JPCERT-IR-2015-01
Issued: 2015/01/14

JPCERT/CC Incident Handling Report
[October 01, 2014 – December 31, 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 October 01, 2014 through December 31, 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

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

[Table1: Number of Incident Reports]

	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports [*2]	1607	1957	2667	6231	4638
Number of Incidents[*3]	1495	1707	2404	5606	4388
Cases Coordinated[*4]	877	768	692	2337	2125

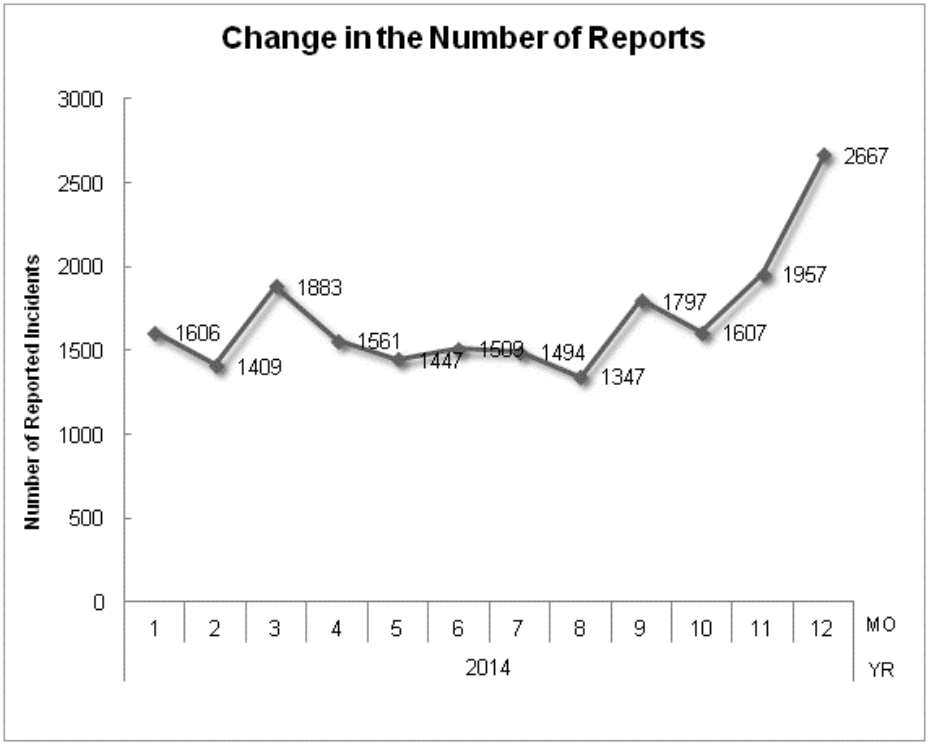
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX

[*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.

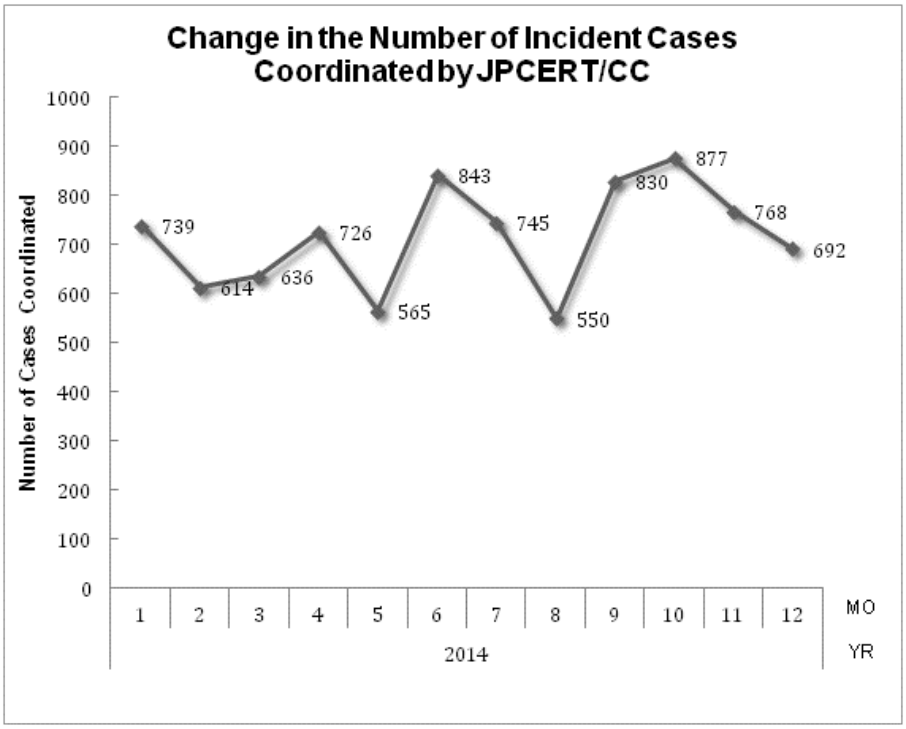
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 6,231. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,337. When compared with the previous quarter, the total number of reports increased 34%, and the number of cases coordinated increased 10%. Year on year, the total number of reports increased 29%, and the number of cases coordinated increased 9%.

