JPCERT-IR-2015-03
Issued: 2015-07-14

JPCERT/CC Incident Handling Report
[April 1, 2015 – June 30, 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 April 1, 2015 through June 30, 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 the 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]

	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports [*2]	2098	1609	1480	5187	6869
Number of Incident [*3]	1621	1320	1247	4188	5485
Cases Coordinated [*4]	1069	813	711	2593	3088

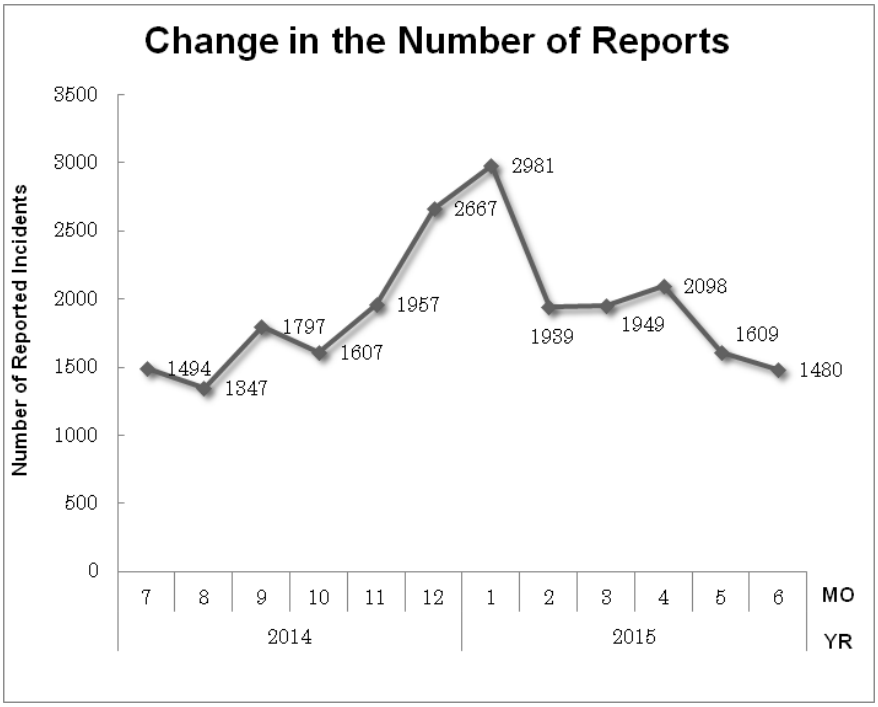
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

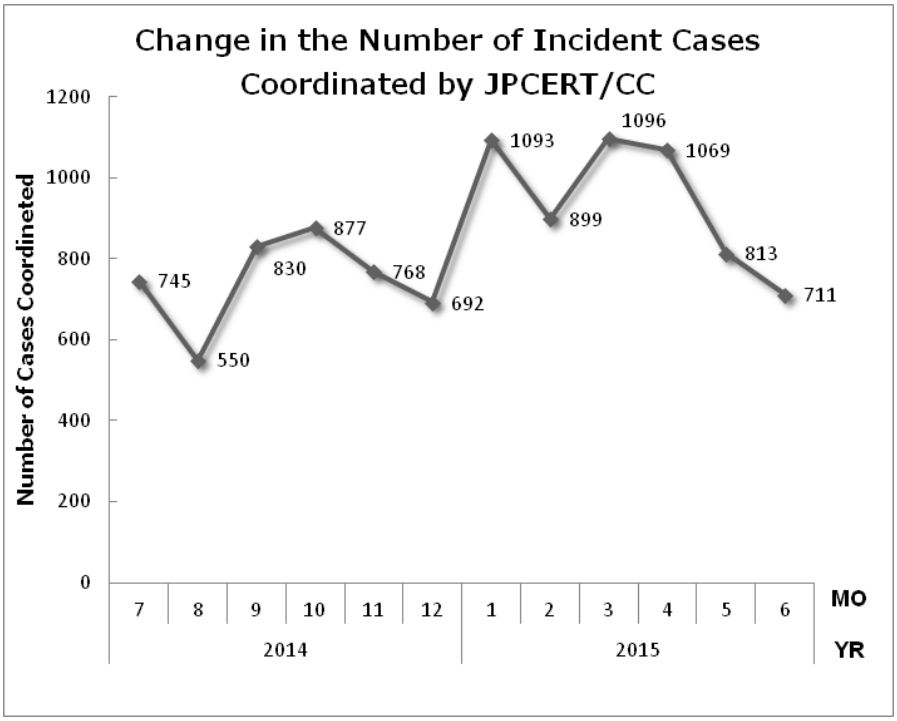
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 5,187. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,593. When compared with the previous quarter, the total number of reports decreased 24%, and the number of cases coordinated decreased 16%. Year on year, the total number of reports increased 15%, and the number of cases coordinated increased 22%.

