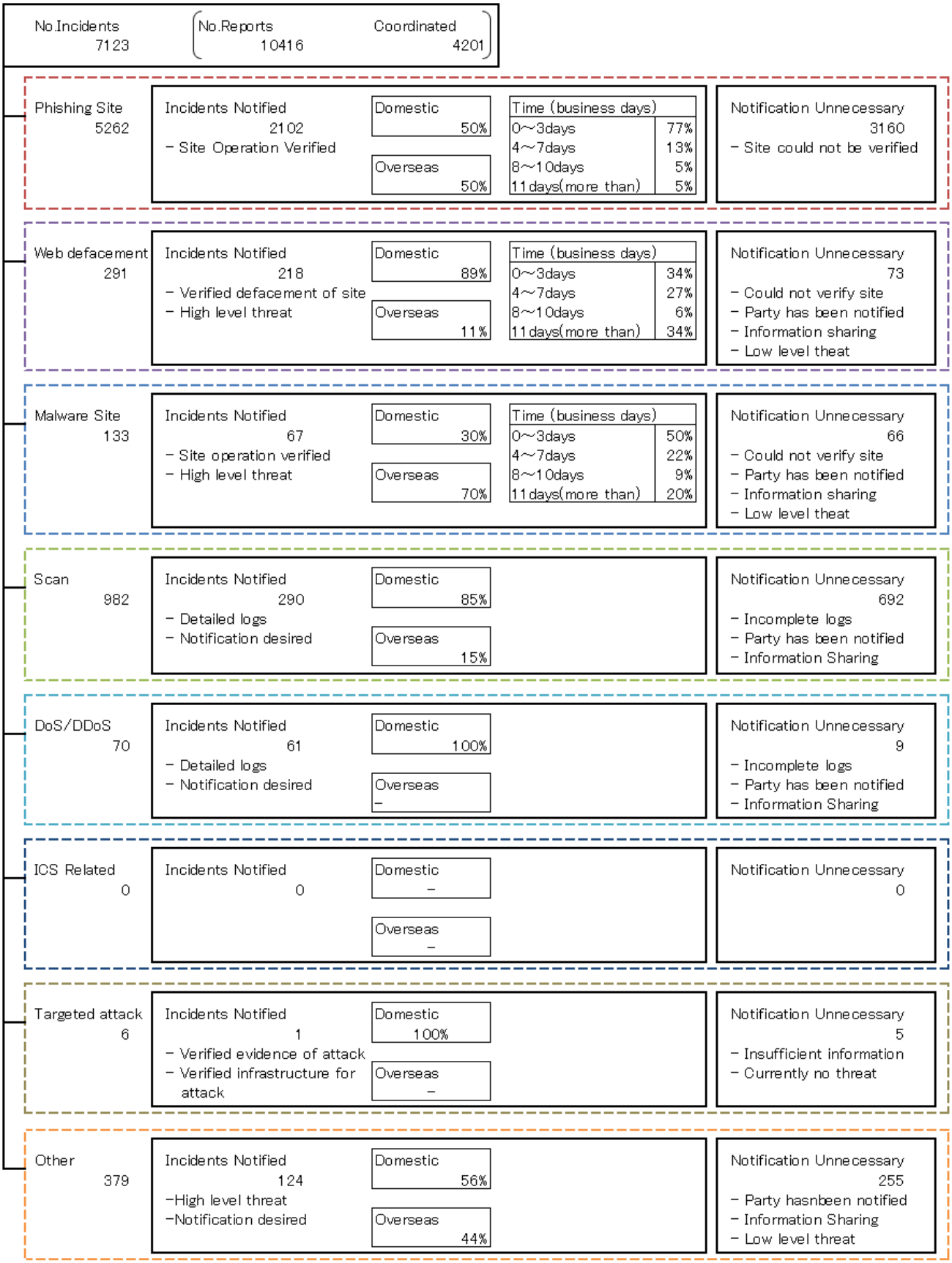


[Figure 6: Change in the number of malware sites]