[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**]



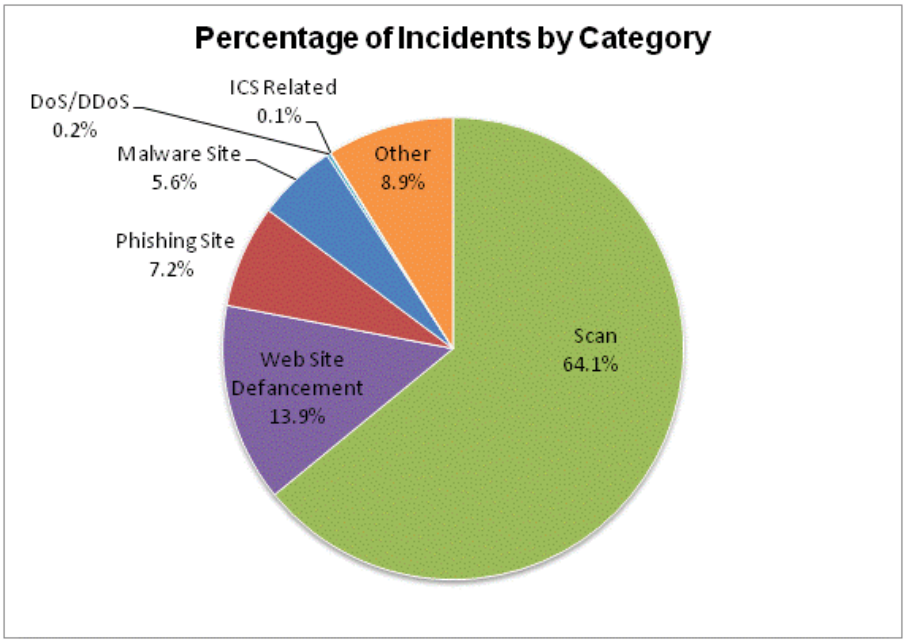
[Figure 2: **Change in the Number of Incident Cases Coordinated**]

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". [Table 2] shows the number of incidents received per category in this quarter.

[**Table 2: Number of Incidents per Category**]