[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]

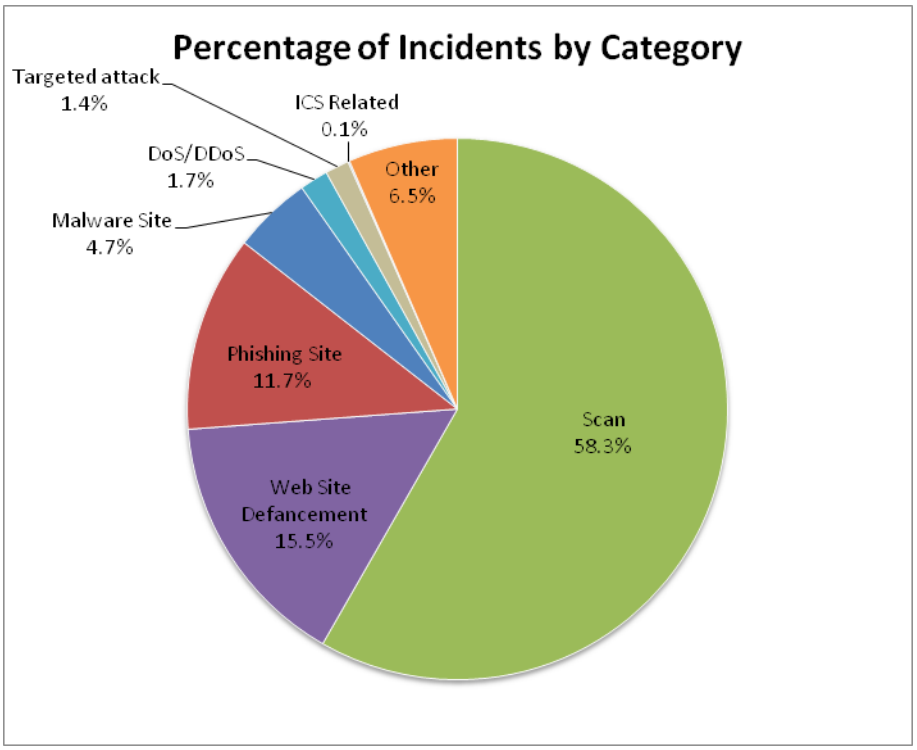
At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on each incident category, please see "Appendix 1 - Incident Categories". [Chart 2] shows the number of incidents received per category in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

[Chart 2: Number of incidents by category]

Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	191	144	156	491	466
Website Defacement	209	175	265	649	792
Malware Site	56	59	82	197	260
Scan	976	823	643	2442	2980
DoS/DDoS	61	3	7	71	32
ICS Related	0	4	0	4	5
Targeted attack	12	21	27	60	-
Other	116	91	67	274	950

