JPCERT/CC Incident Handling Report

July 1, 2020 ～ September 30, 2020

JPCERT Coordination Center

October 15, 2020

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 April 1, 2020 through June 30 , 2020.

[*1] JPCERT/CC refers to all events that may occur in the management of information systems, whichinclude events that may be considered security issues and any case related to computer security, asan 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	Total
Number of Reports *2	4,034	4,324	5,473	13,831	10,416
Number of Incident *3	2,640	2,600	3,146	8,386	7,123
Cases Coordinated *4	1,621	1,535	1,651	4,807	4,201

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

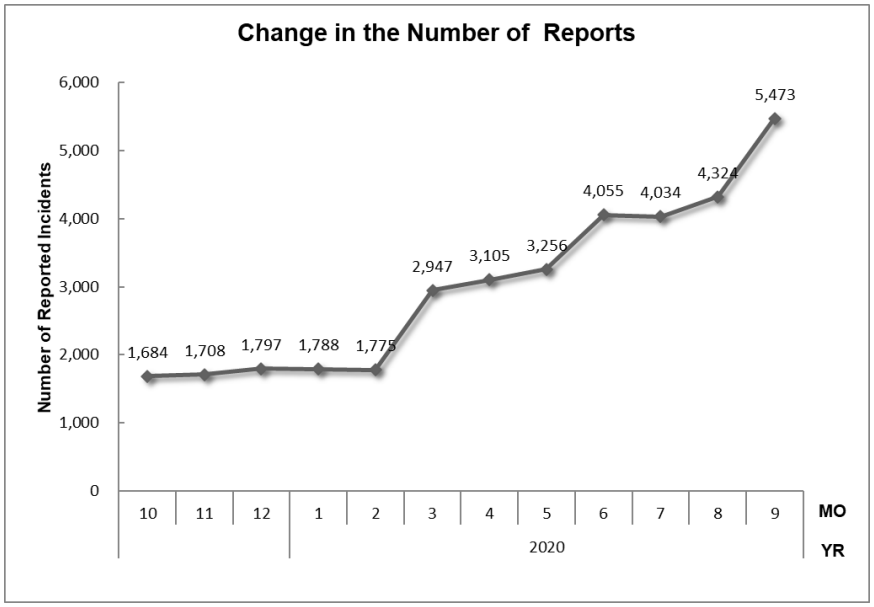
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

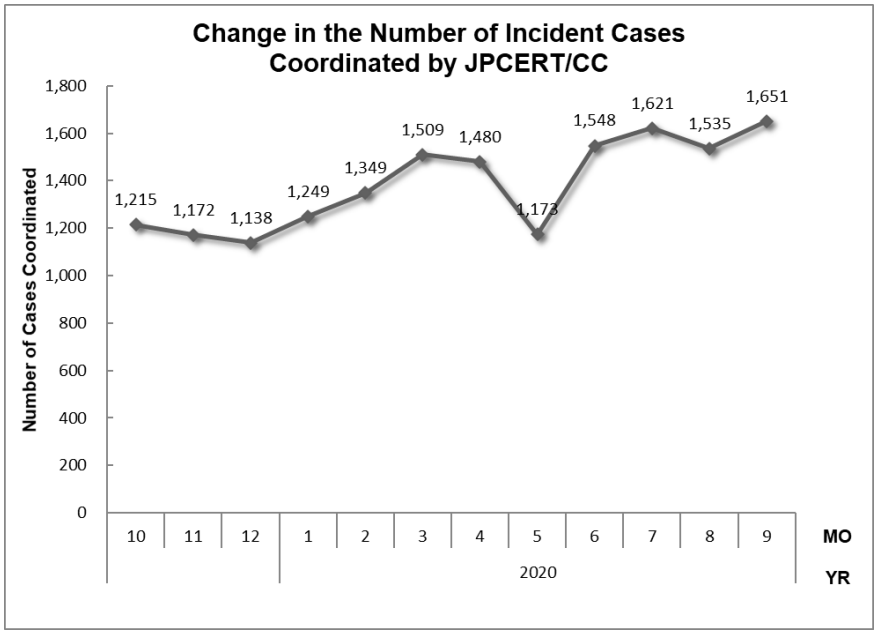
The total number of reports received in this quarter was 13,831. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,807. When compared with the previous quarter, the total number of reports increased by 33%, and the number of cases coordinated increased by 14%. Year on year, the number of reports increased by 200%, and the number of cases coordinated increased

by 16%.