[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

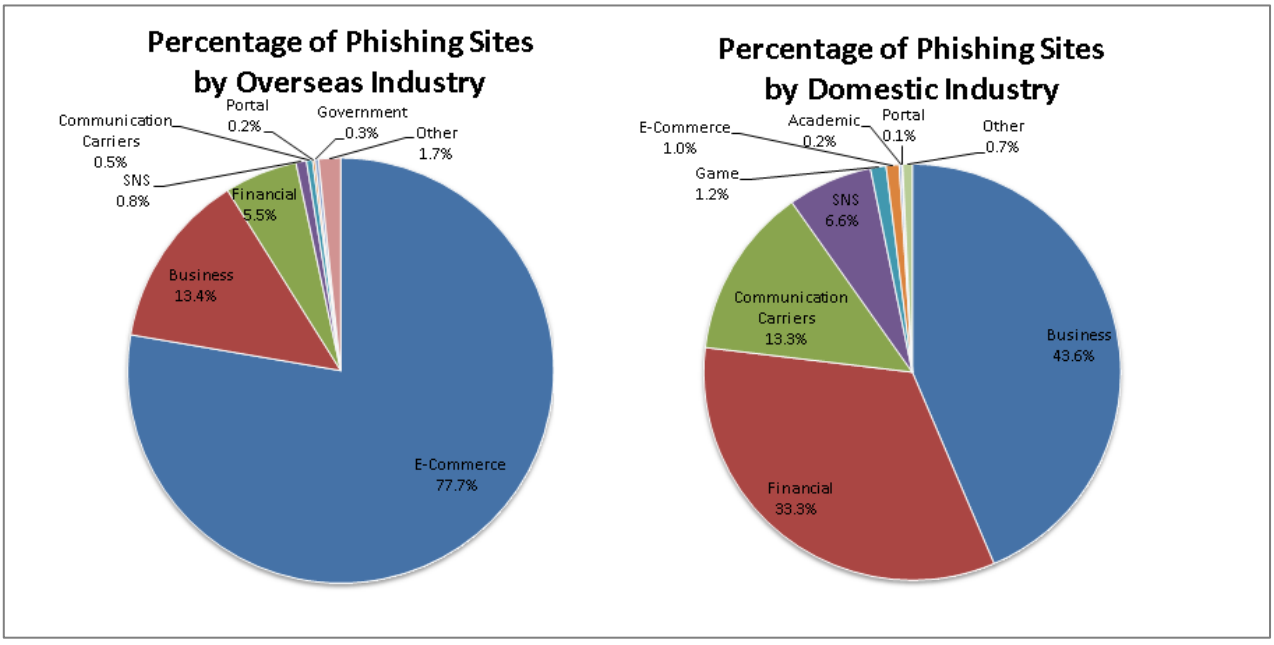
During this quarter, 5,262 reports on phishing sites were received, representing a 37% increase from 3,839 in the previous quarter. This marks a 170% increase from the same quarter last year (1,947).

During this quarter, there were 1,489 phishing sites that spoofed domestic brands, increasing 67% from 894 in the previous quarter. There were 3,265 phishing sites that spoofed overseas brands, increasing 32% from 2,474 in the previous quarter. The 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	542	396	551	1,489(28%)
Overseas Brand	892	1,153	1,220	3,265(62%)
Unknown Brand [*5]	165	155	188	508(10%)
Monthly Total	1,599	1,704	1,959	5,262

[*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, 77.7% spoofed e-commerce websites for overseas brands and 43.6% spoofed corporate websites for domestic brands, both representing the largest share respectively.

As in the previous quarter, there were many phishing sites spoofing e-commerce websites overseas, and many phishing sites spoofing corporate websites in Japan.

The URL of some of the phishing sites reported contained the word “COVID-19,” which is not in any way related to the brand, apparently in an attempt to draw the attention of the visitor.

E-mail is the primary method used to lure visitors to phishing sites spoofing e-commerce websites. Many such e-mails contained fraudulent messages that make it appear as if the login account has been misused, such as “Unauthorized login was detected. Please confirm” and “Your account has been locked. See the link for instructions on how to unlock your account,” along with a link to the phishing site.