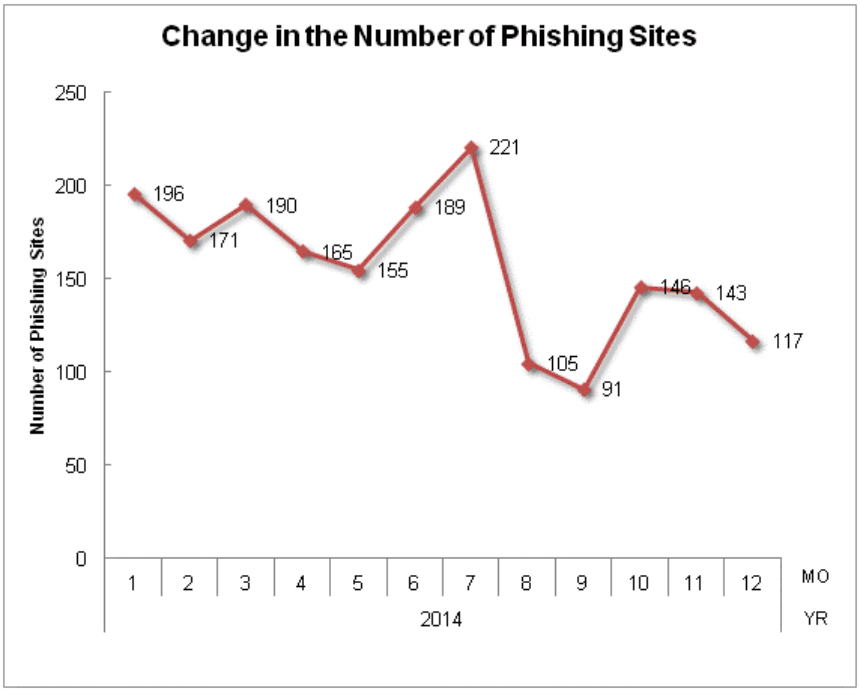
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	146	143	117	406	417
Website Defacement	321	220	240	781	968
Malware Site	110	96	106	312	271
Scan	738	1130	1724	3592	1948
DoS/DDoS	1	0	13	14	18
ICS Related	0	3	0	3	6
Other	179	115	204	498	760

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 64.1%, and incidents categorized as website defacement made up 13.9%. Also, incidents categorized as phishing sites represented 7.2% of the total.

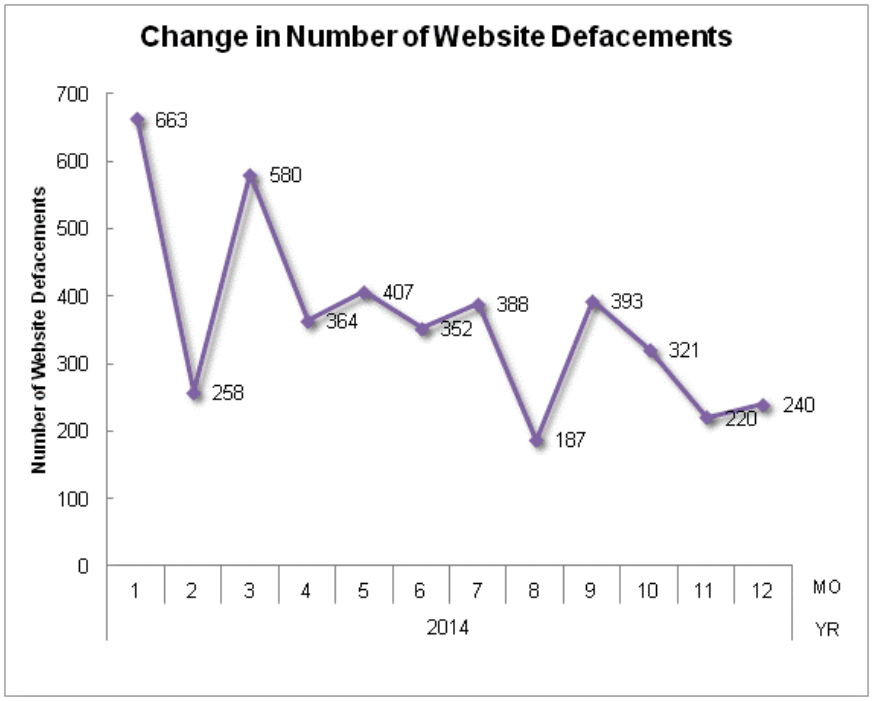


[Figure 3: **Percentage of Incidents by Category**]

