JPCERT-IR-2014-03
Issued: 2014-07-10

JPCERT/CC Incident Handling Report[April 1, 2014 – June 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 April 1, 2014 through June 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

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

[Chart1: Number of Incident Reports]

	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports [*2]	1561	1447	1509	4517	4898
Number of Incidents[*3]	1397	1401	1462	4260	4529
Cases Coordinated[*4]	726	565	843	2134	1989

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

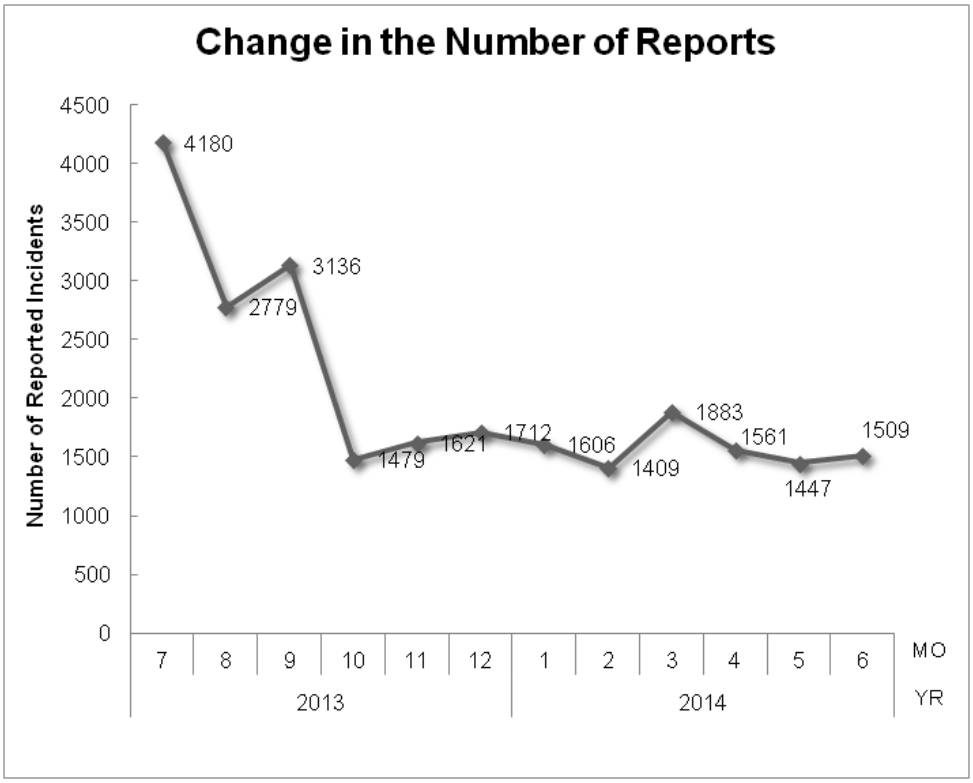
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

