JPCERT-IR-2014-04
Issued: 2014-10-09

JPCERT/CC Incident Handling Report [July 1, 2014 – September 30, 2014]

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 July 1, 2014 through September 30, 2014.

[*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]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports [*2]	1494	1347	1797	4638	4517
Number of Incidents[*3]	1474	1203	1711	4388	4260
Cases Coordinated[*4]	745	550	830	2125	2134

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

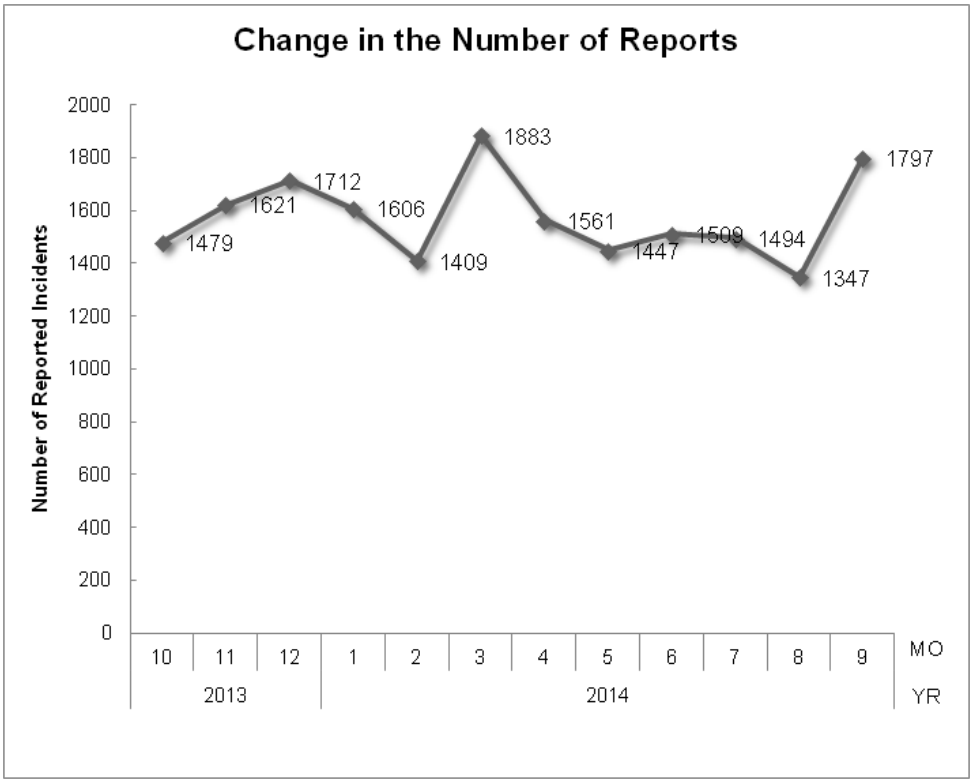
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

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

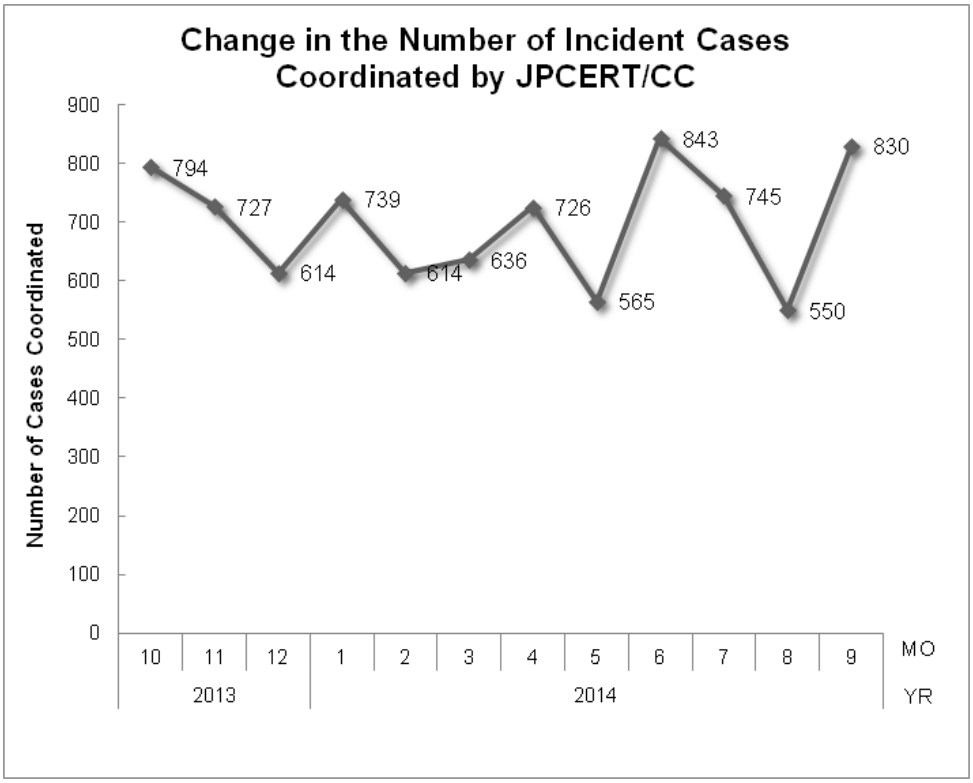
to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,638. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,125. When compared with the previous quarter, the total number of reports increased by 3%, and the number of cases coordinated decreased by 0.4%. When compared with the same quarter of the previous year, the total number of reports decreased by 54%, and the number of cases coordinated decreased by 12%.