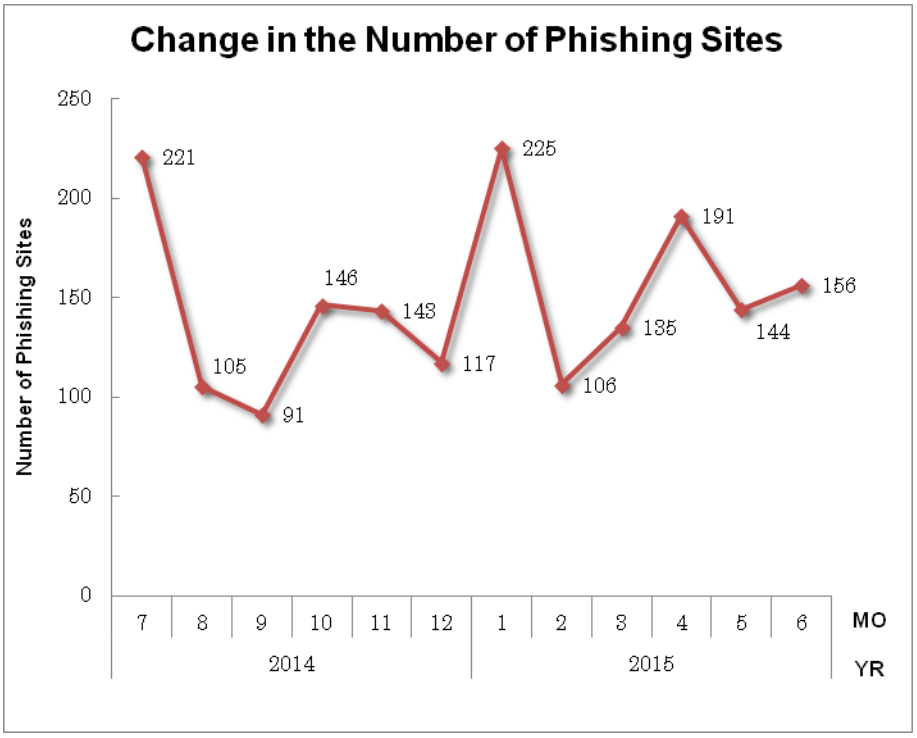
The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 58.3%, and incidents categorized as website defacement made up 15.5%. Also, incidents categorized as phishing sites represented 11.7% of the total.

JPCERT/CC has added "targeted attacks" as a new incident category from this quarter.

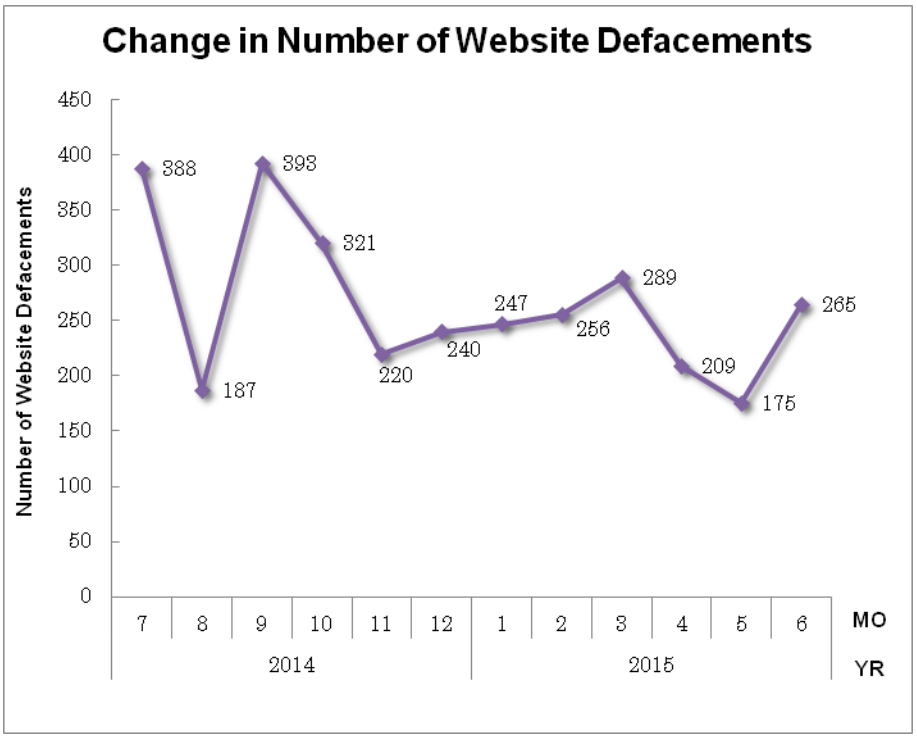


[Figure 3: Percentage of incidents by category]

