JPCERT CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IR-2016-01
Issued: 2016-04-14

JPCERT/CC Incident Handling Report
[January 1, 2016 - March 31, 2016]

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, 2016 through March 31, 2016.

[*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]

	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports [*2]	1176	1405	2006	4587	3440
Number of Incident [*3]	994	1410	1739	4143	3169
Cases Coordinated [*4]	678	1013	1264	2955	2053

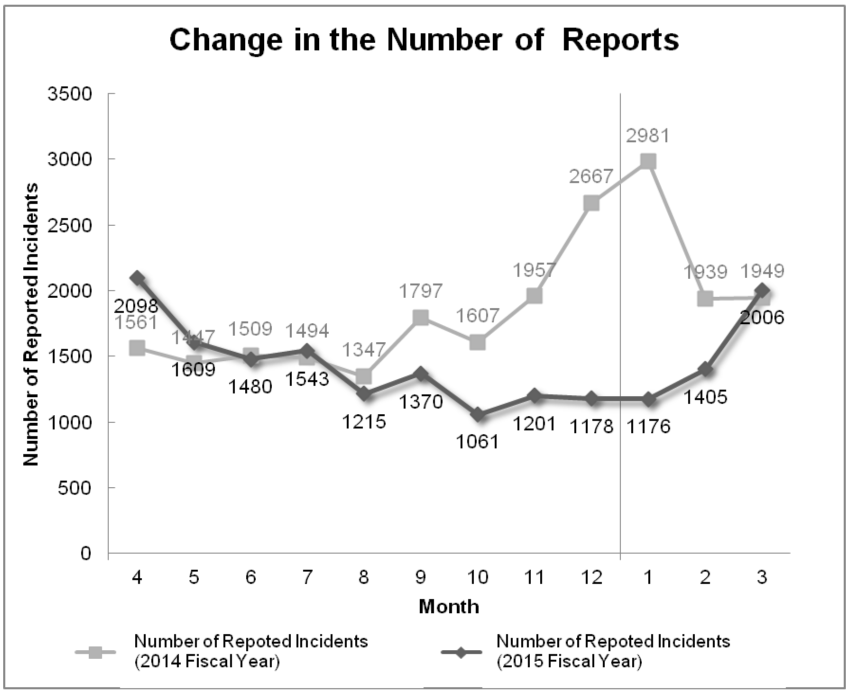
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

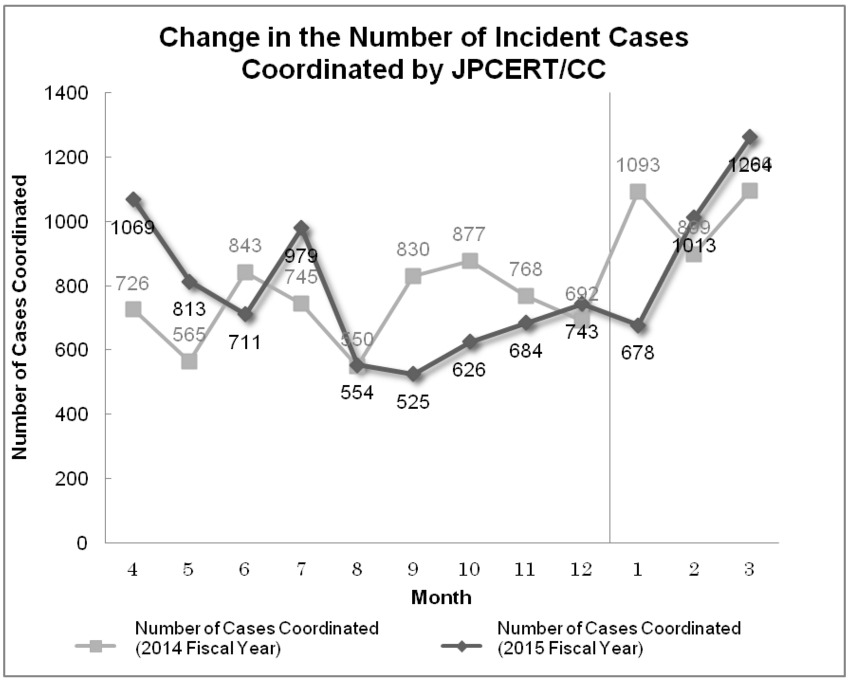
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,587. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,955. When compared with the previous quarter, the total number of reports increased 33%, and the number of cases coordinated increased 44%. When compared with the same quarter of the previous year, the total number of reports decreased 33%, and the number of cases coordinated decreased 4%.

