JPCERT-IR-2015-02
Issued: 2015-04-16

JPCERT/CC Incident Handling Report
[January 1, 2015 – March 31, 2015]

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, 2015 through March 31, 2015.

[*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]	2981	1939	1949	6869	6231
Number of Incident [*3]	2127	1695	1663	5485	5606
Cases Coordinated [*4]	1093	899	1096	3088	2337

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

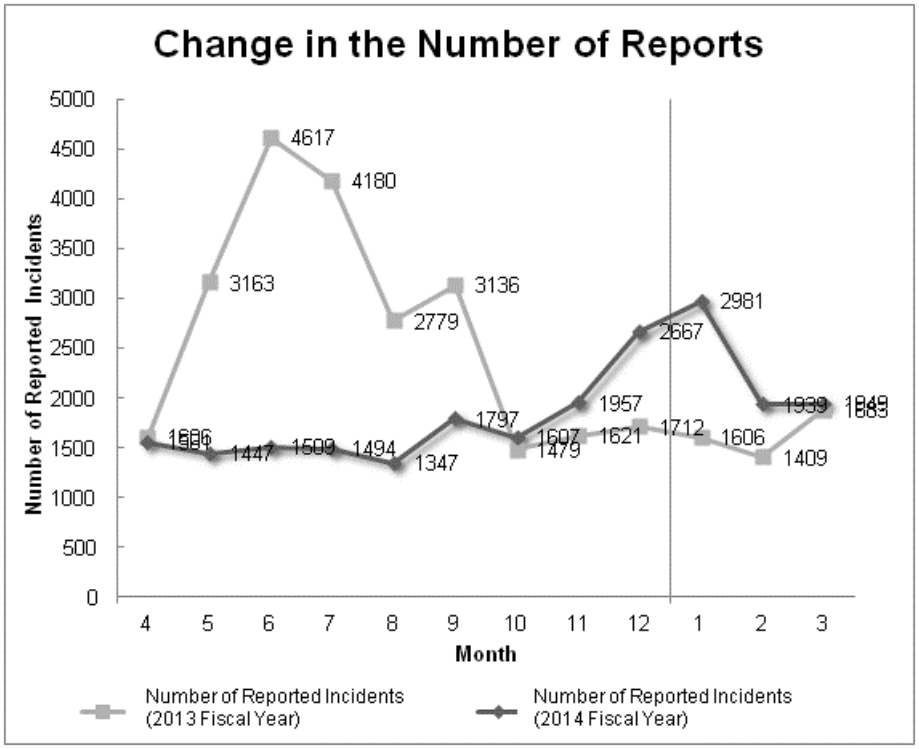
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to

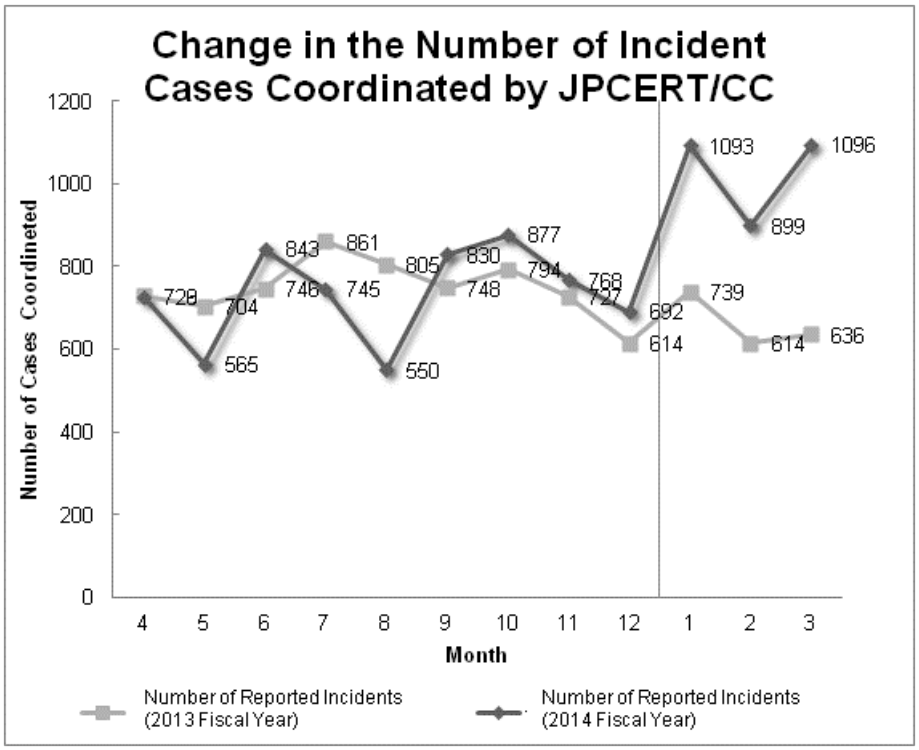
prevent the spreading of an incident by asking the site administrator to conduct an investigation and address any issues.