[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]



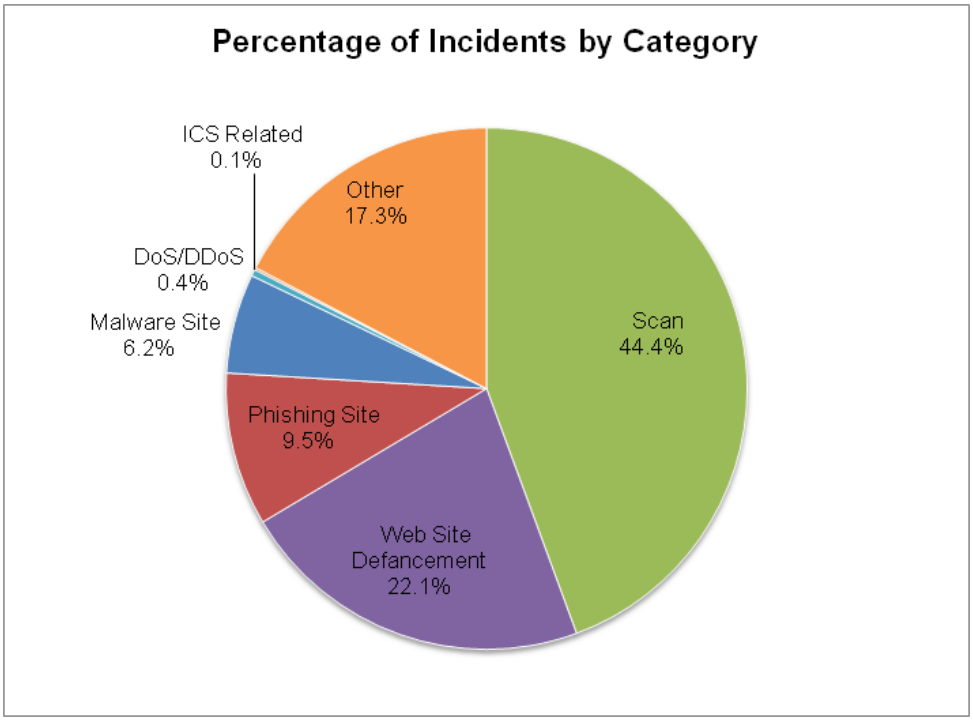
[**Figure 2:** Change in the Number of Incident Cases Coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on each incident category, please see "Appendix 1 - Incident Categories". [Chart 2] shows the number of incidents received per category in this quarter.