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

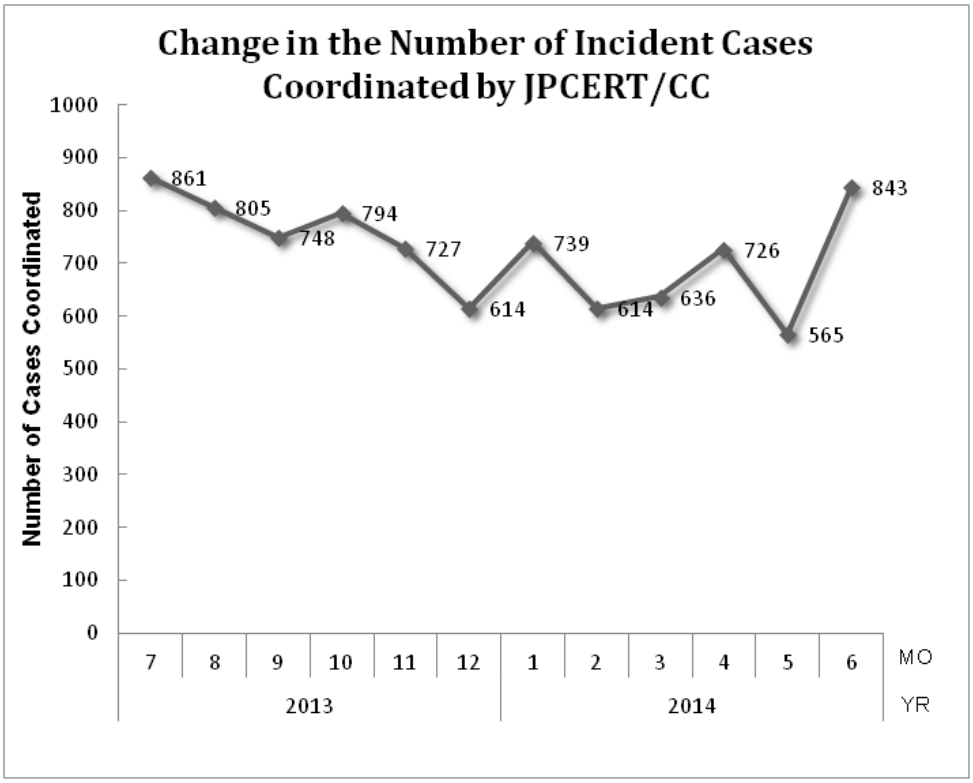
to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,517. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,134. When compared with the previous quarter, the total number of reports decreased by 8%, and the number of cases coordinated increased by 7%. When compared with the same quarter of the previous year, the total number of reports decreased by 52%, and the number of cases coordinated decreased by 2%.

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



[Figure1: Change in the Number of Reports]



[Figure2: Change in the Number of Incident Cases Coordinated]

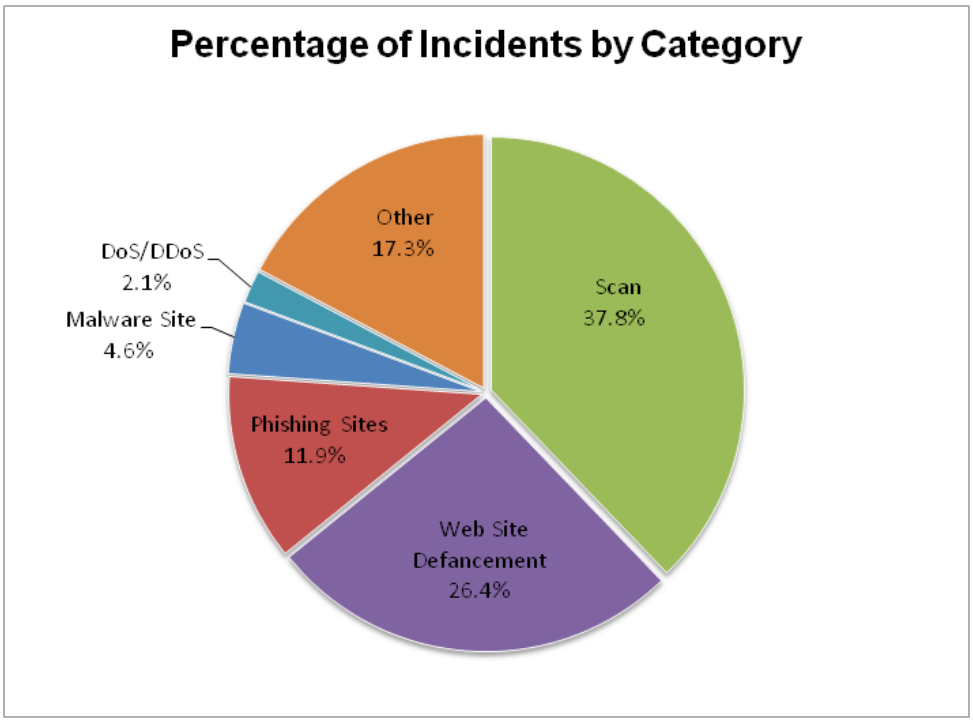
At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on each incident category, please see "Appendix 1 - Incident Categories". [Chart2: Chart2] shows the number of incidents received per category in this quarter.