[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]

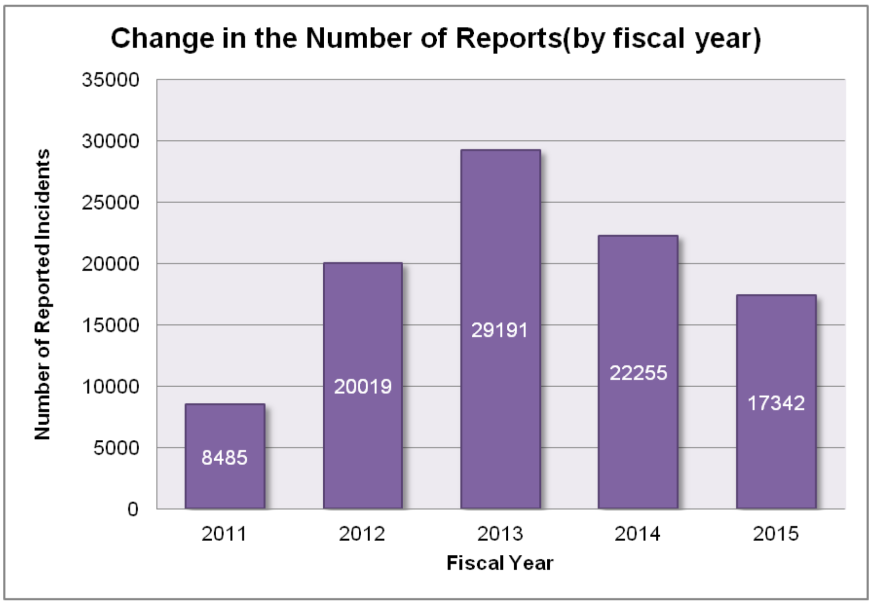
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2015. 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	2011	2012	2013	2014	2015
No. Reports	8485	20019	29191	22255	17342

The total number of reports received in FY2015 was 17,342. This marked a 22% decrease from the 22,255 reports received in the previous fiscal year. [Figure **3**] shows the change in the total number of reports in the past 5 years.



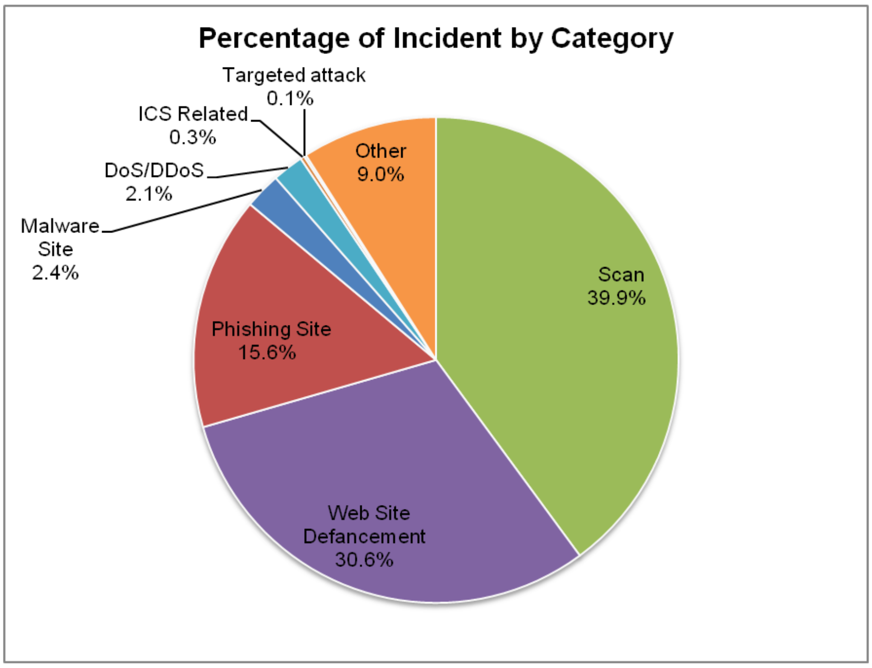
[Figure 3: Change in the total number of reports (by fiscal year)]