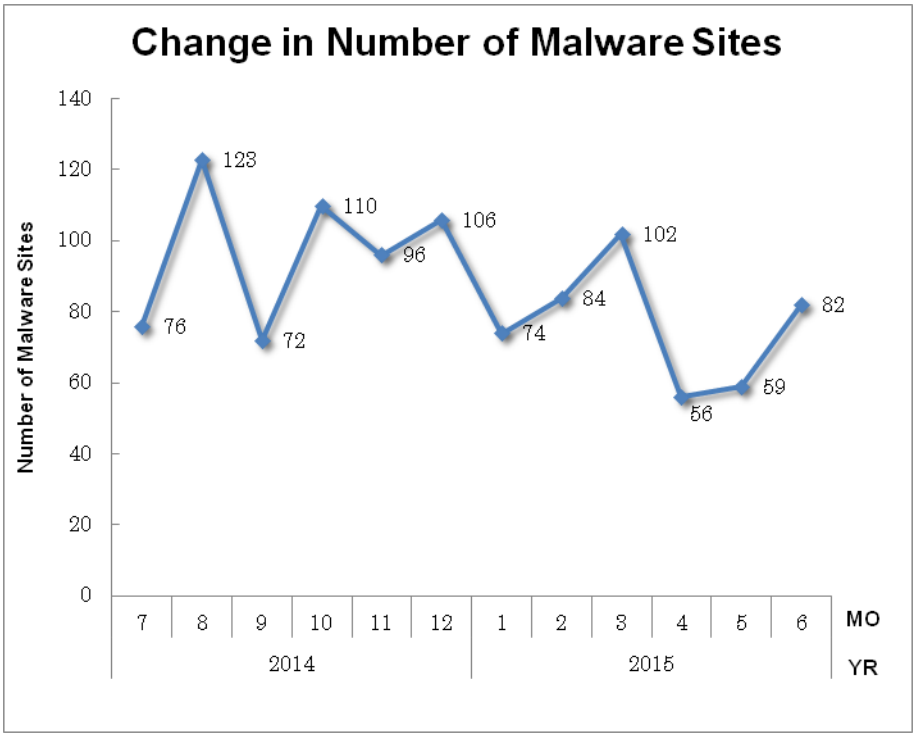
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



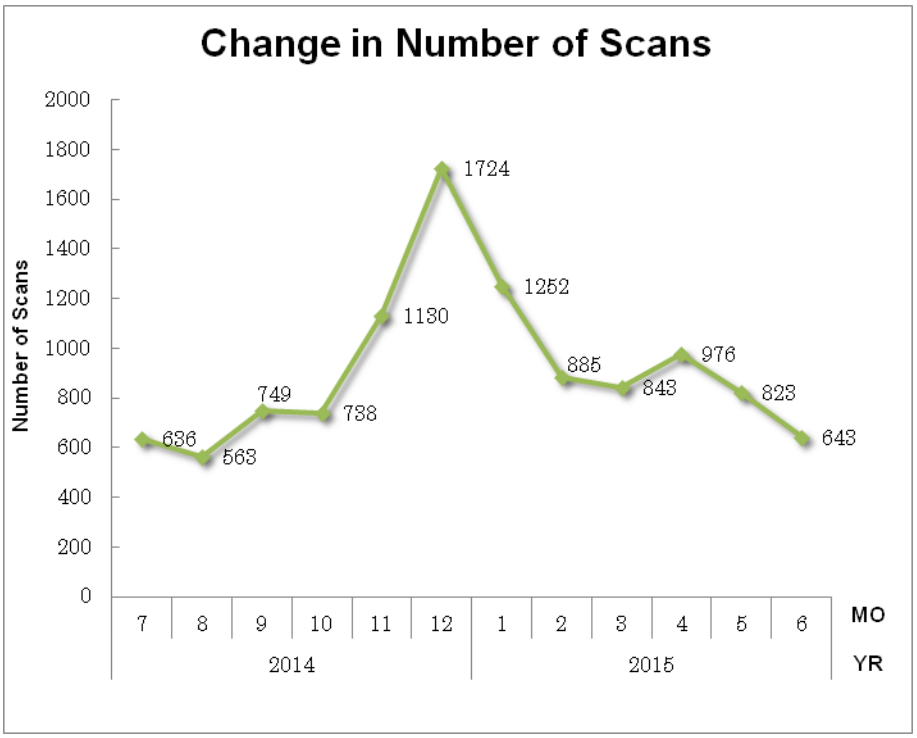
[Figure 4: Change in the number of phishing sites]