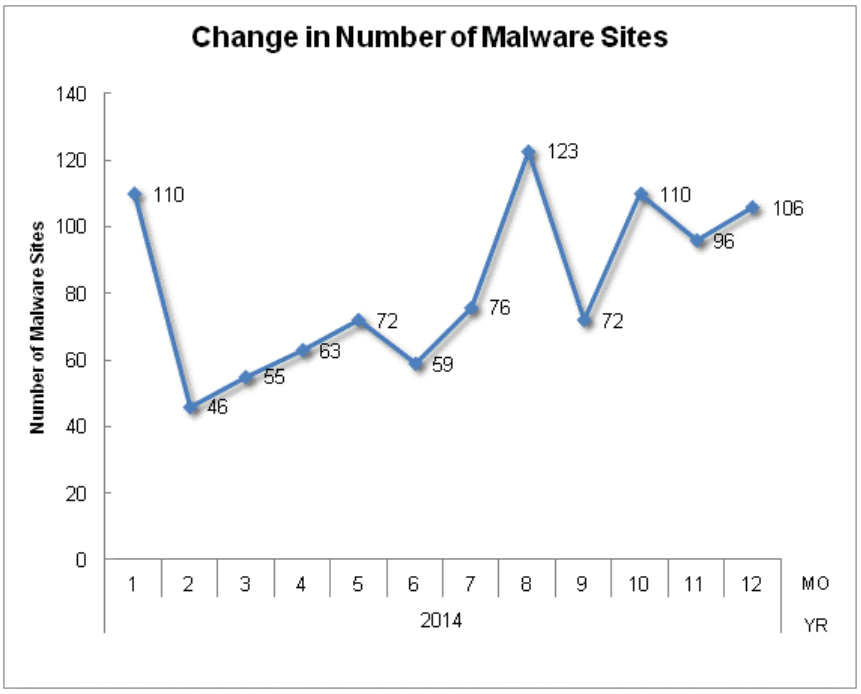
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



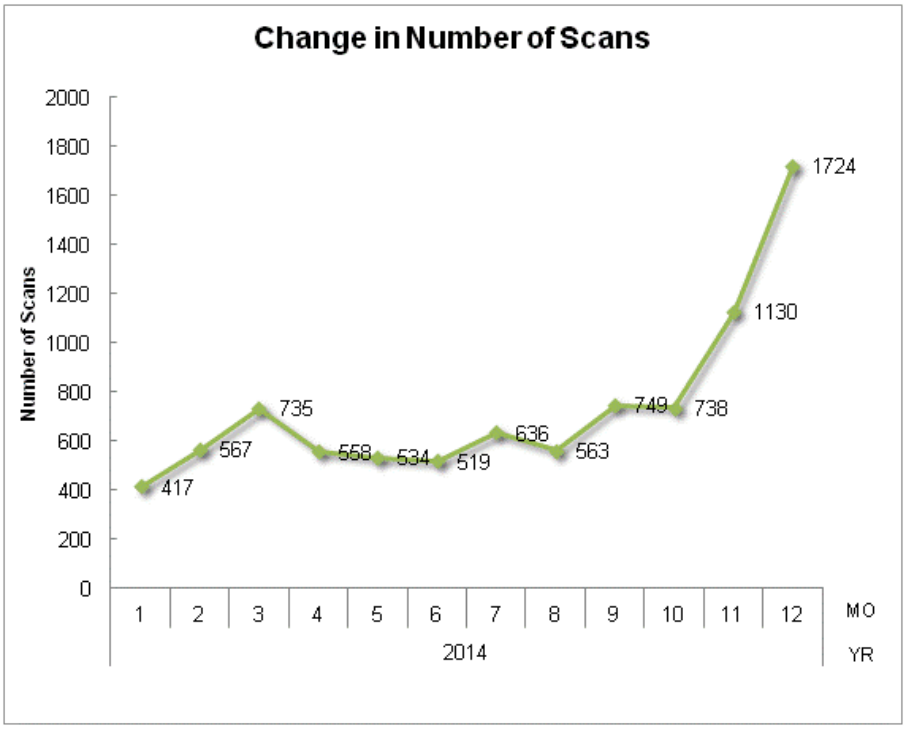
[Figure 4: **Change in the number of phishing sites**]