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

[Chart 3: Number of incidents by category]

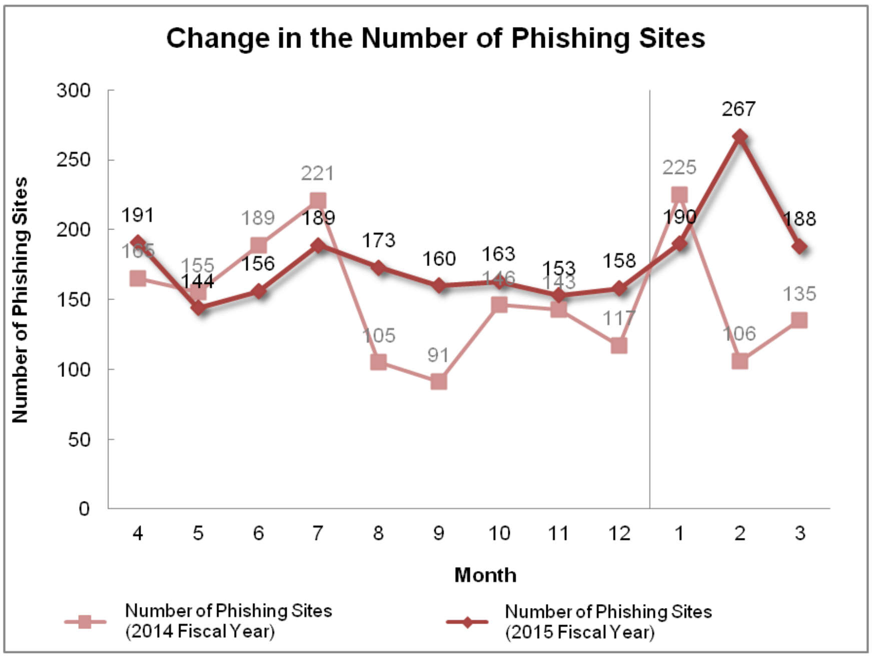
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	190	267	188	645	474
Website Defacement	283	519	466	1268	826
Malware Site	29	14	57	100	84
Scan	374	457	823	1654	1526
DoS/DDoS	14	39	33	86	11
ICS Related	8	3	0	11	12
Targeted attack	2	4	0	6	12
Other	94	107	172	373	224

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 4]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 39.9%, and incidents categorized as website defacement made up 30.6%. Also, incidents categorized as phishing sites represented 15.6% of the total.

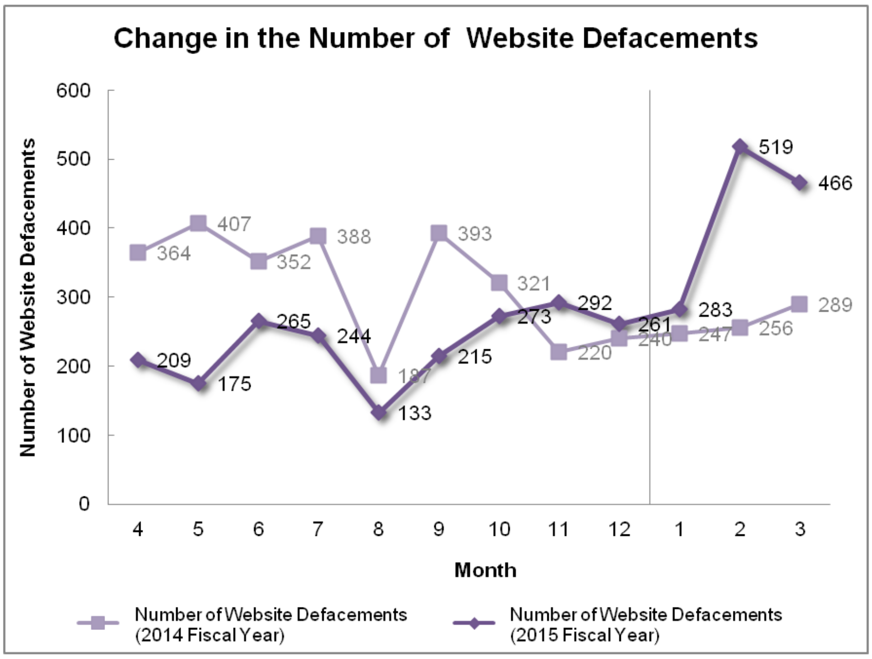


[Figure 4 Percentage of incidents by category]