[Chart 2: Number of Incidents per Category]

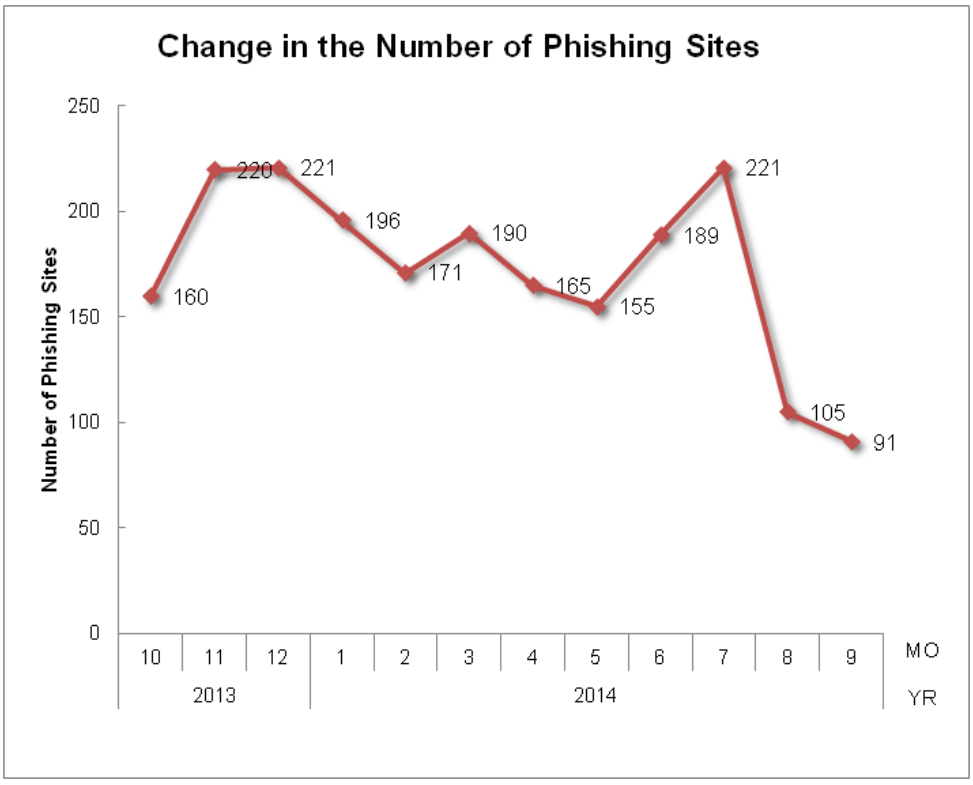
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	221	105	91	417	509
Website Defacement	388	187	393	968	1123
Malware Site	76	123	72	271	194
Scan	636	563	749	1948	1611
DoS/DDoS	7	0	11	18	88
ICS Related	0	0	6	6	0
Other	146	225	389	760	735

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 44.4%, and incidents categorized as website defacement made up 22.1%. Also, incidents categorized as phishing sites represented 9.5% of the total.