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

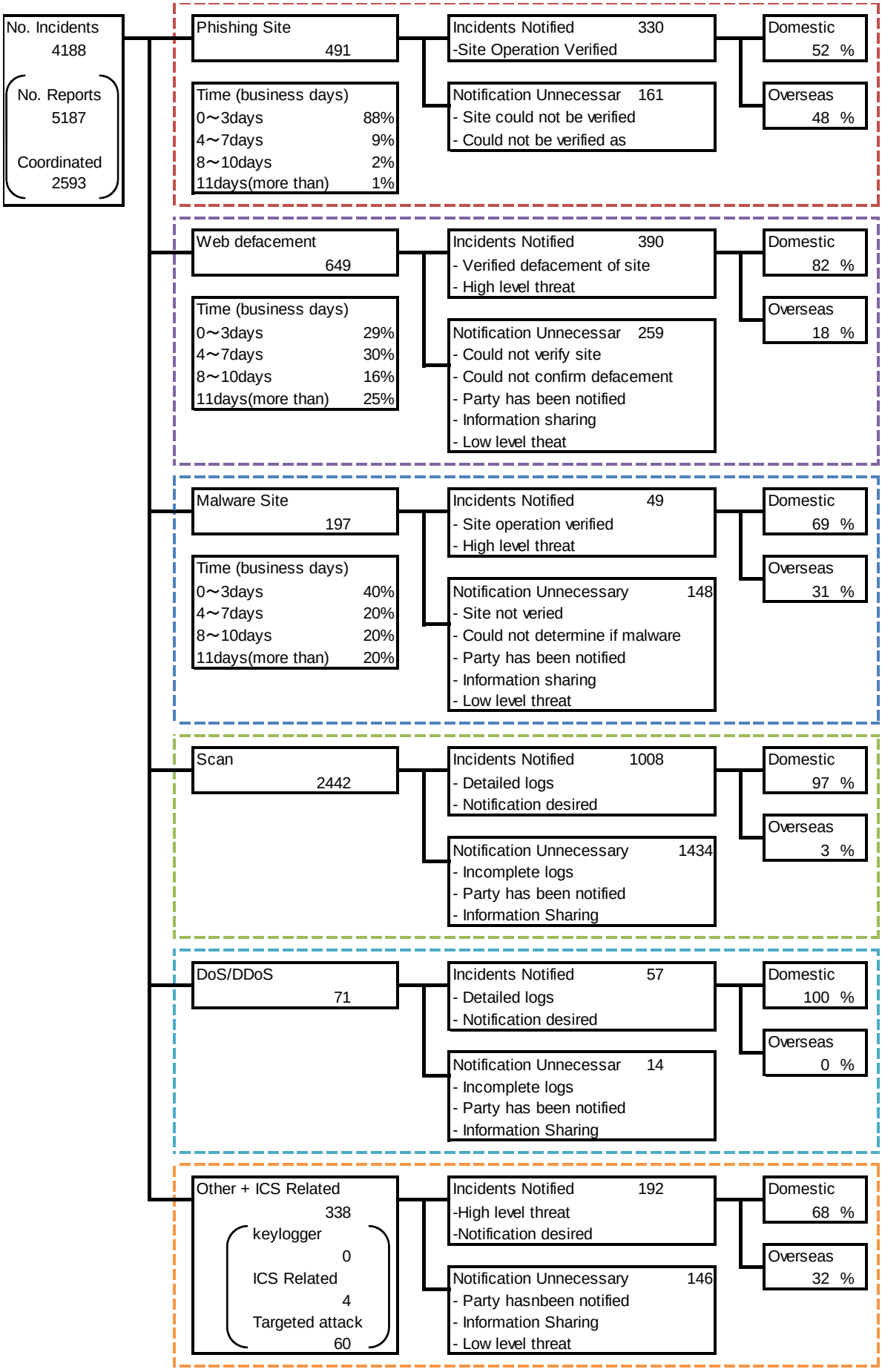


[Figure 6: Change in the number of malware sites]