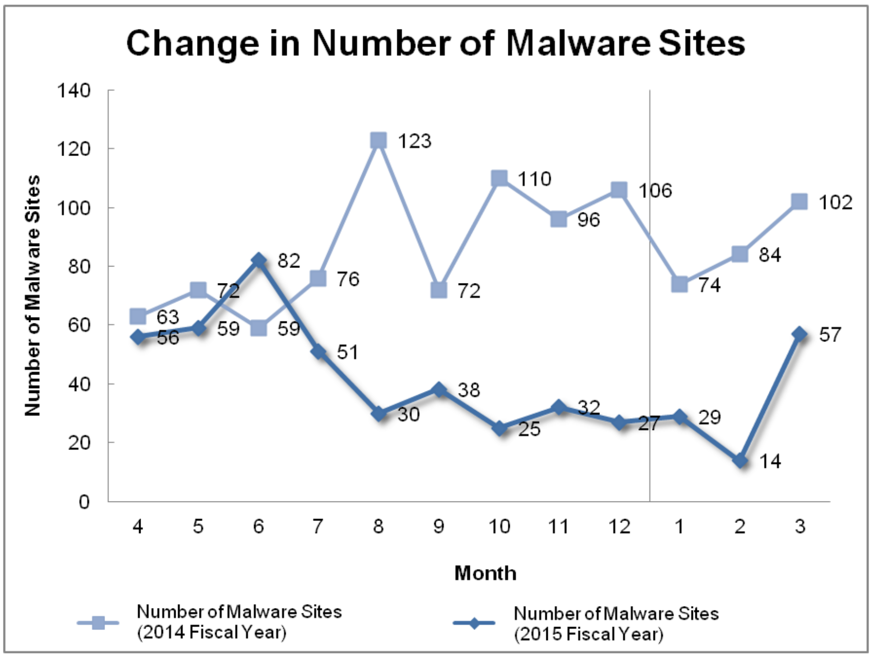
[Figure 5] through [Figure 8] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



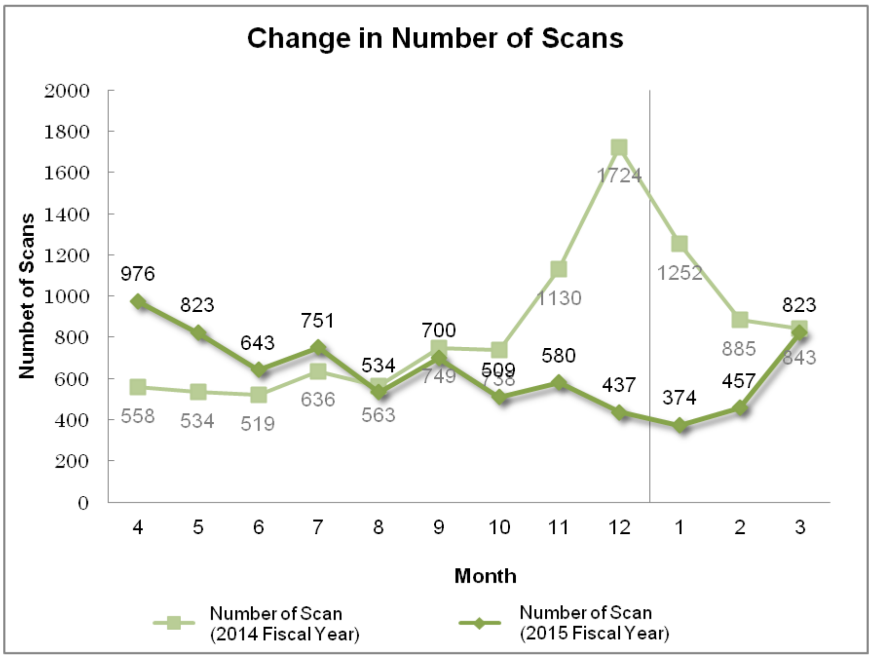
[Figure 5 Change in the number of phishing sites]