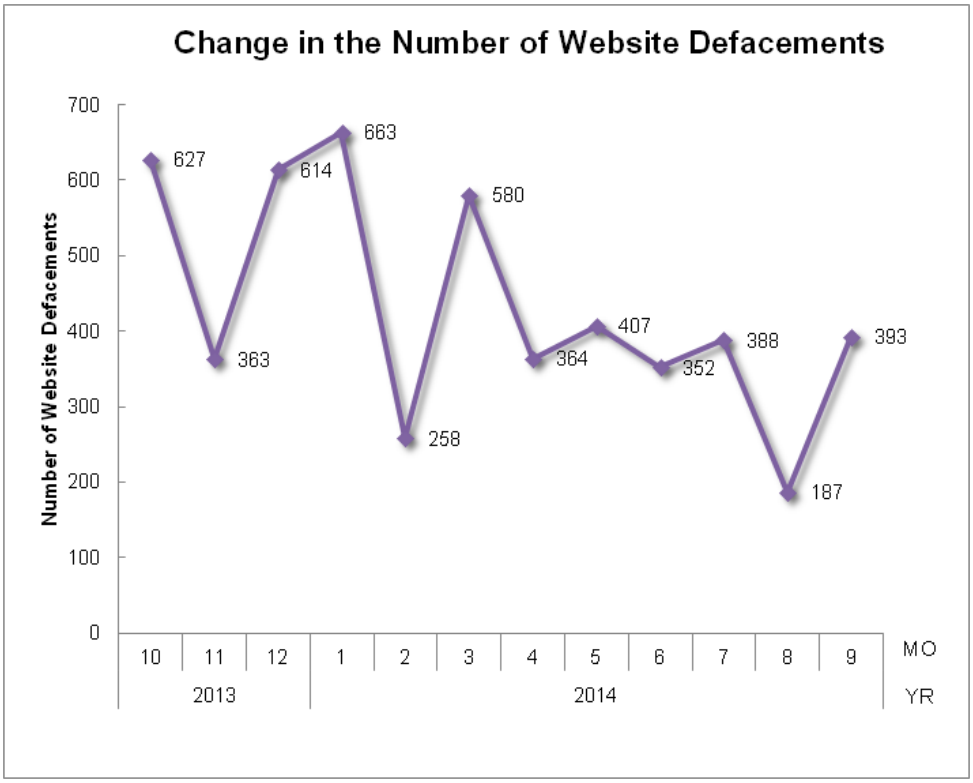


[Figure 1: Percentage of Incidents by Category

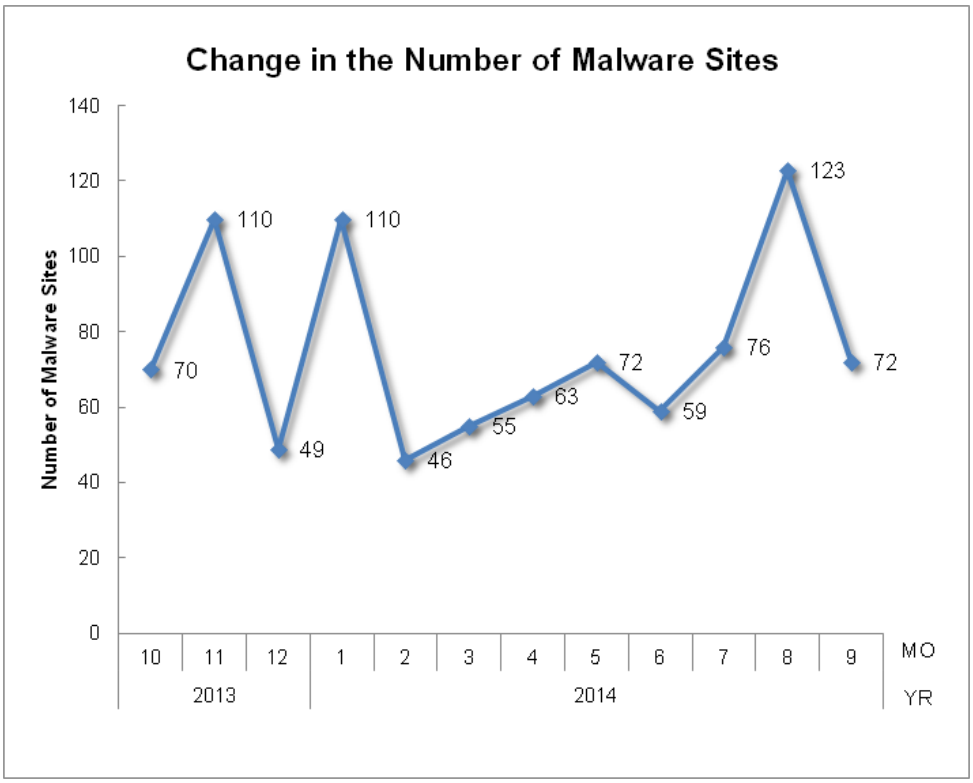
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