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

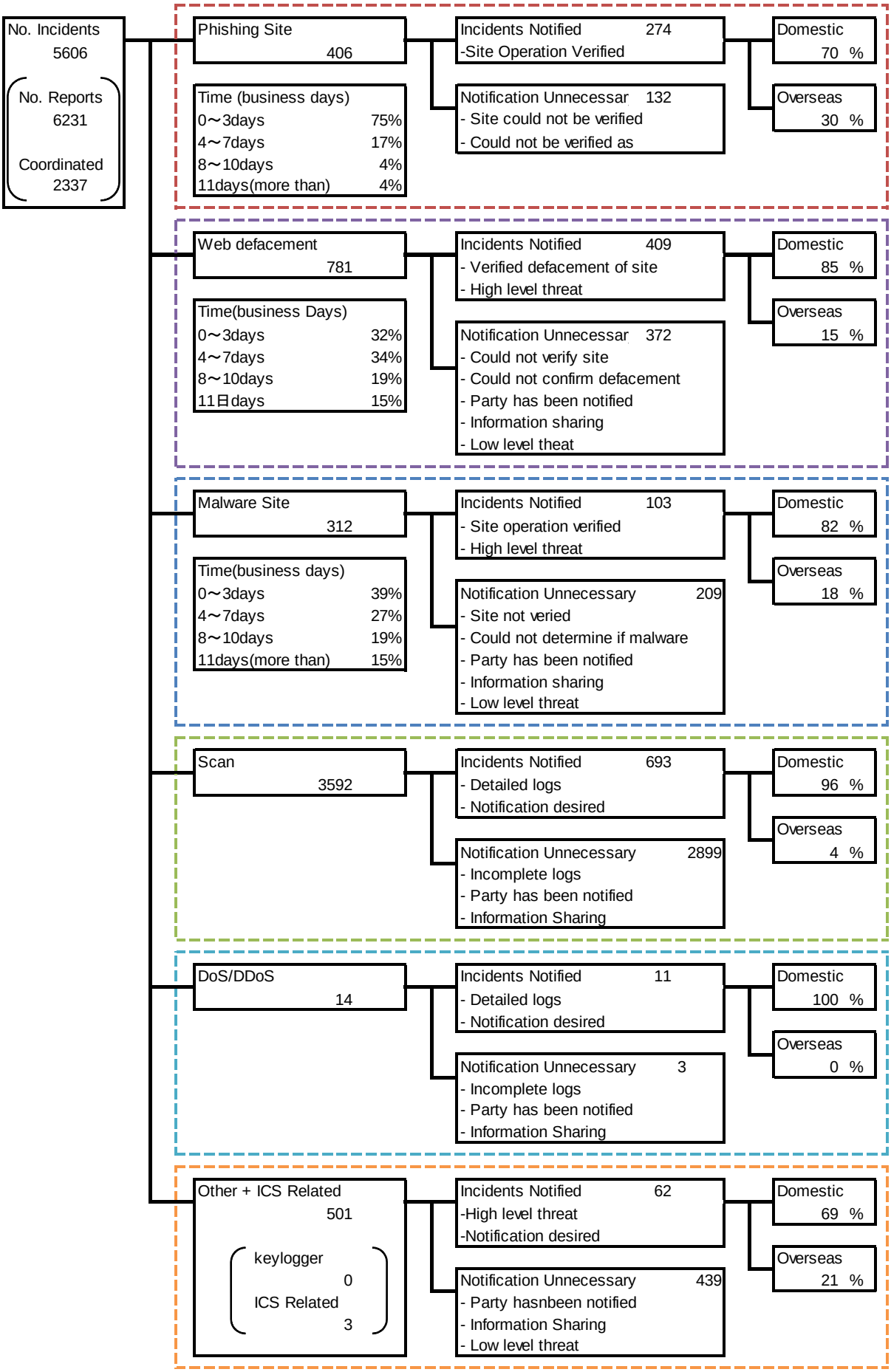


[Figure 6: **Change in the number of malware sites**]