The total number of reports received in this quarter was 6,869. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 3,088. When compared with the previous quarter, the total number of reports increased by 10%, and the number of cases coordinated increased by 32%. Year on year, the total number of reports increased by 40%, and the number of cases coordinated increased by 55%.

[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 reports]



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

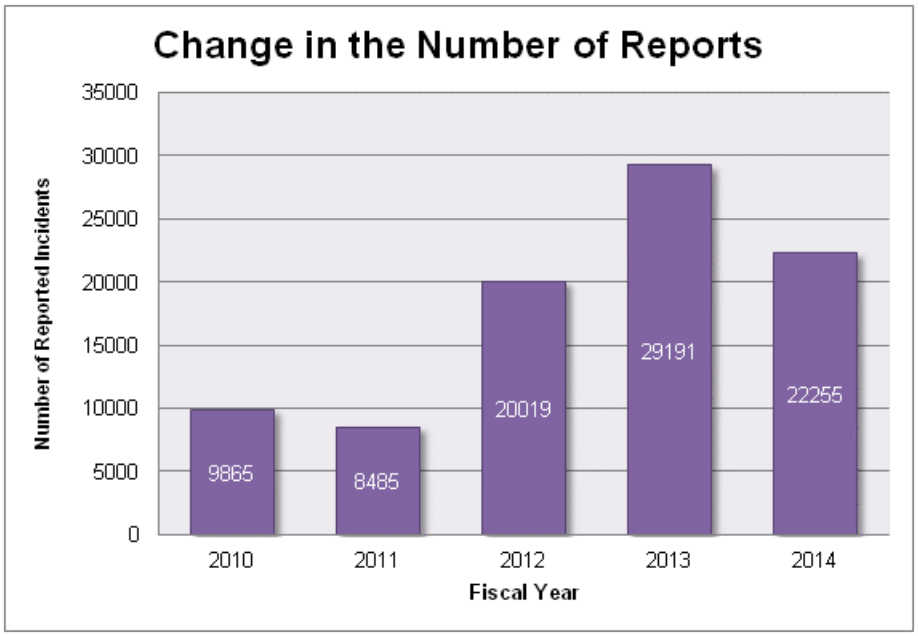
[Reference] Statistic information by fiscal year

The total number of reports for each of the past 5 years including FY2014 is shown in [Chart **2**]. The period of each fiscal year is from April 1 of that year to March 31 of the following year.

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

FY	2010	2011	2012	2013	2014
No. Reports	9865	8485	20019	29191	22255

The total number of reports received in FY2014 was 22,255, decreasing by 24% year-on-year from 29,191. [Figure **3**] shows the change in the total number of incident reports over the past 5 years.