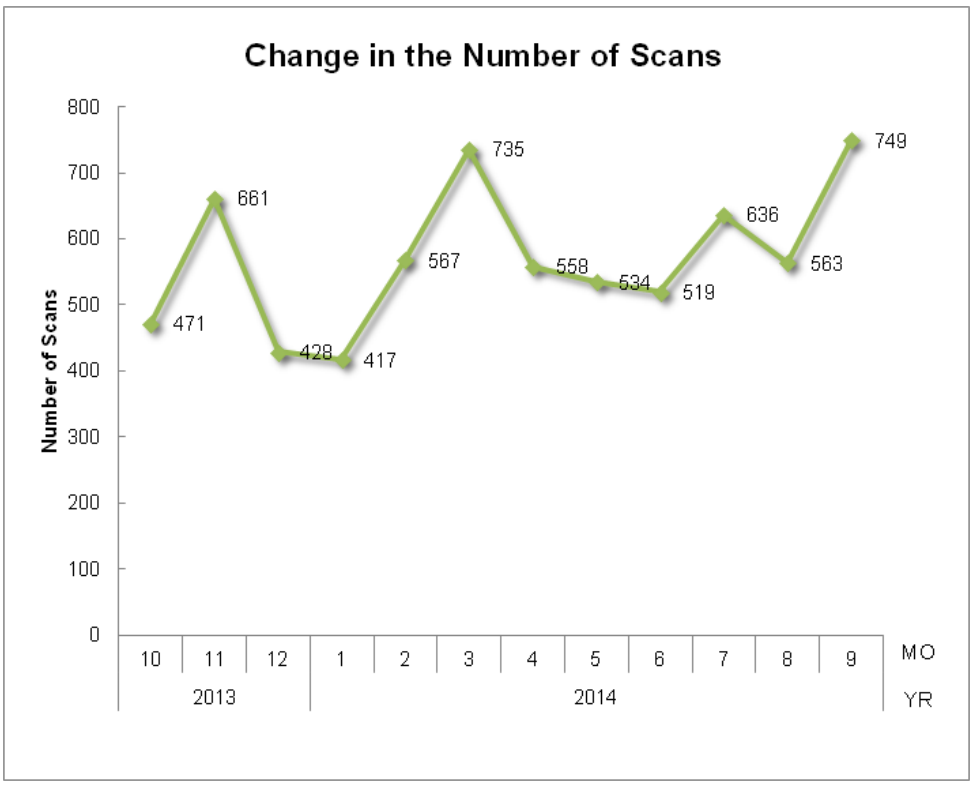
[**Figure 4:** Change in the number of phishing sites]