Many of the phishing sites spoofing overseas brands used .com, .top and .buzz domains containing the domain and brand name of legitimate websites with alphanumeric characters added.
Some phishing sites were created using hosting services in Japan.

The parties that JPCERT/CC contacted for coordination of phishing sites were 50% domestic and 50% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 38%, overseas: 62%).

3.2. Website Defacement Trends

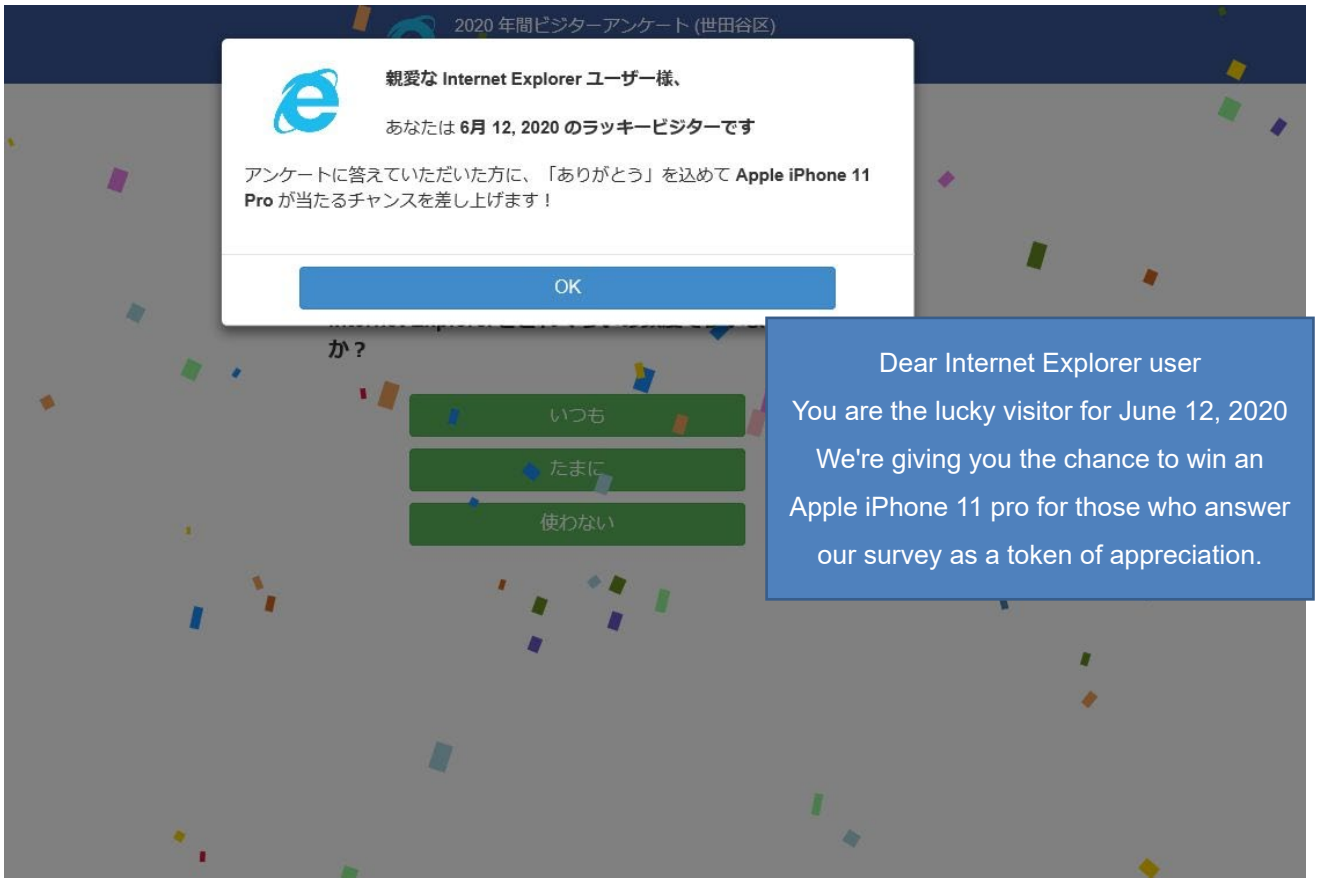
The number of website defacements reported in this quarter was 291. This was a 52% increase from 192 in the previous quarter.