[Figure 6 Change in the number of website defacements]

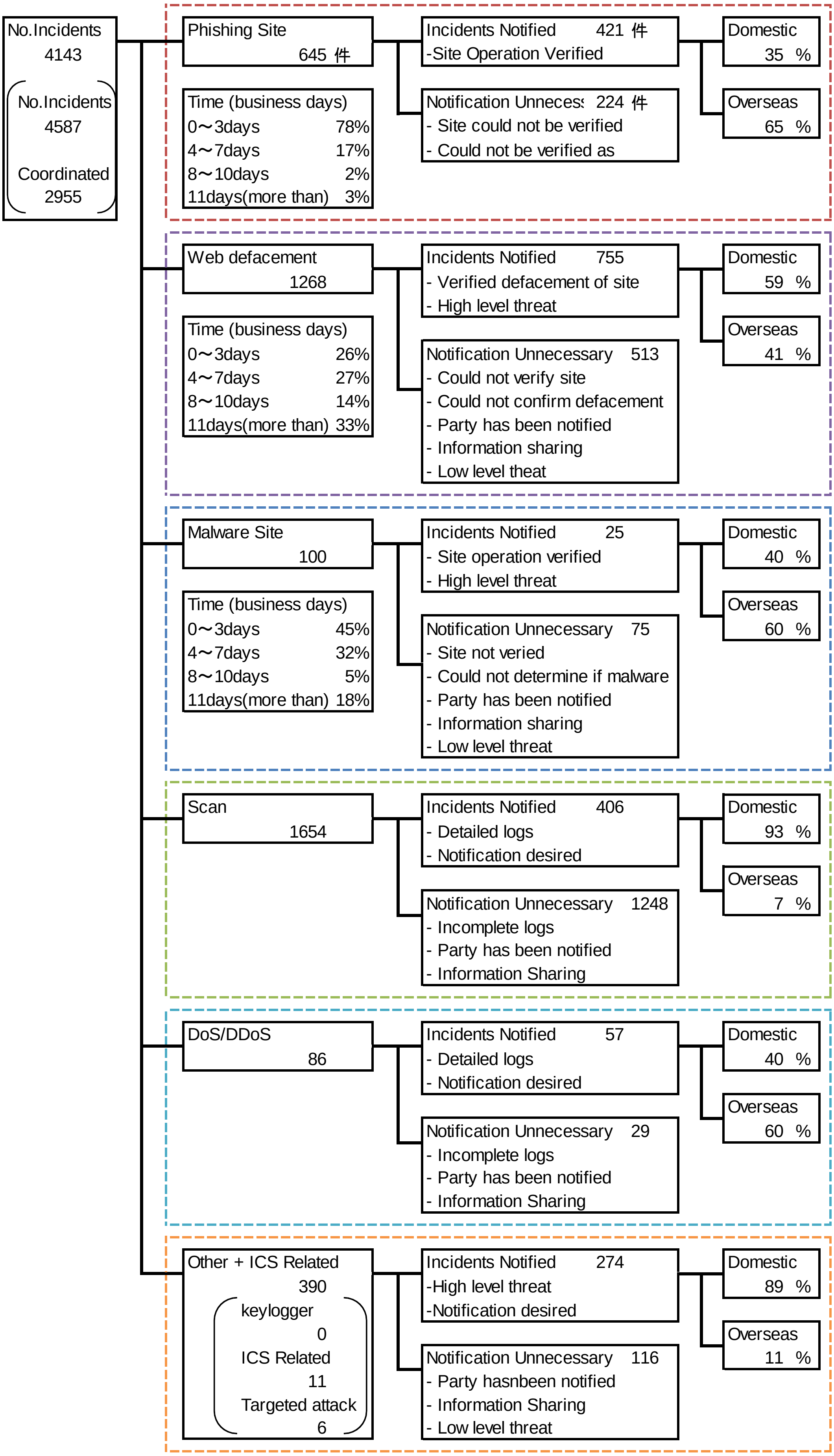


[Figure 7 Change in the number of malware sites]



[Figure 8 Change in the number of scans]

[Figure 9] provides an overview as well as a breakdown of the incidents that were coordinated/handled.