[Chart2: Number of Incidents per Category]

Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	165	155	189	509	557
Website Defacement	364	407	352	1123	1501
Malware Site	63	72	59	194	211
Scan	558	534	519	1611	1719
DoS/DDoS	50	33	5	88	23
ICS Related	0	0	0	0	0
Other	197	200	338	735	518

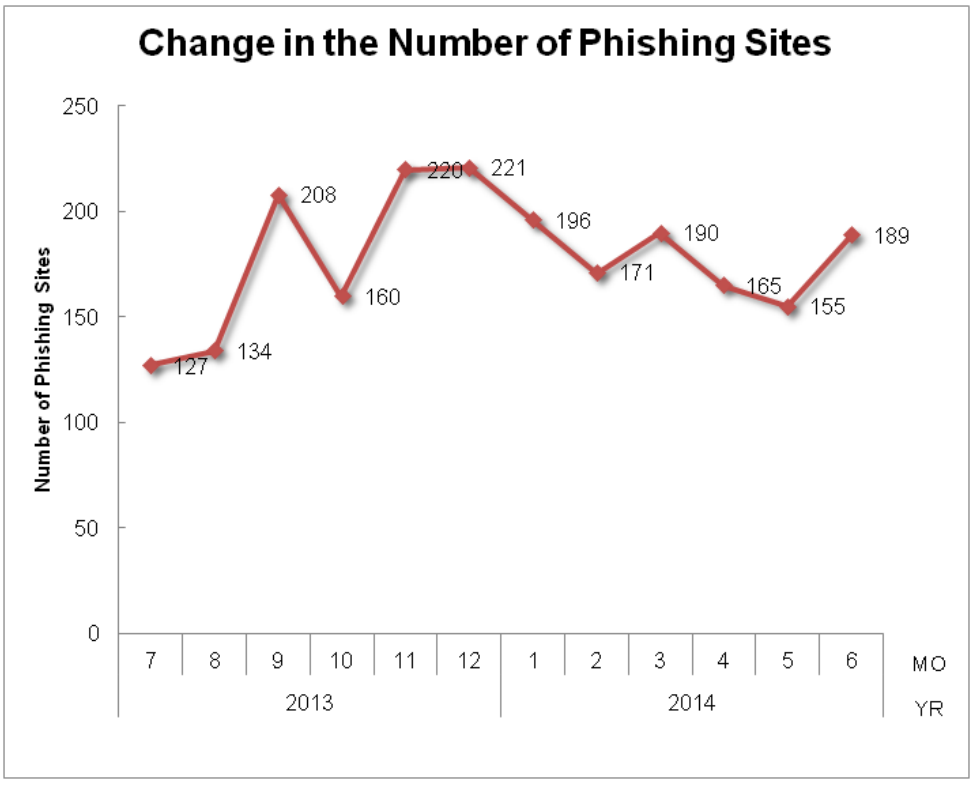
The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure1]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 37.8%, and incidents categorized as website defacementmade up 26.4%. Also, incidents categorized as

phishing sites represented 11.9% of the total.