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

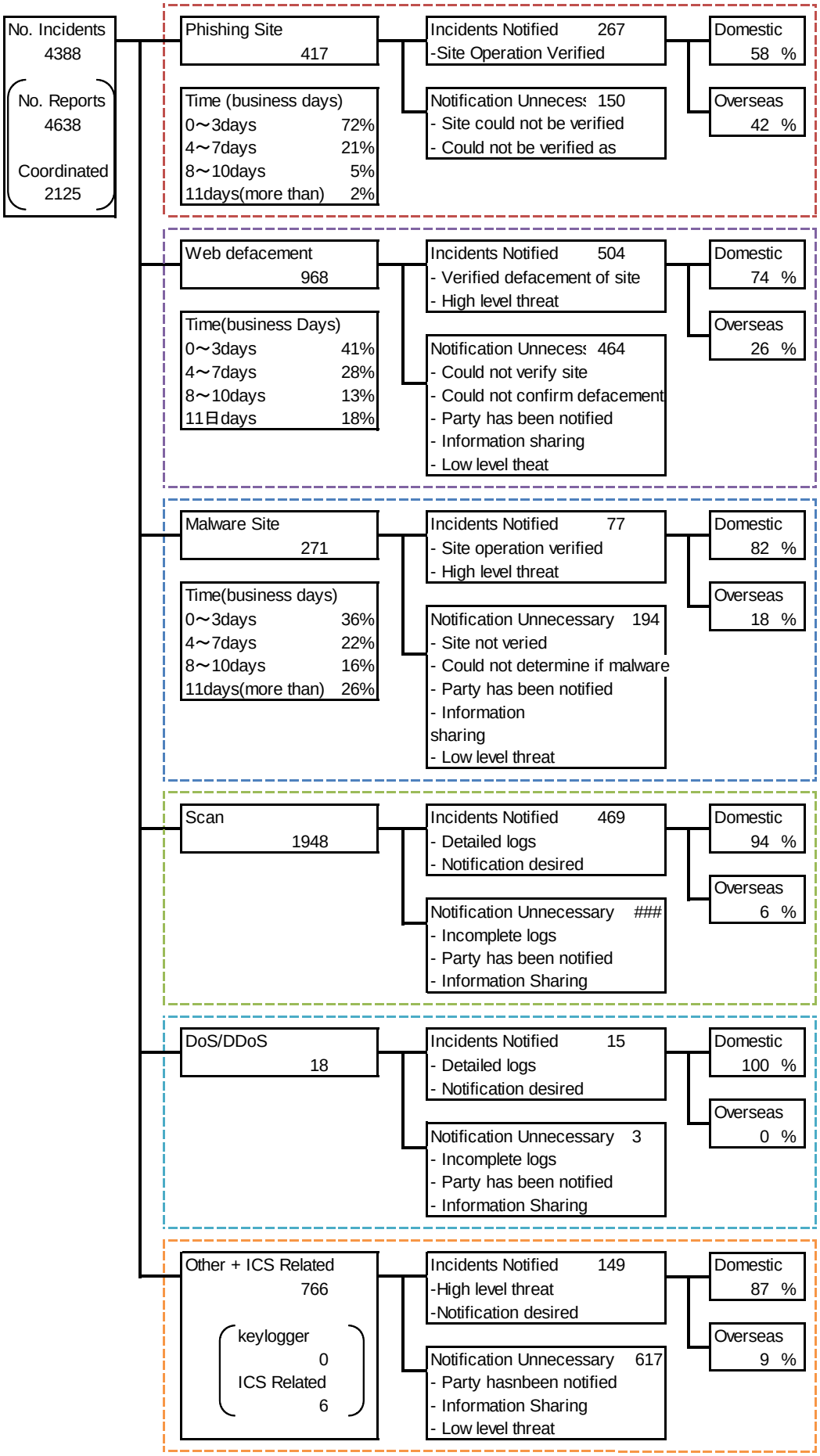


[**Figure 6:** Change in the number of malware sites]



[**Figure 7:** Change in the number of scans]

[Figure 8] provides an overview as well as a breakdown of the incidents that were coordinated / handled.



[Figure 8: Breakdown of Incidents Coordinated / Handled]

3. Incident Trends

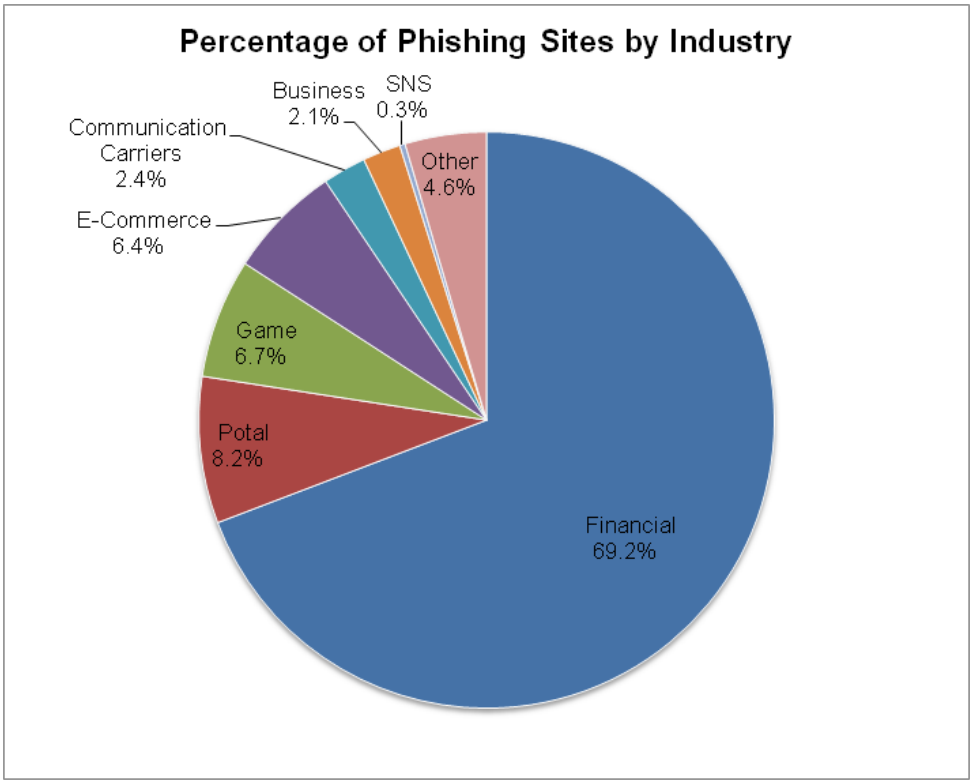
3.1. Phishing Site Trends

417 reports on phishing sites were received in this quarter, representing an 18% decrease from 509 of the previous quarter. This marks an 11% decrease from the same quarter last year (469). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 3], and a breakdown by industry is shown in [Figure 9].