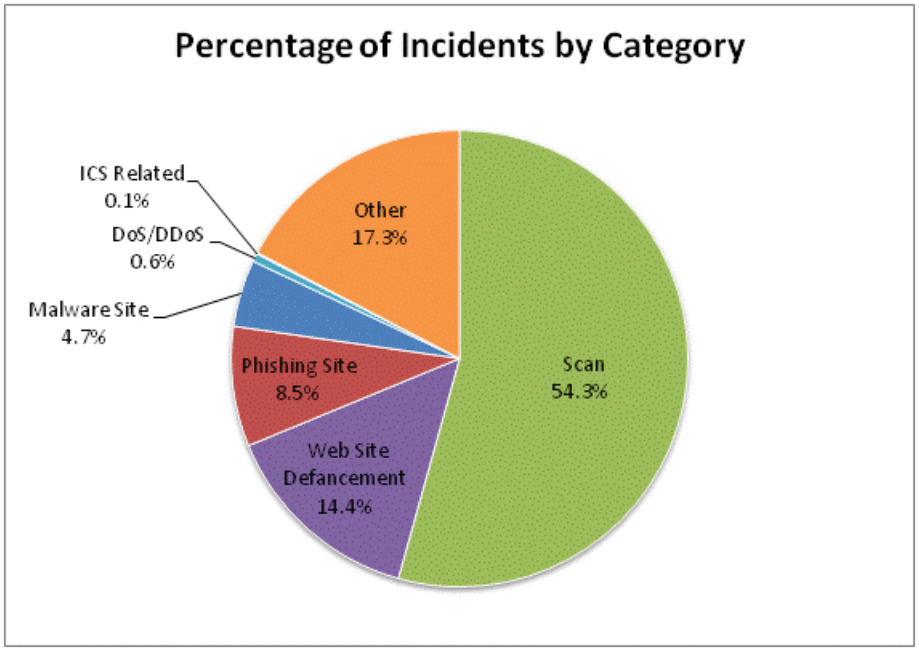
[Figure 3: Change in the total number of incident reports (by fiscal year)]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on 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]

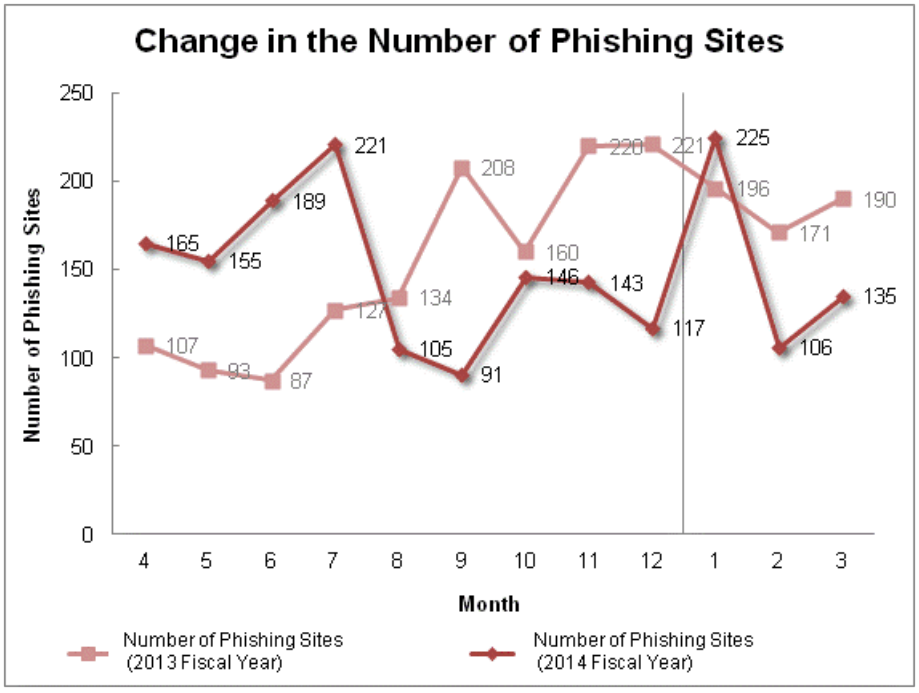
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	225	106	135	466	406
Website Defacement	247	256	289	792	781
Malware Site	74	84	102	260	312
Scan	1252	885	843	2980	3592
DoS/DDoS	23	1	8	32	14
ICS Related	0	4	1	5	3
Other	306	359	285	950	498

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure4]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 54.3%, and incidents categorized as website defacement made up 14.4%. Also, incidents categorized as phishing sites represented 8.5% of the total.