[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]

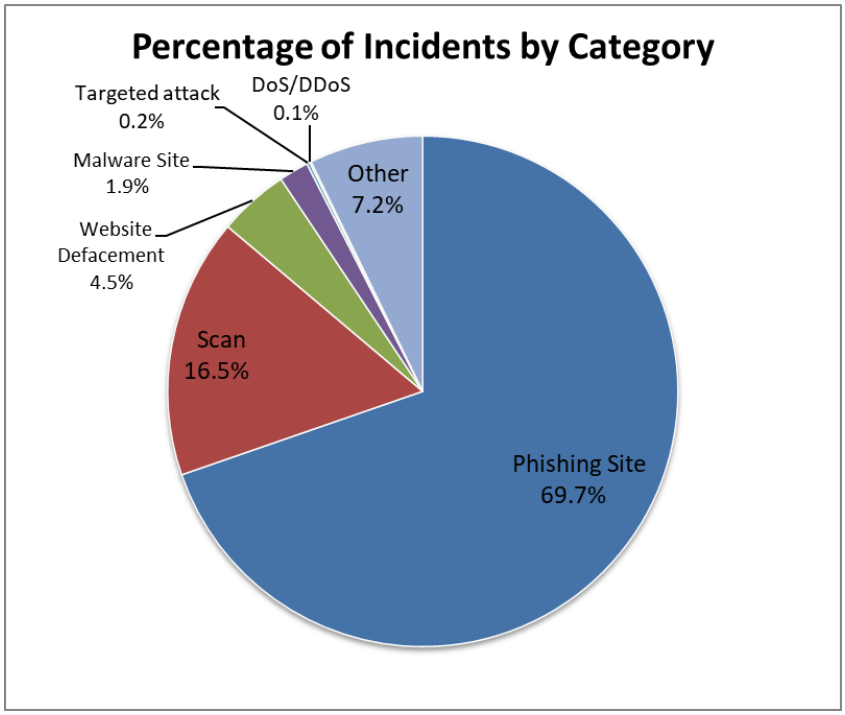


[Figure 2: Change in the number of incident cases coordinated]

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]

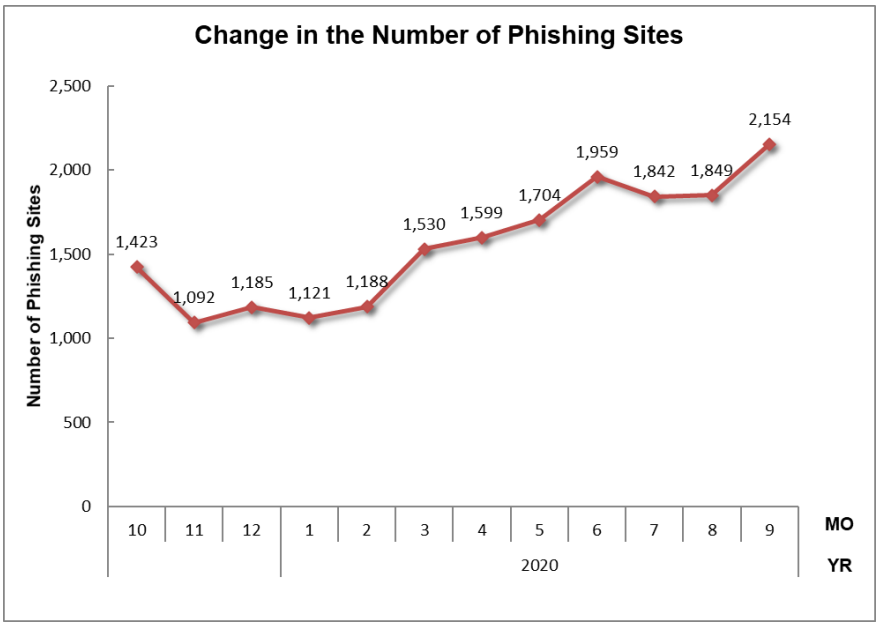
Incident Category	Jul.	Aug.	Sept.	Total	Last Qtr. Total
Phishing Site	1,842	1,849	2,154	5,845	5,262
Website Defacement	179	91	104	374	291
Malware Site	67	38	53	158	133
Scan	392	477	511	1,380	982
DoS/DDoS	4	4	0	8	70
ICS Related	0	0	0	0	0
Targeted attack	10	1	5	16	6
Other	146	140	319	605	379