[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

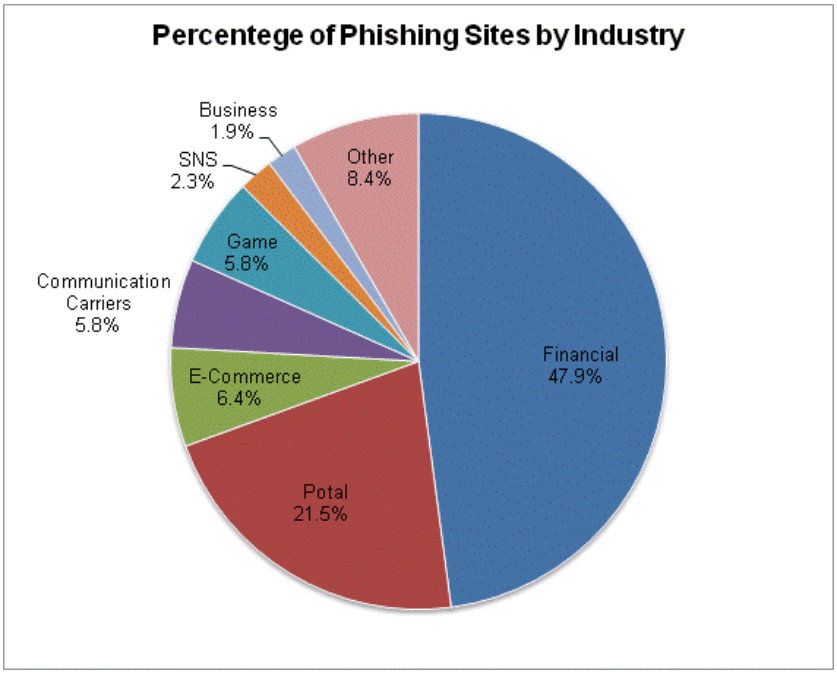
3.1. Phishing Site Trends

406 reports on phishing sites were received in this quarter, representing a 3% decrease from 417 of the previous quarter. This marks a 32% decrease from the same quarter last year (601). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Table 3], and a breakdown by industry is shown in [Figure 9].

[**Table 3**: **Number of Phishing Sites by Domestic/Overseas Brand**]

Phishing Site	Oct	Nov	Dec	Domestic/ Overseas Total (%)
Domestic Brand	41	23	11	75(18%)
Overseas Brand	78	91	67	236(58%)
Unknown Brand*[5]	27	29	39	95(23%)
Monthly Total	146	143	117	406(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 9: Percentage of phishing sites by industry**]

During this quarter, there were 75 phishing sites that spoofed domestic brands, decreasing 46% from 139 of the previous quarter. And there were 236 phishing sites that spoofed overseas brands, increasing 25% from 189 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 47.9 % spoofed websites of financial institutions, and 21.5% spoofed portal sites. Domestically and overseas, the industry that had the most phishing sites was the financial sector.

During this quarter, the number of phishing sites that spoofed domestic brands showed a marked decrease from the previous quarter. This decrease was due to the drop seen in October of the number of phishing sites spoofing domestic financial institutions—none has been identified since November—which were seen in large numbers during the previous quarter. While the number of phishing sites that spoof domestic online gaming services has also decreased from the previous quarter, JPCERT/CC has been continually receiving reports on such sites since the end of October.

The parties that JPCERT/CC contacted for coordination of phishing sites were 70% domestic and 30% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 58%, overseas: 42%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 781. This was a 19% decrease from 968 of the previous quarter.

A number of malware infection cases confirmed between late November and mid-December were found to be caused by a code that exploits a vulnerability in a Microsoft program (MS14-064). The code was embedded in a web page to which Internet users are directed from another defaced website.

This vulnerability was announced in a security update in November and reported to have been used in targeted attacks to a limited extent. With respect to the instance mentioned above, it is presumed that the attacker analyzed the modification program, obtained the vulnerability informationand developed the code that exploits that vulnerability,in order to embed it in the website in a very short time after the announcement in November. As this instance makes clear, it is recommended that security updates be applied as soon as they are announced, so as not to fall victim to this type of attack.

Further, in a large number of website defacements identified since early December, an obfuscated JavaScript code was embedded at the foot of a web page to direct site visitors to another suspicious website with a URL that looks like "tag[1-2 numeric characters].php". Other cases seen in large numbers included defacements in which an obfuscated JavaScript code and a link to an external site were embedded with the apparent purpose of making certain sites show up prominently in web search results,

which is a type of attack known as SEO poisoning. An instance of an unauthorized web page containing only transfer settings that redirect site visitors to another site apparently set up for the purpose of selling or advertising pharmaceuticals was also found in great numbers.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 312. This was a 15% decrease from 271 of the previous quarter.