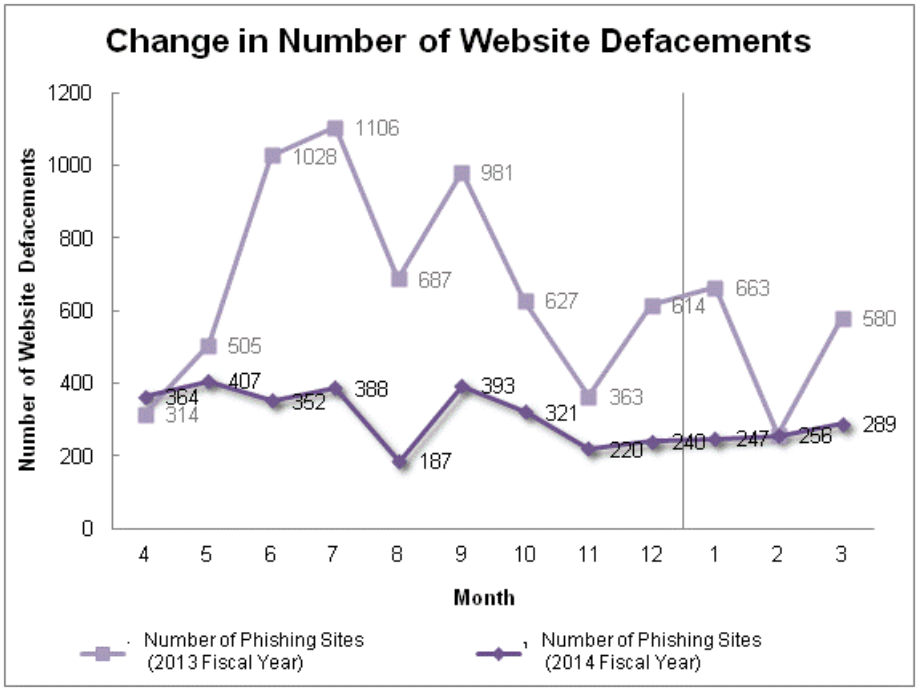


[Figure 4: Percentage of incidents by category]

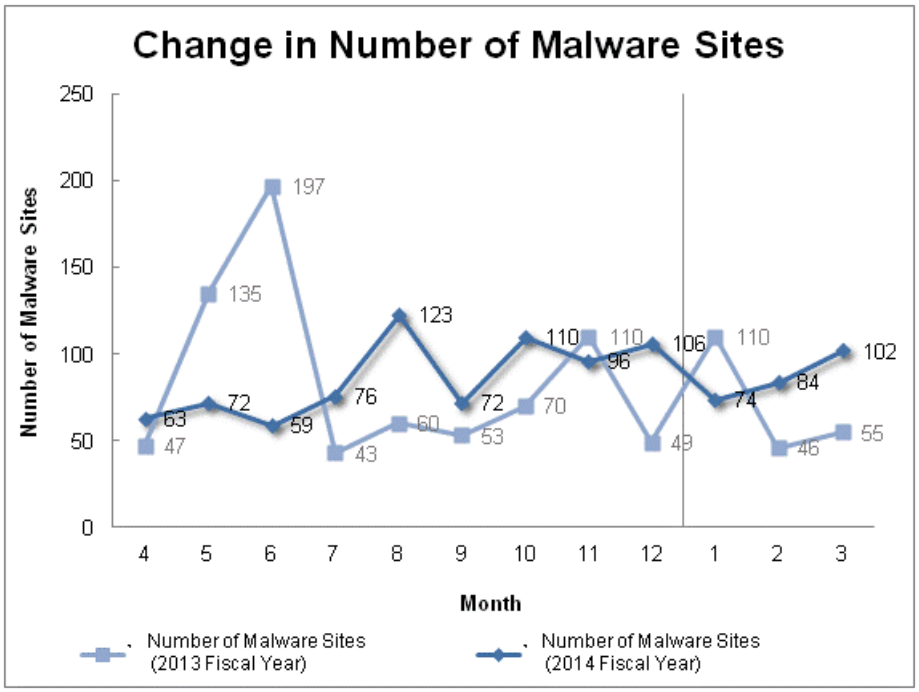
[Figure 5] through [Figure 8] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