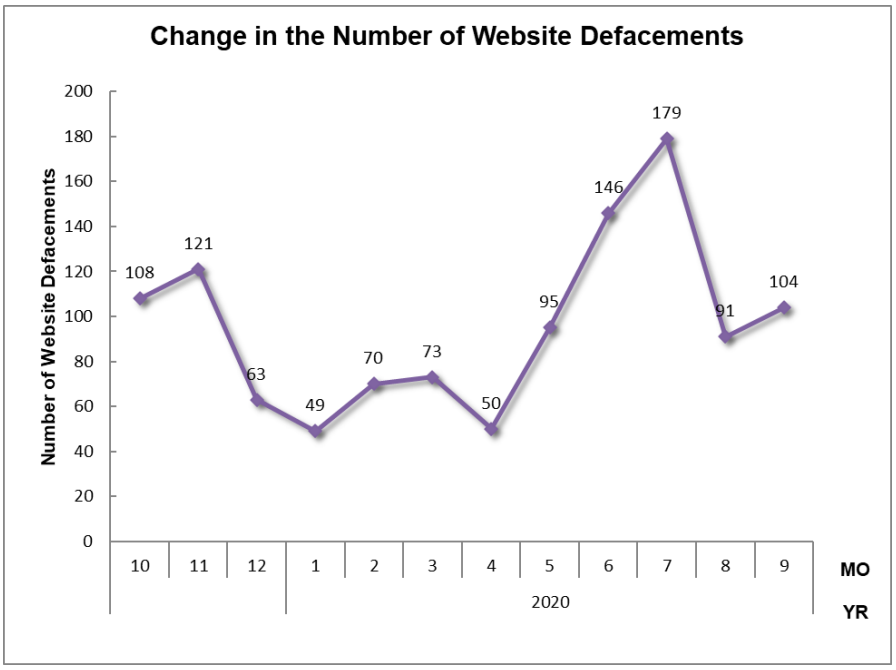
[Figure 3: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 69.7%, and those categorized as scans, which search for vulnerabilities in systems, made up 16.5%.