[Figure 9 Breakdown of incidents coordinated/handled]

3. Incident Trends

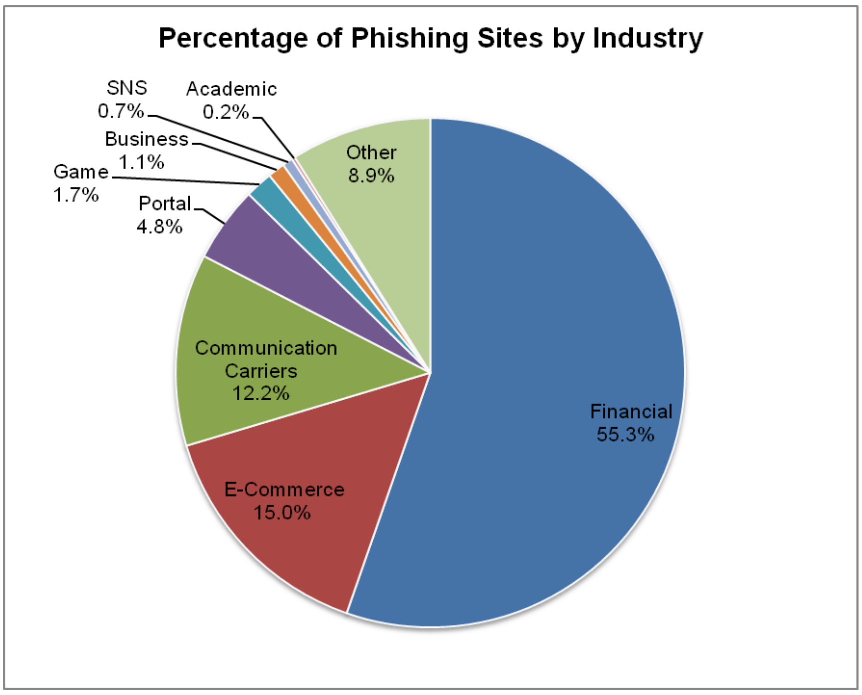
3.1. Phishing Site Trends

645 reports on phishing sites were received in this quarter, representing a 36% increase from 474 of the previous quarter. This marks a 38% increase from the same quarter last year (466). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in[Chart 4], and a breakdown by industry is shown in [Figure 10].

[Chart 4 Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jan	Feb	Mar	Domestic/ Overseas Total (%)
Domestic Brand	48	96	45	189(29%)
Overseas Brand	75	95	100	270(42%)
Unknown Brand [*5]	67	76	43	186(29%)
Monthly Total	190	267	188	645(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 10 **Percentage of reported phishing sites by industry**]

During this quarter, there were 189 phishing sites that spoofed domestic brands, increasing 52% from 124 of the previous quarter. There were 270 phishing sites that spoofed overseas brands, increasing 8% from 250 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 55.3% spoofed websites of financial institutions, and 15.0% spoofed e-commerce sites. In both Japanese and overseas brands, financial institutions accounted for most of the spoofed brands.

Numerous phishing sites spoofing a specific Japanese financial institution were identified between the end of January and early March. Phishing mails related to this case listed a fraudulent page set up in the "/images" directory of a number of websites in China, and phishing sites to which recipients are transferred from this page used hosts with IP addresses in Hong Kong and China.

Around the same time, numerous phishing sites using a domain similar to that of another Japanese financial institution were also identified. These phishing sites used a .com domain spoofing the legitimate site and hosts with IP addresses in South Korea.

Since mid-March, JPCERT/CC has received many reports on phishing sites spoofing online gaming services. Approximately 60 URLs were identified for phishing sites spoofing a specific game, but there were only 6 unique IP addresses, all of which belonged to a telecommunications operator in Hong Kong. As a distinctive trait, these phishing sites all used a .cc domain, which can be registered free of charge.

The parties that JPCERT/CC contacted for coordination of phishing sites were 35% domestic and 65% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 46%, overseas: 54%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 1,268. This was a 54% increase from 826 of the previous quarter.

As in the previous quarter, a great many websites using CMS were compromised.

Malicious JavaScript embedded in compromised websites redirected visitors to another site, where an attack targeting vulnerabilities in Internet Explorer, Adobe Flash Player, Silverlight and other applications is initiated to download and execute malware. JPCERT/CC has confirmed that the vulnerability in Silverlight exploited in the attack is a relatively new one (CVE-2016-0034) that was fixed in January 2016.