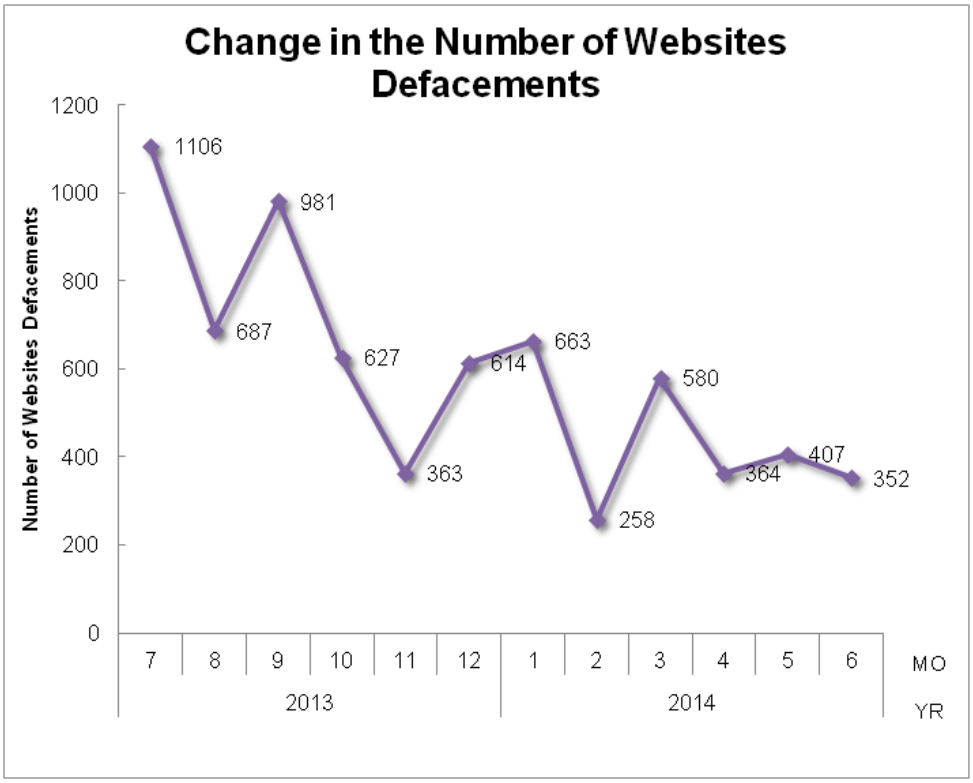


[Figure1: Percentage of Incidents by Category]

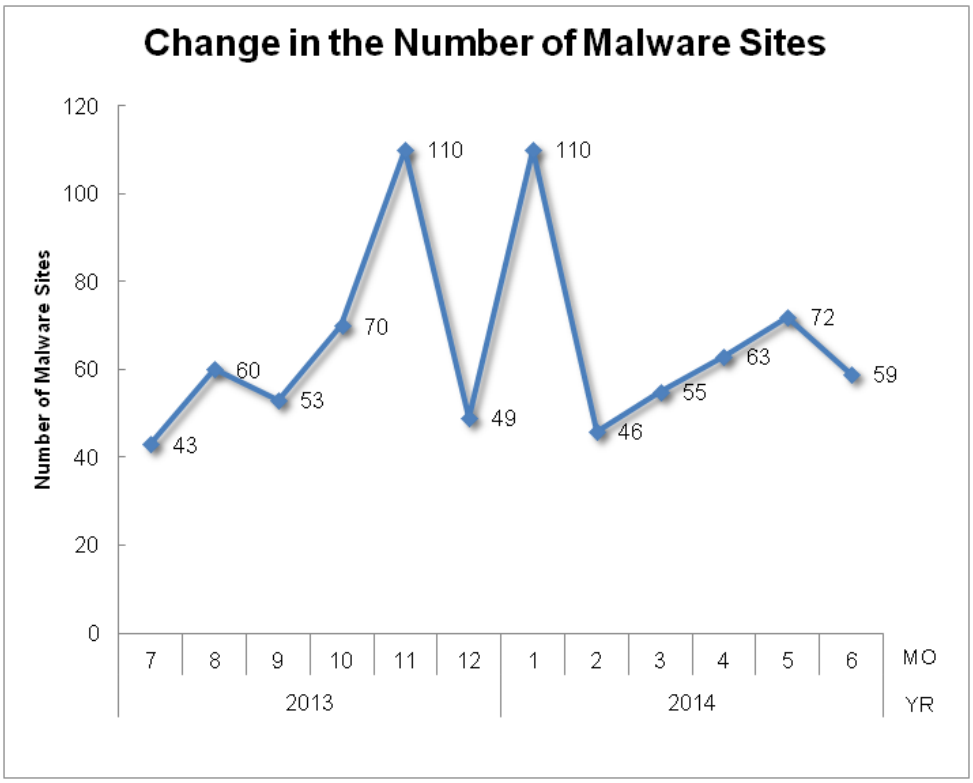
[Figure4] through [Figure7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