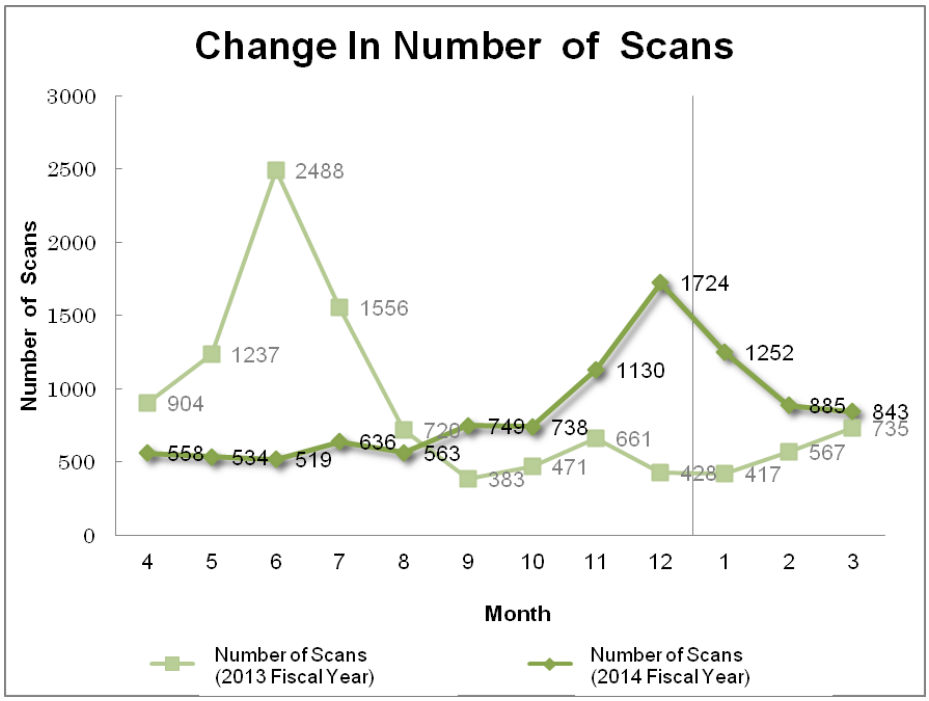
[Figure 5: Change in the number of phishing sites]



[Figure 6: Change in the number of website defacements]

