JPCERT-IR-2016-02

Issued: 2016-07-14

JPCERT/CC Incident Handling Report
[April 1, 2016 - June 30, 2016]

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, 2016 through June 30, 2016.

[*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]

	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports *2	1891	1488	1307	4686	4587
Number of Incident *3	1497	1168	1126	3791	4143
Cases Coordinated *4	984	820	755	2559	2955

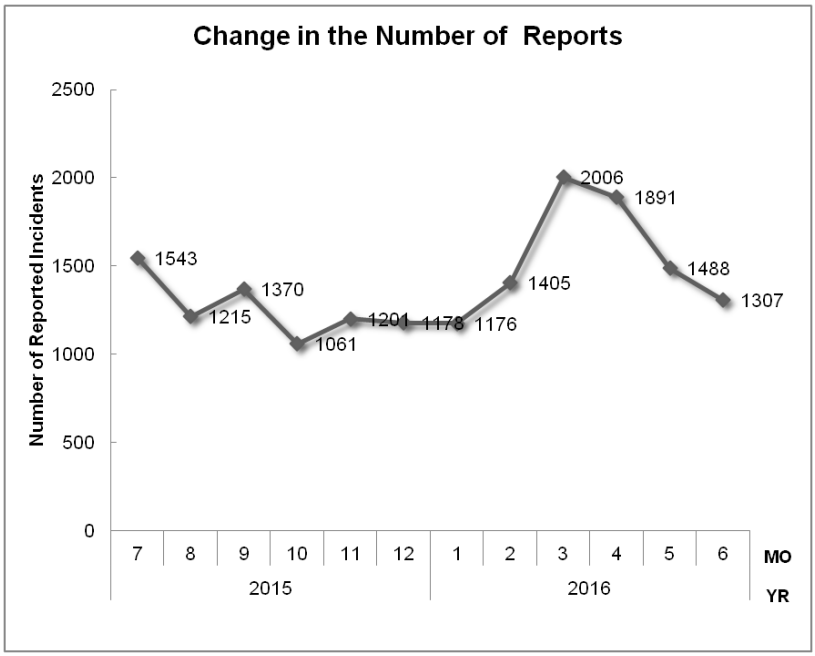
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

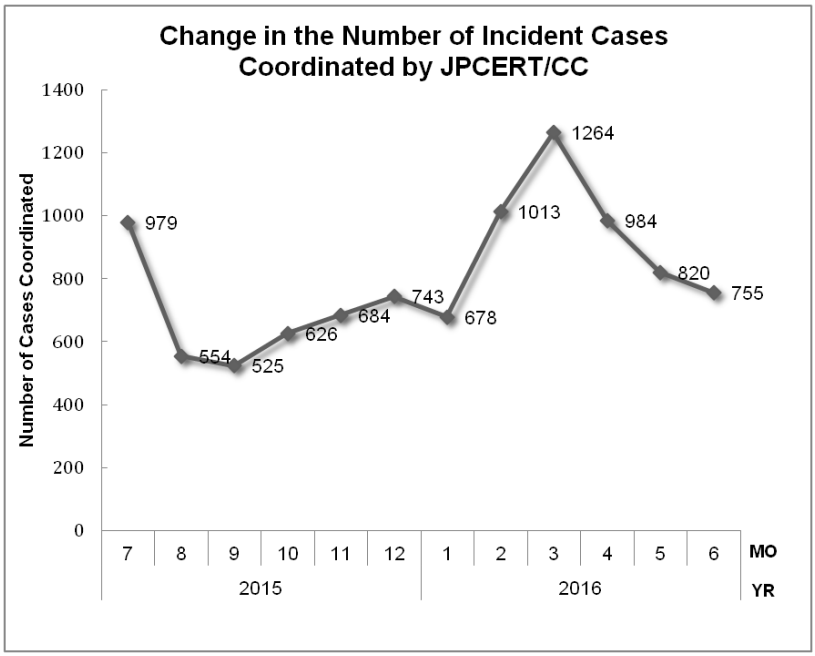
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,686. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,559. When compared with the previous quarter, the total number of reports increased by 2%, and the number of cases coordinated decreased by 13%. When compared with the same quarter of the previous year, the total number of reports decreased by 10%, and the number of cases coordinated decreased by 1%.