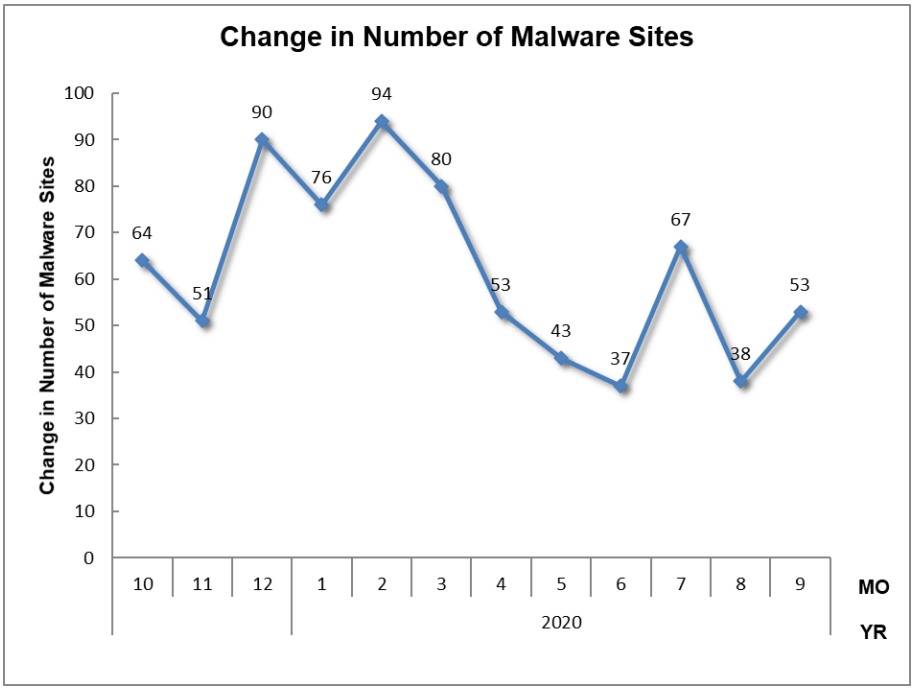
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



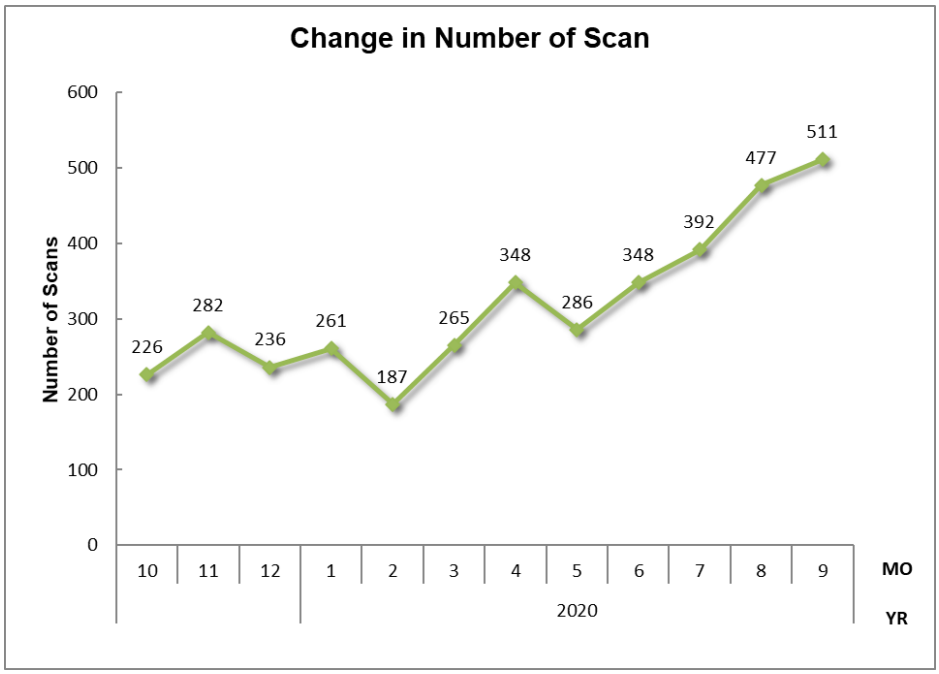
[Figure 4: Change in the number of phishing sites]