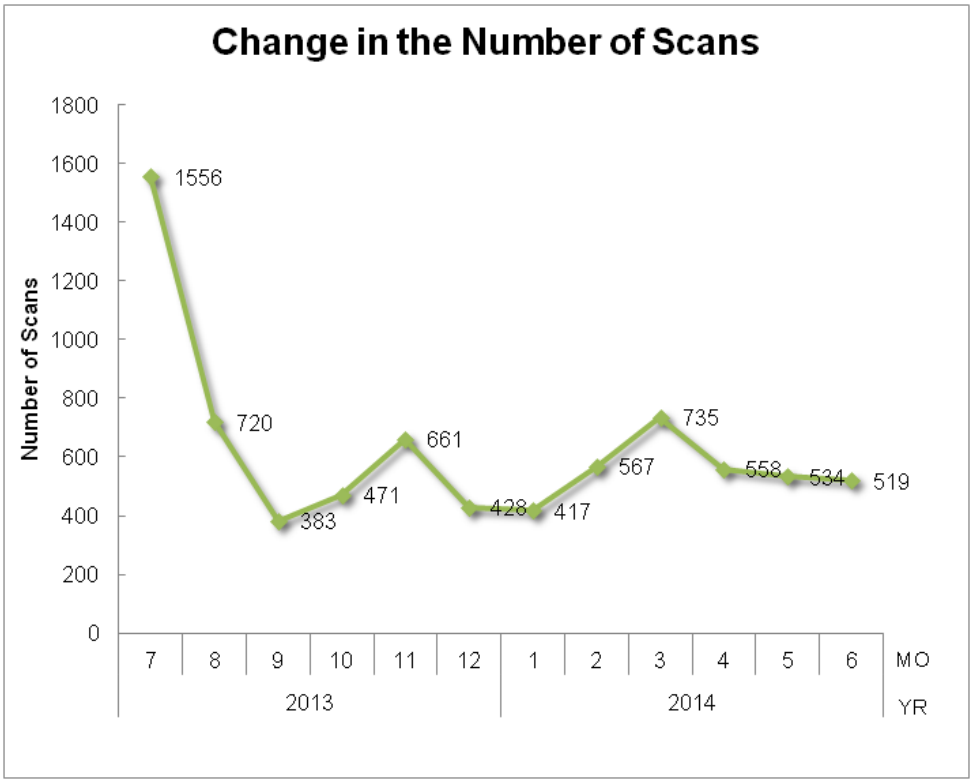
[Figure4: Change in the number of phishing sites]



[Figure5: Change in the number of website defacements]