During this quarter, JPCERT/CC observed many cases where victims were redirected to a lottery scam website by means of malicious code embedded in a website. JPCERT/CC confirmed that JavaScript code similar to the example shown below was inserted in many compromised websites.

```
34  href="https://statcounter.com/" target="_blank"><img
35  class="statcounter"
36  src="https://c.statcounter.com/12180693/0/22249354/1/"
37  alt="web stats"></a></div></noscript>
38  <!-- End of Statcounter Code -->
39
40  <script>
41  setTimeout("location.href='http://www.jjokgo.xyz/jjgo'",300);
42  </script>
43
44  </head>
45
46  <body class="home blog">
47  <div id="page" class="hfeed site">
48      <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
49
```

[Figure 10: Inserted JavaScript code]

When the compromised website is accessed through a web browser, the visitor is redirected to a fraudulent website, where similar code and HTTP status code (300, etc.) are used to redirect the visitor to yet another website, displaying a lottery scam page like the one shown in [Figure 11] in the end. On the lottery scam page, the visitor is asked to enter personal information, which suggests that the aim is to collect personal information.



[Figure 11: Lottery scam page displayed in the end]

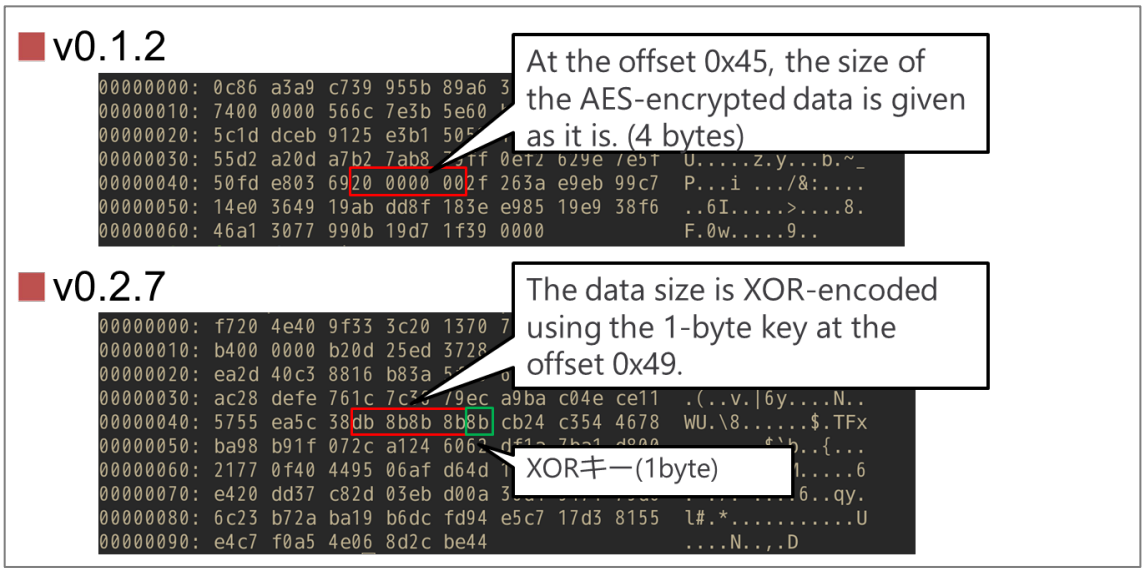
3.3. Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This was a 200% increase from 2 in the previous quarter. The incidents identified are described below.