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

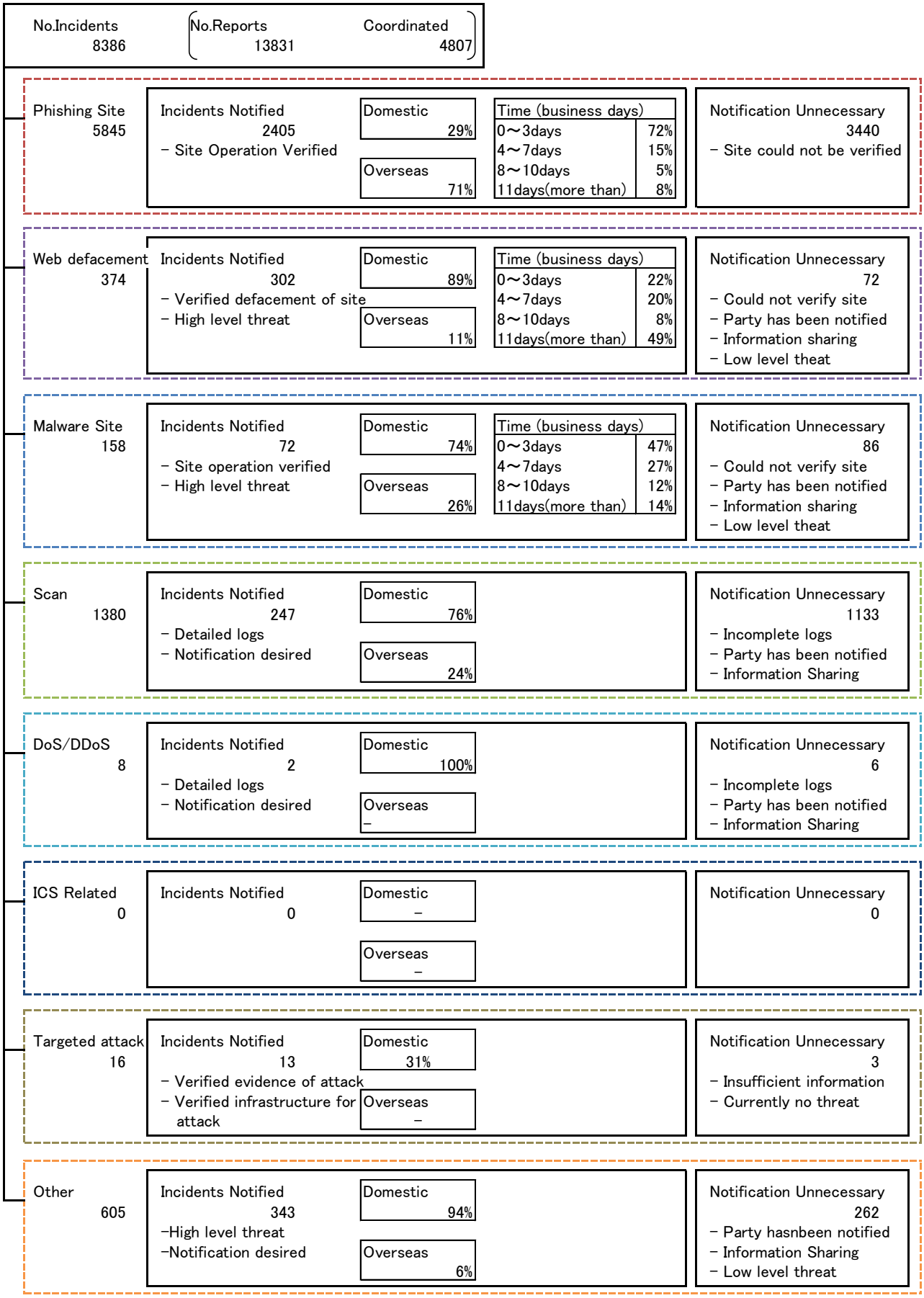


[Figure 6: Change in the number of malware sites]