[Figure 7: Change in the number of scans]

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



[Figure 8: Breakdown of incidents coordinated / handled]

3. Incident Trends

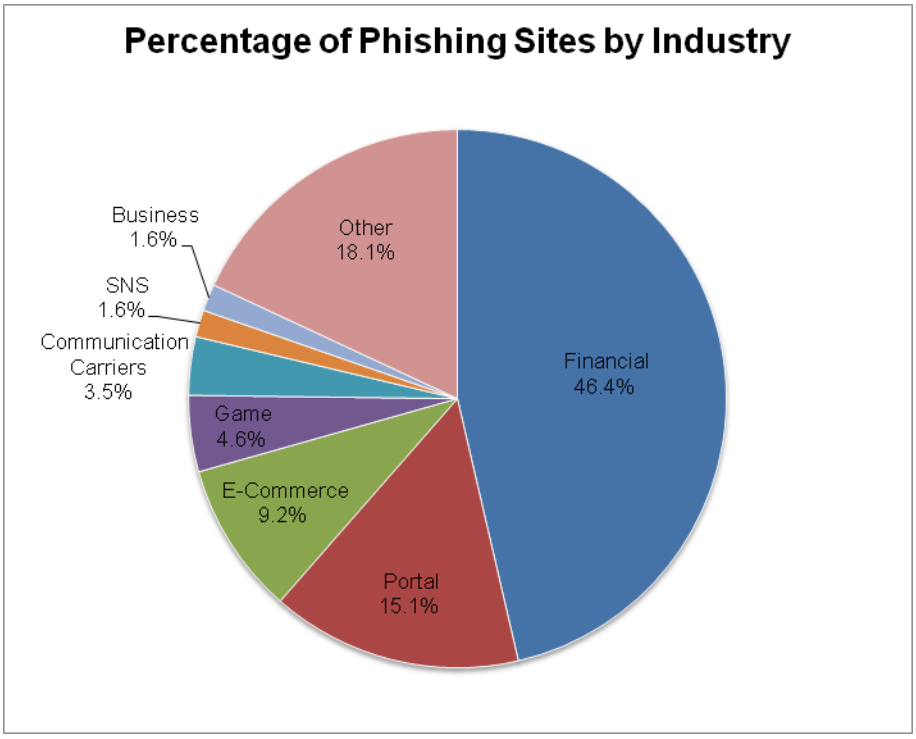
3.1. Phishing Site Trends

491 reports on phishing sites were received in this quarter, representing a 5% increase from 466 of the previous quarter. This marks a 4% decrease from the same quarter last year (509). 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 3: Number of phishing sites by domestic/overseas brand]

Phishing Site	Apr	May	Jun	Domestic/ Overseas Total (%)
Domestic Brand	53	35	44	132(27%)
Overseas Brand	92	74	73	239(49%)
Unknown Brand[*5]	46	35	39	120(24%)
Monthly Total	191	144	156	491(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 132 phishing sites that spoofed domestic brands, increasing 144% from 54 of the previous quarter. And there were 239 phishing sites that spoofed overseas brands, which was a 15% decrease from 281 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 46.4% spoofed websites of financial institutions, and 15.1% 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 financial institutions showed a marked increase from the previous quarter. Until late May, many of these phishing sites had a cn.com domain, but since then, ccTLDs such as .pw, .ml, .gq, and .ga were more often seen in such sites. Most phishing sites had an overseas IP address, and Japanese IP addresses were only seen in a handful of sites identified in mid-April.