The number of scans reported in this quarter was 3,592. This was an 84% increase from 1,948 of the previous quarter. The ports that the scans targeted are listed in [Table 4]. Ports targeted frequently were http (80/tcp), smtp (25/tcp) and dns (53/udp).

During this quarter, JPCERT/CC received a number of reports concerning damages caused by attacks exploiting a vulnerability in GNU bash and domestic IP addresses that were identified as attack sources. In December, there were numerous reports concerning scans targeting 8080/tcp, in which network-attached storage (NAS) devices were used as attack sources.

[**Table 4: Number of Scans by Port**]

Port	Oct	Nov	Dec	Total
80/tcp	185	531	948	1664
25/tcp	129	172	234	535
53/udp	147	182	126	455
22/tcp	97	105	245	447
21/tcp	8	37	47	92
31385/udp	30	23	19	72
2632/udp	38	13	19	70
8080/tcp	4	3	54	61
61222/udp	17	17	25	59
16358/udp	24	12	20	56
10000/tcp	32	0	1	33
53/tcp	2	8	0	10
23/tcp	0	3	5	8
445/tcp	5	2	0	7
3389/tcp	2	4	0	6
1451/tcp	6	0	0	6
143/tcp	3	3	0	6
123/udp	0	6	0	6
80/udp	0	4	0	4
3544/udp	1	1	1	3
22/udp	2	0	0	2
Other	13	18	2	33
Monthly Total	745	1144	1746	3635

4. Incident Handling Case Examples

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

[Coordination involving domain hijacking of domestic websites]
Early in October, an overseas security firm published information about a malicious code embedded in a JavaScript file specified to be loaded on the website of a Japanese company. According to the published information, the code was redirecting site visitors to an external site. JPCERT/CC requested the company concerned to look into the matter and the overseas security firm to provide detailed information.

The information provided by the security firm revealed the possibility that the domain name of the Japanese company had been allocated a false IP address for a certain period in the past. JPCERT/CC examined the domain name's registered information and the record of its past name resolution. As a result of this investigation, it was revealed that a suspicious name server had been registered as the name server of the domain name for a certain period, and that the domain name had been resolved into a fraudulent IP address during this period.

The Japanese company in question was not able to identify any evidence that JavaScript used on its website had been altered, which also indicates the high likelihood that the domain name had been hijacked and site visitors were being redirected to a host installed with a fraudulent JavaScript.

Further investigation revealed the existence of similar cases with the domain names of a number of other organizations in Japan. JPCERT/CC advised those organizations to request the registrar to investigate the possibility that the domain registration information had been fraudulently altered. Given the severity of the impact, an alert was issued on November 5.

[Coordination involving a document sharing site where the database information of domestic organizations was uploaded]
In late November, JPCERT/CC received a report that information that appears to have leaked from the databases of a number of domestic organizations through a vulnerable website was published on an overseas text sharing site. JPCERT/CC notified the administrator of the text sharing site that information that may have leaked from Japanese organizations was published on the site. The administrator replied that any unauthorized content will be removed if reported.

JPCERT/CC requested the domestic organizations whose database information may have leaked to look into the matter and advised them to contact the text sharing site administrator if there was any information that needed to be removed. JPCERT/CC also responded to the request of some of the organizations to contact the text sharing site administrator on their behalf.

[Coordination involving SSH brute force attacks that occurred in early December]
In early December, JPCERT/CC received numerous reports from overseas claiming that SSH brute force attacks had been executed from IP addresses in Japan. JPCERT/CC analyzed the logs provided by the reporters and found that in a number of attacks, a specific user account was subjected to login attempts. At around the same time, there were reports from Japanese sources claiming that SSH scans were carried out from hundreds of IP addresses both in Japan and overseas.

Based on the scan logs provided by the reporters, JPCERT/CC requested the organizations managing the IP addresses of the attack source in some of the attacks to look into the matter. As a result, one of the organizations reported an irregular process that appeared to indicate that a malicious file had been installed on a server through a vulnerability in GNU bash, and that SSH scans were being carried out.

Based on this report, it was inferred that the attacks were a part of the consequences of the vulnerability announced at the end of September.

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".