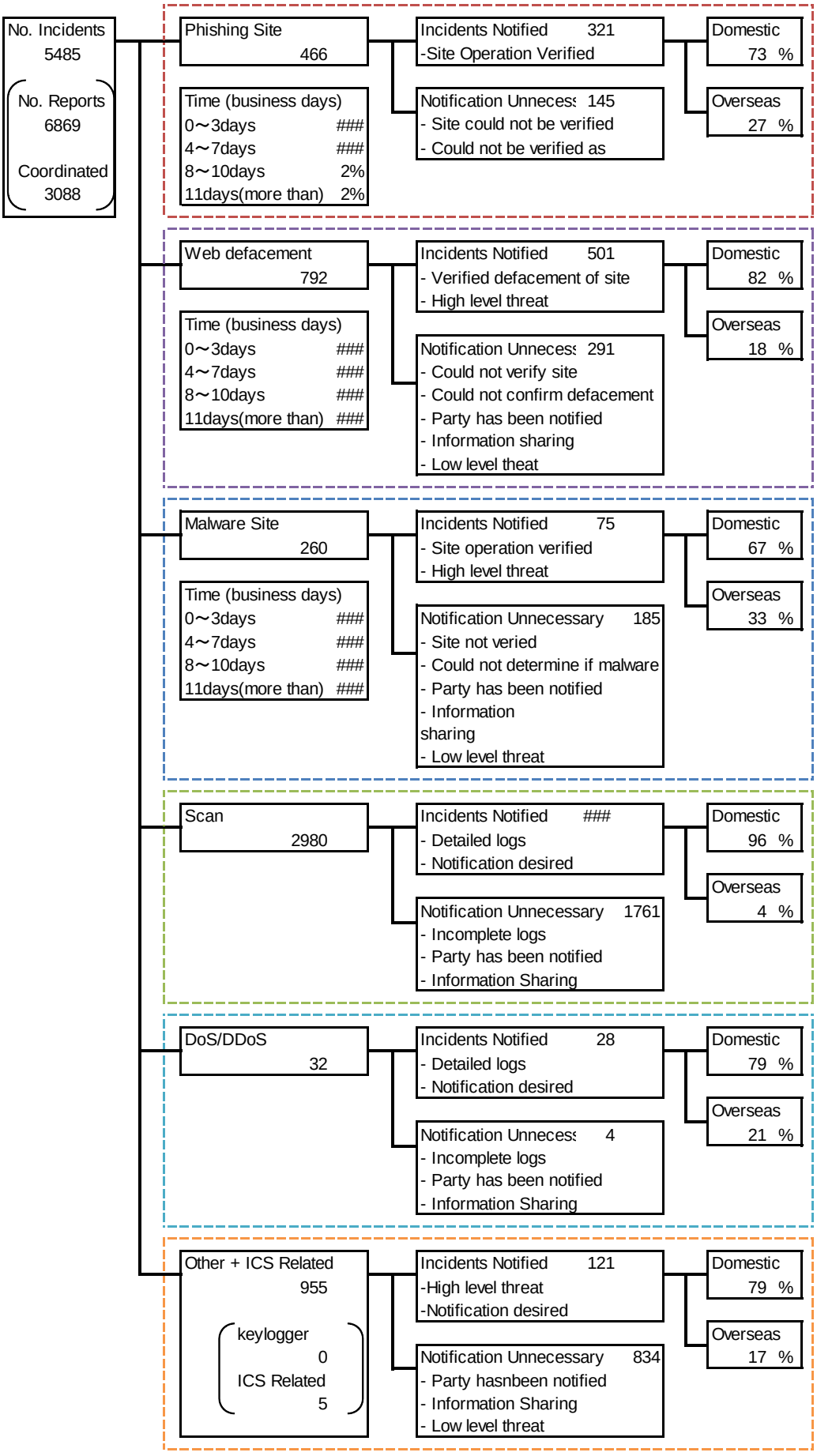


[Figure 7: Change in the number of malware sites]



[Figure 8: Change in the number of scans]

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



[Figure 9: Breakdown of incidents coordinated / handled]