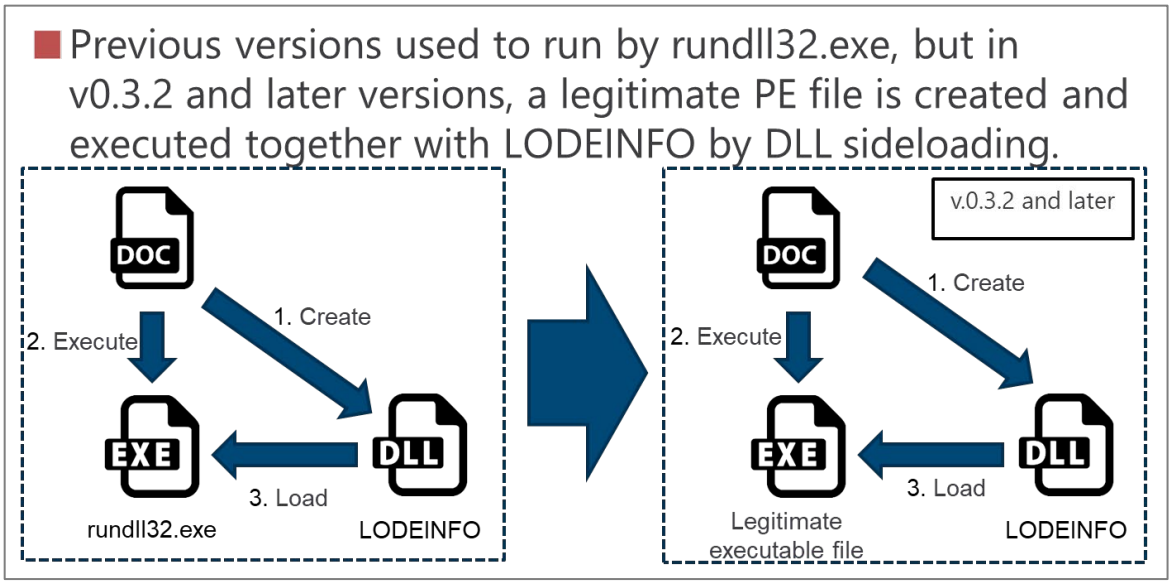
(1) Attacks using LODEINFO malware

As in the previous quarter, JPCERT/CC continued to receive reports of targeted attacks using LODEINFO malware this quarter. The method observed uses an e-mail with a Word or Excel attachment containing a malicious macro to infect the recipient's computer with LODEINFO malware. These e-mails and attachments contain various content, ranging from information about COVID-19 to a fake resume.

JPCERT/CC posted a blog article discussing LODEINFO in detail during the previous quarter, but the malware identified this quarter used a different format for sending and receiving data (see [Figure 12] and a different execution method (see [Figure 13]). This shows that the malware is being updated frequently and continued vigilance is required.



[Figure 12: Changes in data transmission/reception format]



[Figure 13: Changes in execution method]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 133. This was a 47% decrease from 250 in the previous quarter.

The number of scans reported in this quarter was 982. This was a 38% increase from 713 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), HTTP (80/TCP) and SMTP (25/TCP).

[Chart 4：Number of scans by port]

Port	Jan	Feb	Mar	Total
22/tcp	211	106	170	487
80/tcp	53	61	84	198
25/tcp	40	28	43	111
23/tcp	15	12	13	40
445/tcp	0	29	2	31
443/tcp	6	8	11	25
37215/tcp	7	12	2	21
62223/tcp	14	0	4	18
26/tcp	8	8	2	18
3389/tcp	3	3	6	12
8080/tcp	3	5	2	10
60001/tcp	1	3	5	9
5555/tcp	5	3	1	9
2323/tcp	2	5	2	9
9530/tcp	3	3	2	8
81/tcp	1	6	1	8
1433/tcp	3	3	1	7
21/tcp	1	4	0	5
88/tcp	0	2	2	4
Unknown	15	18	13	46
Monthly Total	391	319	366	1076

There were 379 incidents categorized as other. This was a 23% decrease from 492 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 report of DDoS attacks using open resolvers in Japan

In early April 2020, JPCERT/CC was informed by an overseas security organization that DNS amplification attacks are being carried out from a number of IP addresses in Japan. DNS servers were operating at all the IP addresses reported and acting as open resolvers. JPCERT/CC contacted operators managing the 56 reported IP addresses and requested them to check their DNS server settings.

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 2020 Fiscal Year".