JPCERT/CC has also confirmed that malware downloaded from the site to which visitors are redirected includes ransomware, which encrypts files stored on a computer in order to demand money to decrypt them, and malware that steals account and other information.

3.3.Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This was a 50% decrease from 12 of the previous quarter. JPCERT/CC requested a total of 4 organizations to take action during this quarter.

This quarter, a number of overseas security groups provided JPCERT/CC with information, including domestic IP addresses used as infrastructure for carrying out targeted attacks, and information about malware that might have been used in an attack targeting a specific organization in Japan. Based on the information provided, JPCERT/CC requested the organization to investigate relevant facts.

3.4.Other Incident Trends

The number of malware sites reported in this quarter was 100. This was a 19% increase from 84 of the previous quarter.

The number of scans reported in this quarter was 1,654. This was an 8% increase from 1,526 of the previous quarter. The ports that the scans targeted are listed in[Chart 5]. Ports targeted frequently were HTTP (80/TCP), SMTP (25/TCP) and SSH (22/TCP).

[Chart 5: Number of scans by port]

Port	Jan	Feb	Mar	Total
80/tcp	137	144	338	619
25/tcp	141	172	170	483
22/tcp	45	67	82	194
53/udp	0	1	109	110
23/tcp	12	16	43	71
445/tcp	23	18	17	58
21/tcp	3	7	37	47
123/udp	2	19	2	23
3389/tcp	5	3	5	13
143/tcp	7	1	4	12
53413/udp	4	2	5	11
8080/tcp	2	1	4	7
1433/tcp	0	1	2	3
110/tcp	2	1	0	3
10000/tcp	1	1	1	3
7001/tcp	1	1	0	2
5631/tcp	0	0	2	2
55849/udp	0	0	2	2
53413/tcp	0	1	1	2
139/tcp	0	1	1	2
10686/tcp	0	0	2	2
Unknown	5	74	17	96
Monthly Total	390	531	844	1765

The number of incidents categorized Other was 373. This was a 67% increase from 224 of the previous quarter.

4. Incident Handling Case Examples

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

[Coordination involving the distribution of malware using an Internet ad]
This quarter, JPCERT/CC received a number of reports concerning cases in which an Internet ad redirected visitors from a domestic website to a malicious site where malware was downloaded. The fraudulent ad in these cases was loaded via a legitimate ad distribution platform, and the attacker with the aim of distributing malware had in some way registered the ad through a formal process. JPCERT/CC confirmed a number of cases in which the domain of a domestic website was used in a URL contained in a fraudulent banner ad. It appears that such domain had a subdomain added by rewriting registered information through fraudulent means, and it was linked to an overseas IP address. Another characteristic seen in the server of the fraudulent ad was that it used an SSL certificate that can be obtained for free. JPCERT/CC confirmed that the fraudulent ad redirects visitors to another site where attacks targeting multiple vulnerabilities are launched and malware is downloaded, as in the case of the compromised website described in 3.2.

JPCERT/CC requested the administrator of the domain that could have been abused to confirm whether the host name and IP address used for the fraudulent ad were intended, and it was found out that they were not intended and the DNS information could have been altered without authorization.

[Coordination involving e-mail spoofing a Japanese company with malware attached]
In early March, JPCERT/CC received a number of reports concerning the receipt of a flood of e-mail spoofing a Japanese company with a suspicious file attached. JPCERT/CC investigated the file provided and found that the attachment contained JavaScript, and that by opening it malware is obtained and executed, ultimately infecting the computer with malware that targets domestic Internet banking users. This malware has a web injection function that embeds a page with a fake form for stealing information when a specific Internet banking site is accessed. JPCERT/CC also found out that the malware obtains the JavaScript used for this function from an overseas server.

JPCERT/CC requested the overseas telecommunications operators that manage the server distributing the malware and the server distributing the configuration file that the malware obtains, as well as the overseas CSIRTs in the regions where these servers are located, to take necessary actions.

Request for Cooperation

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

If you would like to encrypt your report, please use JPCERT/CC's PGP public key from the following URL.
Public Key
https://www.jpcert.or.jp/keys/info-0x69ECE048.asc

PGP Fingerprint：

FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

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 2015 Fiscal Year".

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