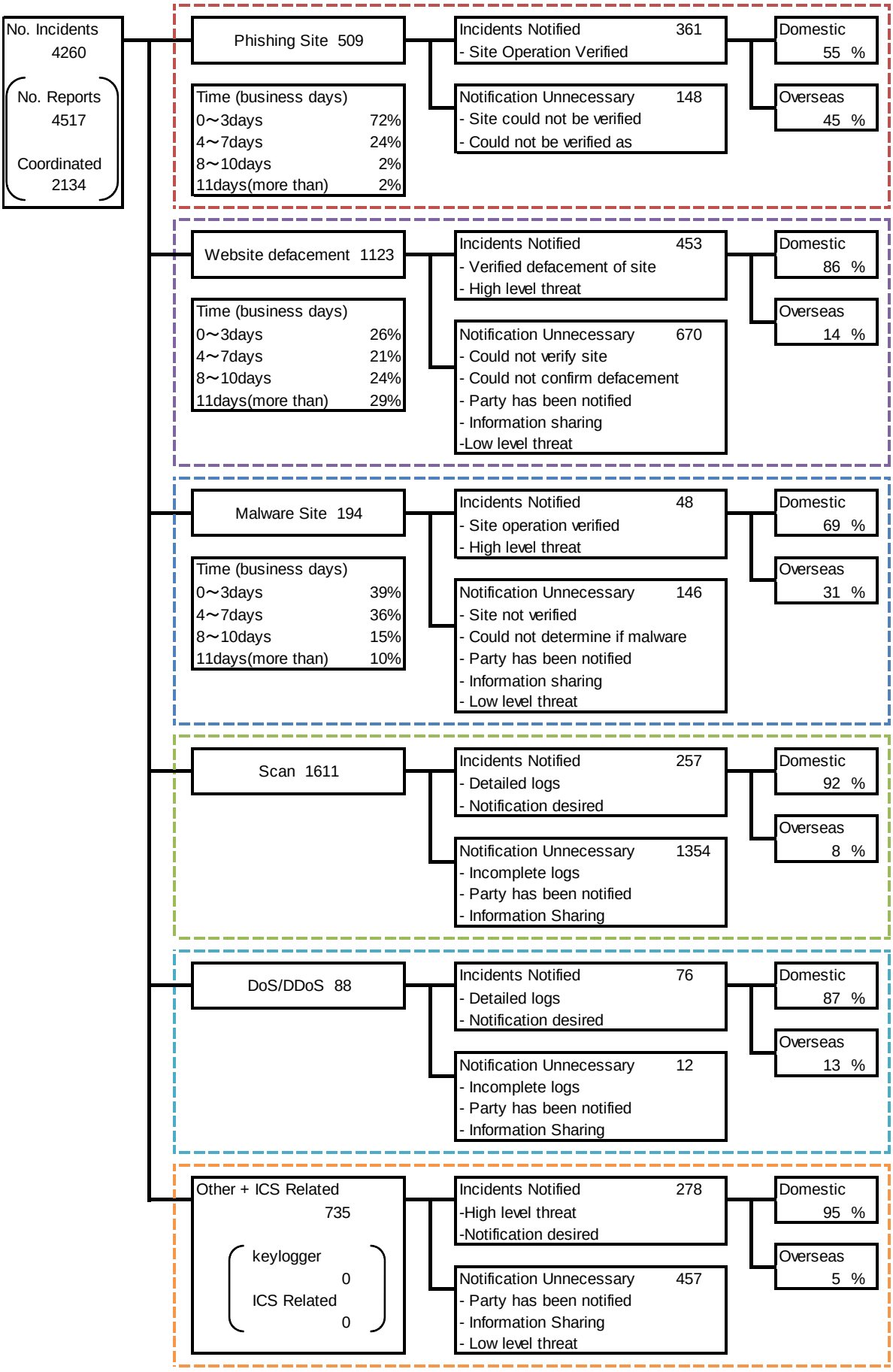


[Figure6: Change in the number of malware sites]



[Figure7: Change in the number of scans]

[] is a breakdown of the incidents that were coordinated / handled.



[Figure8: Breakdown of Incidents Coordinated / Handled]