While there used to be many cases in which a phishing site spoofing a domestic financial institution used a dynamic IP address allocated by a domestic ISP, similar cases are now continually observed with phishing sites that spoof South Korean government agencies.
The parties that JPCERT/CC contacted for coordination of phishing sites were 52% domestic and 48% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 73%, overseas: 27%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 649. This was an 18% decrease from 792 of the previous quarter.

During this quarter, JPCERT/CC received numerous reports of ransomware infection resulting from an access to compromised websites that guide site visitors to a fraudulent site. JPCERT/CC investigated the compromised websites and found that the malicious code that gets embedded contains a JavaScript code that sends a cookie and an iframe that guides site visitors to an attack site right after the body tag. These attack sites were using vulnerabilities in the Internet Explorer and Adobe Flash Player to infect the victims with malware.

It should be noted that websites with this type of defacement were all using WordPress. Websites using a CMS like WordPress may be susceptible to defacements if the CMS or a related plugin is not up-to-date. Website administrators must therefore keep the CMS updated at all times and take measures such as removing any unnecessary plugins.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 197. This was a 24% decrease from 260 of the previous quarter.

The number of scans reported in this quarter was 2,442. This was an 18% decrease from 2,980 of the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were DNS (53/UDP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 4: Number of scans by port]

Port	Apr	May	Jun	Total
53/udp	354	261	159	774
25/tcp	149	208	167	524
80/tcp	213	167	135	515
22/tcp	142	86	78	306
31385/udp	23	18	22	63
61222/udp	15	23	11	49
2632/udp	16	16	15	47
16358/udp	15	17	14	46
21/tcp	16	12	9	37
445/tcp	10	2	7	19
3389/tcp	4	2	13	19
8080/tcp	10	4	2	16
23/tcp	4	1	8	13
1433/tcp	2	1	7	10
3544/udp	4	1	1	6
143/tcp	1	3	2	6
110/tcp	0	1	4	5
Unknown	22	10	21	53
Monthly Total	1000	833	675	2508

For the sources of DNS communication, JPCERT/CC has identified a large number of domestic hosts that are open resolvers. As open resolvers can be used in DDoS attacks, JPCERT/CC has been contacting organizations and users administering the hosts to review the settings of servers, routers, and other related devices.

The number of incidents categorized as "Other" was 274. This was a 71% decrease from 950 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 advanced attacks targeting domestic organizations]
In the event of advanced attacks targeting domestic organizations, JPCERT/CC responds for example by investigating the malware and C&C servers used and cooperating with affected organizations in their investigations.

During this quarter, JPCERT/CC contacted 66 organizations regarding targeted attacks, 44 of which were contacted regarding remote control malware called Emdivi. Organizations infected with Emdivi have reported damages such as leakage of various confidential information and personally identifiable information, resulting from unauthorized access to internal Active Directories and file servers.

JPCERT/CC will continue to support the affected organizations in responding to the incident and conducting investigations, and also help prevent damages from spreading by contacting organizations that could have been affected and cooperating in their investigative efforts.

[Coordination involving domestic C&C servers of ransomware]
During this quarter, JPCERT/CC received numerous reports of ransomware infections, in which the attacker encrypts files stored on a computer and makes a demand for money, etc., to decrypt the encrypted files.

At the end of April, Canada's national CSIRT provided JPCERT/CC with the URL information of domestic websites that served as C&C servers of ransomware. Based on this information, JPCERT/CC discovered that a number of legitimate websites in Japan were installed with a php file for receiving POST requests from terminals infected with the malware. An analysis of related sample malware confirmed that communication was actually made with the URLs of the domestic websites. JPCERT/CC contacted the website administrators to confirm whether the URLs were intended, and received responses that appropriate actions were taken.

Since then, numerous reports started coming in from domestic sources concerning ransomware infections. JPCERT/CC responded by posting an alert to help prevent the spread of damages from ransomware infections.

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 lines of business are targeted for malware infection or unauthorized access to information.

JPCERT/CC categorizes the following as a targeted attack.

- Spoofed e-mail with malware attached sent to a specific organization
- Defacement of a website viewed only by limited organizations
- A website spoofing another website viewed only by limited organizations and attempting to infect site visitors with malware
- A server that malware targeting a specific organization 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".