[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

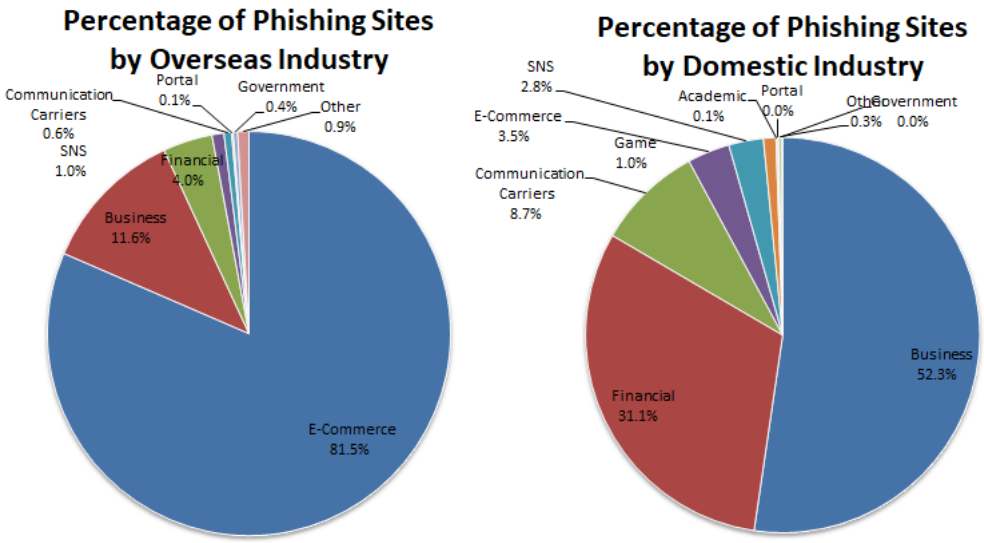
During this quarter, 5,845 reports on phishing sites were received, representing an 11% increase from 5,262 in the previous quarter. This marks a 69% increase from the same quarter last year (3,457).
During this quarter, there were 2,043 phishing sites that spoofed domestic brands, increasing 37% from 1,489 in the previous quarter. And there were 3,122 phishing sites that spoofed overseas brands, decreasing 4% from 3,265 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	Jul.	Aug.	Sept.	Domestic/ Overseas Total (%)
Domestic Brand	590	607	846	2,043(35%)
Overseas Brand	1,089	1,047	986	3,122(53%)
Unknown Brand[*5]	163	195	322	680(12%)
Monthly Total	1,842	1,849	2,154	5,845

[*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, 81.5% spoofed e-commerce websites for overseas brands and 52.3% spoofed corporate websites for domestic brands, both representing the largest share respectively.

For both domestic and overseas brands, there were many phishing sites spoofing the login screens of specific shopping sites, accounting for more than a half in both cases.
In the case of domestic brands, an upward trend was seen in phishing sites spoofing the online services of banks and credit card companies as well as login screens of web-based e-mail services offered by Internet service providers and so on.
Many of the phishing sites used .com, .top, .cn and .xyz domains containing the domain and brand name of legitimate websites with alphanumeric characters added.

When accessed from a PC browser, some phishing sites spoofing domestic banks displayed the following content, which was different from the content displayed when accessed from a smartphone or other device.

[Figure 10：Content displayed when accessed from a PC browser]

The parties that JPCERT/CC contacted for coordination of phishing sites were 29% domestic and 71% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 50%, overseas: 50%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 374. This was a 29% increase from 291 in the previous quarter.
During this quarter, JPCERT/CC received multiple reports of cases where users are redirected from compromised websites to suspicious websites via websites with URLs that have the following structure.

```
https[:]//somelandingpage[.]live/?utm_campaign=<  Random alphanumeric characters >&t=main7d
```

This redirect occurred only when accessed via a search engine, and when accessed directly, the web page displayed harmless content. [Figure 11] shows an example of the content displayed when a compromised web page is accessed via a search engine.

```
<html>
  <head>
    <META http-equiv="refresh" content="1;URL=https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d">
   <script>
   window.location = "https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d";
   </script>
  </head>
  <body>
  To the new location please <a href="https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d"><b>click here.</b></a>
  </body>
</html>
```

[Figure 11: Example redirect code]

In these reported cases, it was confirmed that a sweepstakes scam website or a suspicious e-commerce website was eventually displayed.

3.3. Targeted Attack Trends

There were 16 incidents categorized as a targeted attack. This was a 167% increase from 6 in the previous quarter. The incidents identified are described below.