3. Incident Trends

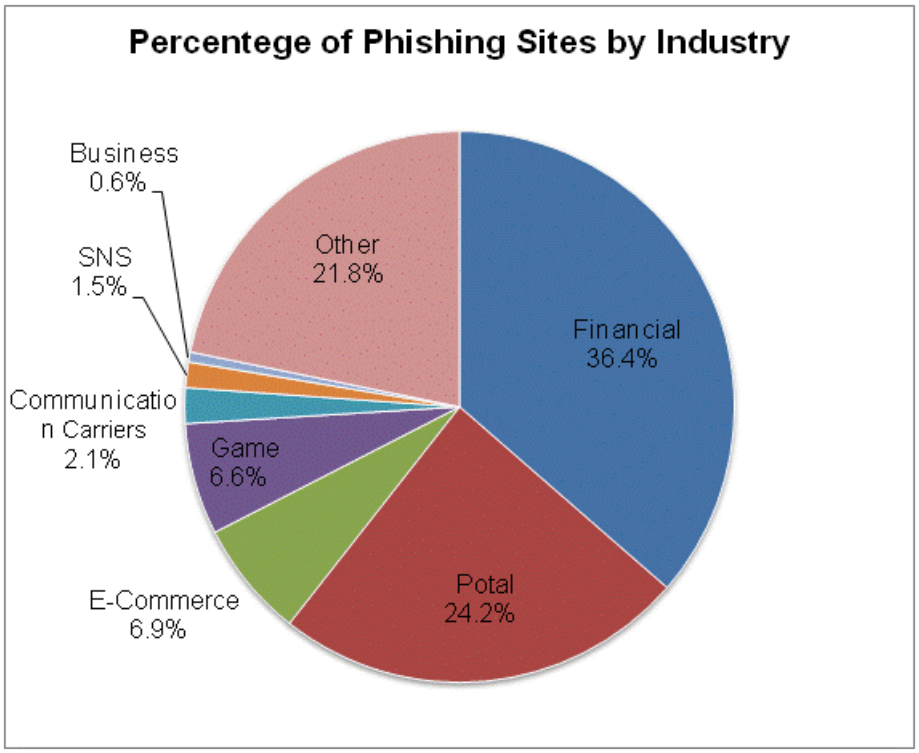
3.1. Phishing Site Trends

During this quarter, 466 reports were received on phishing sites, representing a 15% increase from 406 in the previous quarter. This marks a 16% decrease from the same quarter last year (557). 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 8].

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

Phishing Site	Jan	Feb	Mar	Domestic/ Overseas Total (%)
Domestic Brand	22	18	14	54(12%)
Overseas Brand	136	52	93	281(60%)
Unknown Brand[*5]	67	36	28	131(28%)
Monthly Total	225	106	135	466(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 phishing sites by industry]

During this quarter, there were 54 phishing sites that spoofed domestic brands, decreasing by 28% from 75 in the previous quarter. There were 281 phishing sites that spoofed overseas brands, which was a 19% increase from 236 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 36.4% spoofed websites of financial institutions, and 24.2% spoofed portal sites. Domestically, the industry that had the most phishing sites was the game sector, whereas overseas the financial sector had the most phishing sites.

In the second half of January, a phishing site spoofing a domestic financial institution was seen for the first time since November in the previous quarter, though only for a short period of time. When confirmed the first time, the phishing site was using the IP address of a network managed by a domestic ISP that was also used previously. The IP address was subsequently changed a number of times to that of different domestic ISPs, before finally being changed to an IP address in Hong Kong; the site was later suspended. Judging from the fact that the site switched to different IP addresses of multiple domestic ISPs, it is presumed that the host used as a phishing site was a bot or a proxy under the control of the attacker.

In addition, JPCERT/CC has been continually receiving reports on phishing sites spoofing domestic online gaming services since the previous quarter. These phishing sites were found to be using a large number of URLs with a .com domain consisting of 5 alphabetic characters seemingly assigned randomly. Since these sites with different domains had a common IP address, it is believed that they were hosted on a single server. There is also a case where phishing sites of a number of different games were using the same IP address. It is possible that the same attacker is carrying out phishing attacks using multiple brands.

The parties that JPCERT/CC contacted for coordination of phishing sites were 73% domestic and 27% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 70%, overseas: 30%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 792. This was a 1% increase from 781 in the previous quarter.

During this quarter, JPCERT/CC received a number of reports on cases where the search results of certain brand product names, etc., using Internet search engines listed a large number of suspicious shopping sites. While these websites appear to be Japanese shopping sites in the search results, once the top directory is accessed it becomes evident that they actually have nothing to do with shopping sites. These sites may have had content illegally placed from outside.

The websites contained numerous strings of brand product names and obfuscated JavaScript.