[Chart 1: Number of Phishing Sites by Domestic/Overseas Brand]

Phishing Site	Jul	Aug	Sep	Domestic/ Overseas Total (%)
Domestic Brand	99	26	14	139(33%)
Overseas Brand	73	63	53	189(45%)
Unknown Brand [*5]	49	16	24	89(21%)
Monthly Total	221	105	91	417(100%)

[*5] "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[**Figure9:** Percentage of phishing sites by industry]

During this quarter, there were 139 phishing sites that spoofed domestic brands, which was a 17% decrease from 167 of the previous quarter. And there were 189 phishing sites that spoofed overseas brands, which was a 16% decrease from 226 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 69.2 % spoofed websites of financial institutions, and 6.7% spoofed online gaming services. Domestically and overseas, the industry that had the most phishing sites was the financial sector.

Phishing sites spoofing domestic financial institutions vary in the rate of occurrence depending on the time of year. In July and late September, a large number of cases were observed where users were led from an overseas website apparently set up with a fraudulent file to a phishing site allocated with an IP address of a domestic telecommunications operator; in August through early September, however, there were only sporadic reports of such cases.

In July through August, a large number of reports have been received on phishing sites spoofing domestic online gaming services, but reports significantly decreased in September.

There were also a number of reports on phishing sites spoofing web-based e-mail services of domestic telecommunications operators. It is believed that such phishing sites are set up with an aim to steal the credentials of web-based e-mail to send spam and phishing mails.

The parties that JPCERT/CC contacted for coordination of phishing sites were 58% domestic and 42% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 55%, overseas: 45%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 968. This was a 14% decrease from 1,123 of the previous quarter.

From around the end of August, a large number of reports have been received on web pages embedded with fraudulent JavaScript code.
As with defacements previously seen, such fraudulent code was characterized by script tags appended with comment tags that include a 6-digit hex number. Since a number of patterns can be observed in the destination URLs that such JavaScript code leads to, a number of different types of defacements could exist. JPCERT/CC has confirmed that the final destination sites exploit the vulnerability of computer applications to download and execute malware.

Given the continuing occurrence of website defacements, JPCERT/CC has issued an alert in August calling for early implementation of preventive measures.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 271. This was a 40% increase from 194 of the previous quarter.

The number of scans reported in this quarter was 1,948. This was a 21% increase from 1,611 of the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were http (80/tcp), smtp (25/tcp) and dns (53/udp).

[Chart 2: Number of Scans by Port]

Port	Jul	Aug	Sep	Total
80/tcp	265	322	323	910
25/tcp	281	137	210	628
53/udp	62	52	172	286
22/tcp	57	47	38	142
16358/udp	0	7	18	25
61222/udp	0	5	16	21
21/tcp	7	6	7	20
2632/udp	0	7	11	18
31385/udp	0	6	11	17
3389/tcp	4	5	4	13
445/tcp	3	4	2	9
23/tcp	3	3	2	8
1433/tcp	1	0	2	3
143/tcp	1	0	2	3
icmp	2	0	0	2
7778/tcp	2	0	0	2
5900/tcp	2	0	0	2
5000/tcp	1	1	0	2
443/tcp	2	0	0	2
110/tcp	1	0	1	2
Other/tcp	0	1	4	5
Other/udp	1	0	6	7
Unknown	1	3	27	31
Monthly Total	696	606	856	2158

4. Incident Handling Case Examples

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

[Coordination involving an overseas HTTP proxy site]
Early in July 2014, JPCERT/CC was contacted by a number of organizations in Japan reporting the existence of mock websites closely resembling their own that might be an attempt to steal credentials. The FQDNs of these websites all had the suffix domain common to the legitimate sites' FQDNs added and were apparently implemented by a web-based proxy.

JPCERT/CC contacted the administrator of the website that appeared to be the proxy in order to confirm the intent of the website. The administrator responded that the website was not a phishing site, and was operated with the aim of bypassing web filtering and keeping the browsing source confidential. The administrator offered to remove any website from the proxy target if requested by the website owner. JPCERT/CC communicated the website administrator's intent to the reporting organizations, and informed them that they could be removed from the proxy target if they so request.

[Coordination involving phishing sites using .co.vu domain]
In the first half of July 2014, phishing sites spoofing domestic online gaming services were using free domain .co.vu in large amounts. Since the .vu domain is a top-level domain allocated to the Republic of Vanuatu, JPCERT/CC notified PacCERT, the CSIRT with jurisdiction over the Pacific Islands, that the .vu domain was being abused and requested that the matter be addressed. JPCERT/CC later confirmed that all the .co.vu domains used for the phishing sites were suspended.