3. Incident Trends

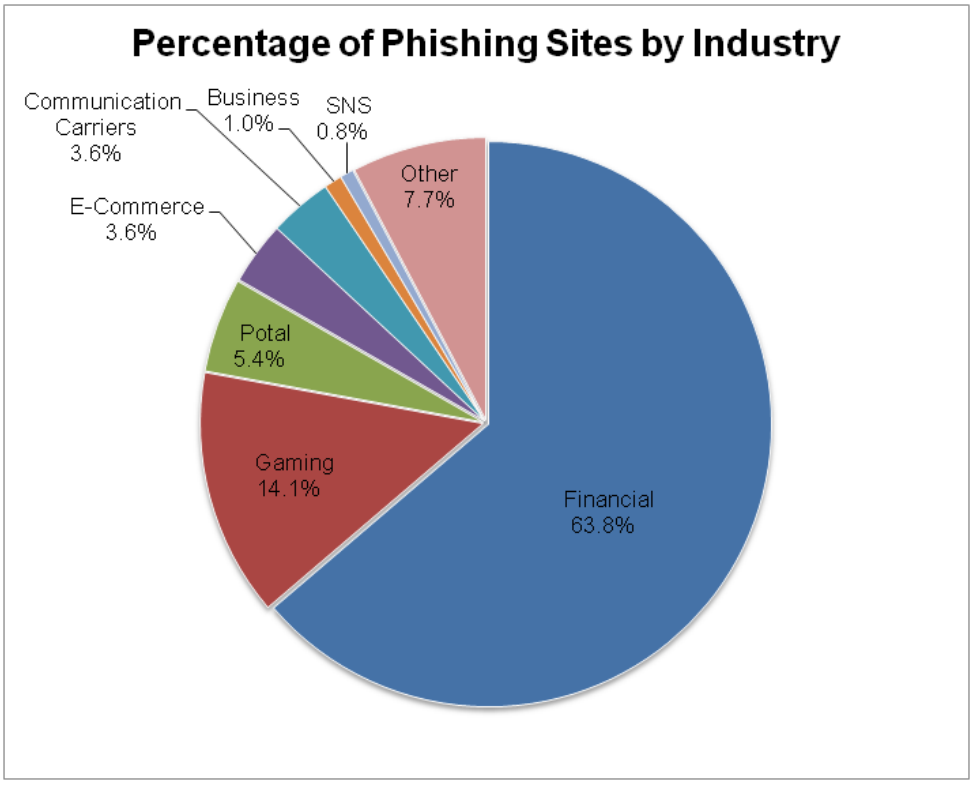
3.1. Phishing Site Trends

509 reports on phishing sites were received in this quarter, representing a 9% decrease from 557 of the previous quarter. This marks a 77% increase from the same quarter last year (287). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart1], and a breakdown by industry is shown in [].

[Chart1: Number of Phishing Sites by Domestic/Overseas Brand]

Phishing Site	Apr	Mar	Jun	Domestic/ Overseas Total (%)
Domestic Brand	50	36	81	167(33%)
Overseas Brand	71	79	76	226(44%)
Unknown Brand [*5]	44	40	32	116(23%)
Monthly Total	165	155	189	509(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 167 phishing sites that spoofed domestic brands, which was a 27% decrease from 229 of the previous quarter. And there were 226 phishing sites that spoofed overseas brands, which was a 21% increase from 187 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 63.8% spoofed websites of financial institutions, and 14% spoofed online gaming services. Domestically and overseas, the industry that had the most phishing sites was the financial sector.

From around mid-June, the number of phishing sites spoofing domestic financial institutions has been increasing. These phishing sites employed a known mechanism in which an overseas website apparently set up with a fraudulent page embedded with code that transfers users to the phishing site. The phishing sites had an IP address dynamically allocated by a domestic telecommunications operator. These sites all had a domain name consisting of "XXX(3 alphabetic characters).co.in," and other commonalities such as the same e-mail address of the domain registrant. One of the cases confirmed had phishing sites for three domestic financial institutions set up on a number of hosts with the same IP address.

A large number of reports have been received on phishing sites that spoof domestic online gaming services. These online gaming phishing sites used free domains such as .tk and .co.vu, or the .pw domain. Phishing sites with the .tk domain used a frame to display the body of a phishing site placed on another domain, and phishing mails contained a URL with the .tk domain. This is assumed to be a device to make it difficult for the main site to be put on the block list.

The parties that JPCERT/CC contacted for coordination of phishing sites were 55% domestic and 45% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 43%, overseas: 57%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 1,123. This was a 25% decrease from 1,501 of the previous quarter.