JPCERT/CC reverse engineered the obfuscated JavaScript and found iframe referencing suspicious shopping sites, as well as JavaScript used for access analysis. It is presumed that these modifications were made to fraudulently manipulate search results.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 260. This was a 17% decrease from 312 in the previous quarter.

The number of scans reported in this quarter was 2,980. This was a 17% decrease from 3,592 in the previous quarter. The ports that the scans targeted are listed in [Chart 5]. Ports targeted frequently were DNS(53/UDP), HTTP(80/TCP) and SMTP(25/TCP).

[Chart 5: Number of scans by port]

Port	Jan	Feb	Mar	Total
53/UDP	267	221	294	782
80/TCP	426	200	149	775
25/TCP	186	212	181	579
22/TCP	114	84	108	306
8080/TCP	134	46	9	189
10000/TCP	49	18	1	68
2632/UDP	23	17	12	52
31385/UDP	17	18	16	51
16358/UDP	27	15	9	51
21/TCP	7	4	35	46
61222/UDP	14	17	10	41
23/TCP	9	16	5	30
3389/TCP	4	2	3	9
445/TCP	2	5	0	7
1433/TCP	0	2	4	6
143/TCP	2	0	3	5
123/UDP	0	1	3	4
443/TCP	2	0	1	3
3306/TCP	0	1	2	3
110/TCP	1	1	1	3
Unknown	15	30	22	67
Monthly Total	1299	910	868	3077

A large number of the DNS communication sources have been confirmed to be hosts in Japan that have become open resolvers. Because open resolvers can be used to carry out DDoS attacks, JPCERT/CC has been contacting organizations and users managing such hosts to request that they review the settings of servers, routers and other relevant devices.

The number of incidents under other categories was 950. This was a 91% increase from 498 in the previous quarter. One of the reasons for the significant increase seen in this quarter was the increase in the number of reports on fast-flux, which makes it difficult to suspend a host used for fraudulent purposes by assigning numerous IP addresses to a single domain, and switching the IP addresses with high frequency.

4. Incident Handling Case Examples

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

[Coordination involving domestic websites modified to direct visitors to a site with a .pw domain]
In early March, JPCERT/CC received a report on a suspicious iframe found embedded in the websites of a number of Japanese companies. The iframe was directing visitors to a URL with a .pw domain. .pw domains are not subject to registration restriction by the user's address (location), etc., and they are also available to individuals. Compromised websites had a fraudulent iframe embedded in an HTML file or a JavaScript file. JPCERT/CC confirmed that the URL with a .pw domain to which the iframe directs visitors redirects the visitors to yet another site, where an attack is carried out exploiting the vulnerabilities of a number of applications. One of the vulnerabilities used in the attack was in Adobe Flash Player (CVE-2015-0311), which was fixed at the end of January 2015.

JPCERT/CC requested the administrators of the compromised websites to investigate and address the issue.

[Coordination involving overseas servers installed with a file used by financial malware]
In mid-February, JPCERT/CC received information about a number of overseas servers installed with a file that is downloaded to computers infected by financial malware. This financial malware is known to obtain a configuration file that contains the information of a Japanese bank from an overseas server, and when the relevant Internet banking site is accessed with the infected computer, it obtains JavaScript from another overseas server to generate a web form which is used to steal entered information.

JPCERT/CC has contacted the overseas hosting operator that manages the servers where the configuration file and JavaScript were installed, and requested the operator to take appropriate measures.

JPCERT/CC was later notified by the operator that the issue had been addressed, and confirmed that the files were actually removed.

[Coordination involving server applications accessible from outside]
Around mid-February, a German academic organization released information about the existence of numerous servers running the database application MongoDB without adequate access control. As a result, these servers were accessible from outside to view information and susceptible to manipulation. Around the same time, JPCERT/CC was contacted by a German academic CSIRT and received a list of hosts in Japan that did not restrict access to server applications including MongoDB.

JPCERT/CC contacted the hosting operators that manage the hosts on the list, and requested them to check with the users whether the settings were intended.

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

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

○ 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 2014 Fiscal Year".