(1) Lazarus Group attacks

During this quarter, JPCERT/CC received reports of targeted attacks aimed at Japanese organizations by a group called Lazarus (also known as Hidden Cobra). The malware used to carry out the attacks differed from the one used for network intrusion. The attackers also used free tools available on GitHub and other sources to spread infection within the network. The malware used after intrusion is discussed in detail on JPCERT/CC Eyes.

BLINDINGCAN - Malware Used by Lazarus –
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html

(2) Attacks using the Winnti malware

The Winnti malware was used in targeted attacks reported around August. A number of cloud servers were found infected with malware, which suggests that the attackers target not just internal corporate servers but also servers using external cloud services.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 158. This was a 19% increase from 133 in the previous quarter.

The number of scans reported in this quarter was 1,380. This was a 41% increase from 982 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 4：Number of scans by port]

Port	Jul.	Aug.	Sept.	Total
22/tcp	208	179	178	565
25/tcp	50	135	188	373
80/tcp	92	89	76	257
143/tcp	10	10	18	38
445/tcp	4	13	19	36
23/tcp	5	15	14	34
443/tcp	14	10	8	32
62223/tcp	8	9	8	25
1433/tcp	1	7	6	14
8080/tcp	1	4	3	8
9530/tcp	5	2	0	7
81/tcp	5	2	0	7
3306/tcp	1	4	1	6
8081/tcp	0	2	3	5
37215/tcp	0	1	4	5
3389/tcp	2	2	1	5
7547/tcp	0	2	2	4
60001/tcp	0	3	1	4
26/tcp	1	2	1	4
Unknown	11	9	11	31
Monthly Total	418	500	542	1460

There were 605 incidents categorized as other. This was a 60% increase from 379 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 ransomware

This quarter, a number of Japanese organizations reported cases of ransomware infection resulting in file encryption at both domestic and overseas offices. JPCERT/CC determined the type of malware based on distinguishing features such as the extensions of encrypted files, and provided information including attack methods and characteristics.
Some of the organizations subjected to attack had information stolen and disclosed on the attacker's website.

(2) Coordination involving reports of Emotet malware

After a period of inactivity, the Emotet malware resumed its campaigns in the middle of July 2020. JPCERT/CC has received numerous reports that e-mail accounts whose credentials were stolen by Emotet are being used to send spam e-mails, and that Emotet was found embedded on compromised websites in Japan. JPCERT/CC contacted administrators of mail servers to have them check for unauthorized use of e-mail accounts, and administrators of web servers to request investigation of alterations and appropriate handling of the matter.

Based on cases identified most recently, JPCERT/CC updated the content of "How to Respond to Emotet Infection (FAQ)" and released EmoCheck V1.0 for detecting the new version of Emotet on August 11, 2020.

How to Respond to Emotet Infection (FAQ)
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

JPCERTCC/EmoCheck: Emotet detection tool for Windows OS
https://github.com/JPCERTCC/EmoCheck/releases

(3) Coordination involving reports of subdomain takeover

This quarter, JPCERT/CC received reports of an interesting case of attack in which a method called subdomain takeover was used to post fraudulent content. Subdomain takeover is carried out by using a

CNAME record as shown in [Figure 12] to redirect subdomain (test.example.co.jp in the example) references to a CDN service domain (test.example.net in the example), then later the CDN service is canceled with the domain left abandoned.

```
;; QUESTION SECTION:
;test.example.co.jp.          IN     ANY

;; ANSWER SECTION:
test.example.co.jp.    3600    IN     CNAME   test.examle.net.
```

[Figure 12: Example of a misused CNAME record]

When the attacker signs up for a CDN service with the same domain, the abandoned domain is taken over. This quarter, JPCERT/CC received a number of reports involving a website whose subdomain looks legitimate and which shows a sweepstakes scam page at the end. JPCERT/CC contacted the domain administrator to request correction of the CNAME record and other measures.

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".