In the beginning of April, a number of reports were received on cases where domestic companies using an old version of Movable Type had their websites compromised. On these websites, a JavaScript file loaded on a web page was altered and embedded with code that inserts an iframe that guides users to an external website. The external website had a php script incorporated apparently by the attacker to transfer users to a site that exploits vulnerabilities in a number of applications. To prevent the spreading of damage, JPCERT/CC made an announcement on May 15 calling attention to the risks involved in using old versions of Movable Type.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 194. This was an 8% decrease from 211 of the previous quarter.

The number of scans reported in this quarter was 1,611. This was a 6% decrease from 1,719 of the previous quarter. The ports that the scans targeted are listed in [Chart **2**]. Ports targeted frequently were smtp(25/tcp), http(80/tcp) and ssh(22/tcp).

[Chart 2 : Number of Scans by Port]

Port	Apr	May	Jun	Total
25/tcp	264	301	162	727
80/tcp	256	168	268	692
22/tcp	57	52	34	143
123/udp	0	10	27	37
53/udp	0	1	32	33
21/tcp	2	9	8	19
443/tcp	11	3	2	16
5000/tcp	15	0	0	15
3389/tcp	3	5	5	13
1433/tcp	0	9	3	12
5060/udp	2	3	5	10
23/tcp	3	4	1	8
5900/tcp	1	1	1	3
445/tcp	0	2	1	3
143/tcp	2	1	0	3
7778/tcp	1	0	1	2
3306/tcp	1	1	0	2
110/tcp	1	1	0	2
icmp	0	0	1	1
19/udp	0	1	0	1
137/udp	0	0	1	1
Other/tcp	3	5	1	9
Unknown	28	4	4	36
Monthly Total	650	581	557	1788

4. Incident Handling Case Examples

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

[Coordination for domestic hosts used as a springboard for CHARGEN-based DDoS attacks]
At the end of March 2014, an overseas organization reported to JPCERT/CC that a number of hosts in Japan were being used as springboards for DDoS attacks using the CHARGEN protocol. CHARGEN is a protocol that generates characters in response to a connection to a port (normally 19/udp), and is used to confirm communication, among other purposes. Because UDP does not have an established communication session, it can be exploited to carry out replay attacks in which the IP address is spoofed to send packets to the target of attack.

JPCERT/CC contacted the telecommunications operator managing the IP addresses of the attack sources to request verification of relevant facts. It transpired that the terminals serving as attack sources used Windows XP and had Simple TCP/IP Services installed, and that for this reason CHARGEN could have been enabled involuntarily. Accordingly, steps were taken to disable CHARGEN.

[Coordination involving a financial botnet node in Japan]
In early April 2014, JPCERT/CC received information from an overseas security group that a command-and-control (C&C) node of the GameOver Zeus financial malware botnet was spotted in Japan. Unlike a typical botnet comprised of a C&C server and bots, the GameOver Zeus botnet consists of multiple bots that mutually establish a peer-to-peer (P2P) connection. Some bots in this P2P network that are also called supernodes act as C&C servers and are controlled by a mechanism that makes it difficult to take them down.

JPCERT/CC contacted the telecommunications operator managing the IP address of the host that was acting as a node, and requested it to take necessary steps. JPCERT/CC later received notification from the security group that it confirmed the host in question was removed from the botnet.

[Coordination involving a site exploiting the vulnerability in Adobe Flash Player that was addressed at the end of April]
At the end of May 2014, JPCERT/CC received information regarding a website using a suspicious domain made to look like a specific domestic site. An analysis of the website confirmed that when the site was accessed from a computer with an old version of the Adobe Flash Player installed, an attack exploiting the vulnerability (APSB14-13) addressed at the end of April 2014 was executed, causing malware to be downloaded from an external site.

JPCERT/CC requested the network management organizations responsible for the site exploiting the vulnerability and the site distributing the malware to take necessary actions, and later confirmed that these sites had been suspended.

JPCERT/CC®

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".