Subsequently, phishing sites using .cu.cc domain were found in early August, and those using .pw domain were found in mid-August, but JPCERT/CC has confirmed by the latter half of August that all these have been removed.

[Information found from a C&C server of a botnet led to identification of bots in Japan]
In late July 2014, JPCERT/CC received a report from the Croatian National CSIRT regarding bots using IP addresses in Japan. According to the report, investigation of the bot information found in a C&C server of a botnet showed that many of the bots used IP addresses within a range allocated to Japan.

Based on the bots' communication logs provided by the Croatian National CSIRT, JPCERT/CC requested the organizations that own the IP addresses of the hosts identified as a bot to verify the possible existence of suspicious communication or malware on the hosts in question. As a result, a number of organizations that were notified confirmed the existence of communication matching the logs and they were already aware of the malware infection.

Request from JPCERT/CC

JPCERT/CC attempts to prevent the spread of damages caused by incidents and the recurrence of incidents by understanding the occurrence and trends and also contacting the source of the attack to coordinate in suspending the websites depending on the circumstances. Issuing alerts to notify users to apply countermeasures is also a part of our activities.

JPCERT/CC highly appreciate your cooperation in reporting any information; please refer to the following URLs on how 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: Incident Categories

JPCERT/CC defines each incident included in the reports as follows:

○ Phishing Site

A "Phishing Site" refers to a site that spoofs a legitimate site provided by a service provider (of banks, auction websites etc.), which intends to obtain user ID's, passwords, credit card numbers, etc. for “phishing fraud” purposes.

JPCERT/CC categorizes the following as "phishing sites"

- **Websites that imitate websites of financial institutions, credit card companies etc.**
- **Websites aimed at leading users to phishing sites**

○ Website Defacement

"Website Defacement" refers to a website where the contents have been re-written (including embedding of scripts not intended by the administrator) by an attacker or malware.

JPCERT/CC categorizes the following as "website defacement"

- **Websites where malicious scripts or iframes are embedded by an attacker or malware**
- **Websites where information has been altered as a result of an SQL injection attack**

○ Malware Site

"A Malware Site" refers to a website where a PC may be infected by malware when viewing the site or a website that hosts malware for an attack.

JPCERT/CC categorizes the following as "malware site"

- **Websites that attempt to infect its visitors’ PC with malware**
- **Websites where malware is hosted by an attacker**

○ Scan

"Scan" refers to access by attackers (that do not affect the system) to search for vulnerabilities (security holes, etc.) in a server, PC or any system targeted for an attack to gain unauthorized access. Attempts to infect with malware are also included here.

JPCERT/CC categorizes the following as "scan"

- **Vulnerability searching (checking program versions, service operation etc.)**
- **Attempts at intrusion (that do not result in intrusion)**
- **Attempts (that do not result in infection) to infect with malware (virus, bots, worms, etc.)**
- **Brute force attacks against ssh, ftp, telnet, etc. (that do not result in successful attack)**

○ DoS/DDoS

"DoS / DDoS" refers to an attack against network resources of servers, PC's and other devices that form the network, which results in not being able to provide services.

JPCERT/CC categorizes the following as "DoS / DDoS"

- **Attacks that exhaust network resources as a result of large number of communications**
- **Bad response or suspension of server programs due to large amount of access**
- **Interference of services by forcing reception of a large number of e-mails (error e-mails, spam e-mails, etc.)**

○ ICS Related Incidents

"ICS Related Incidents" refer to any incidents related to industrial control systems or any type of plant.

JPCERT/CC categorizes the following as "ICS related incidents"

- **Industrial control systems that can be attacked over the internet**
- **Servers that communicate with malware targeting control systems**
- **Attacks that cause malfunctioning of industrial control system**

○ Other

"Other" refers to incidents that cannot be categorized in any of the above.

For example, JPCERT/CC categorizes the following as "other"

- **Unauthorized intrusions into a system leveraging a vulnerability**
- **Unauthorized intrusion as a result of a successful brute force attack against ssh, ftp, telnet, etc.**
- **Information stealing by malware that contains a key logging function**
- **Malware (virus, bots, worms, etc.) infections**

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Information Security Countermeasure Promotion Activities for the 2013 Fiscal Year".