[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 incident reports]



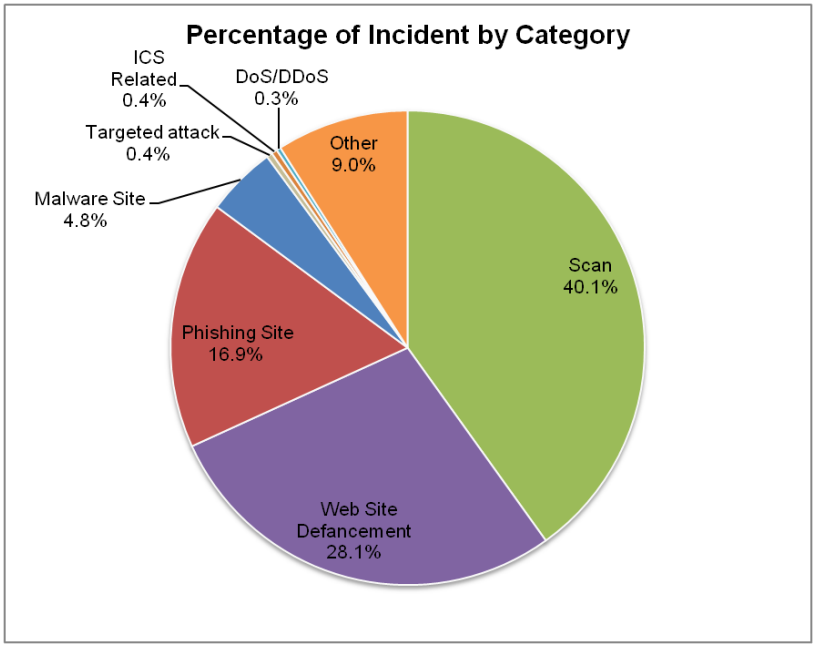
[Figure 2 :Change in the number of incident cases coordinated]

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]

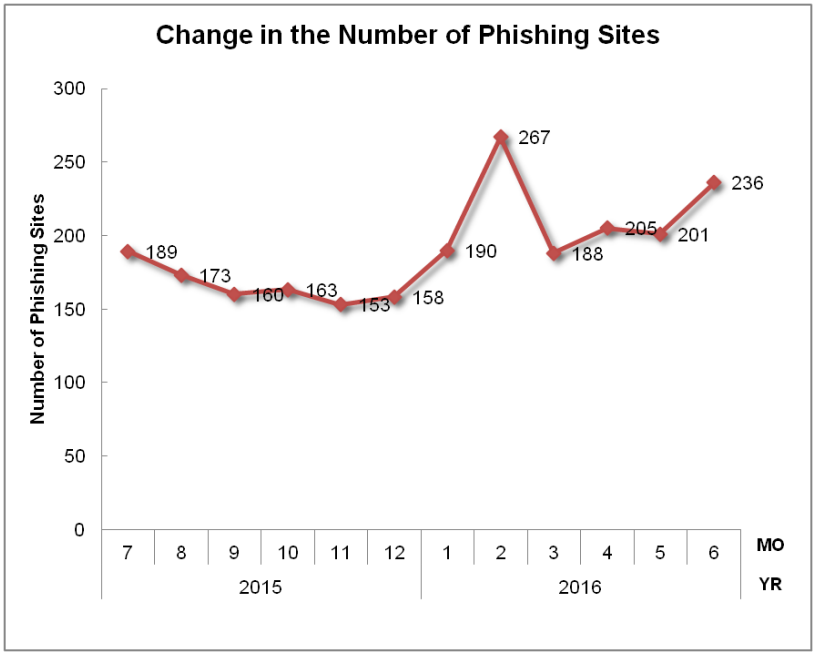
Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	205	201	236	642	645
Website Defacement	623	186	256	1065	1268
Malware Site	71	43	67	181	100
Scan	445	576	499	1520	1654
DoS/DDoS	5	1	5	11	86
ICS Related	6	9	0	15	11
Targeted attack	1	9	5	15	6
Other	141	143	58	342	373

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 40.1%, and incidents categorized as website defacement made up 28.1%. Also, incidents categorized as phishing sites represented 16.9% of the total.

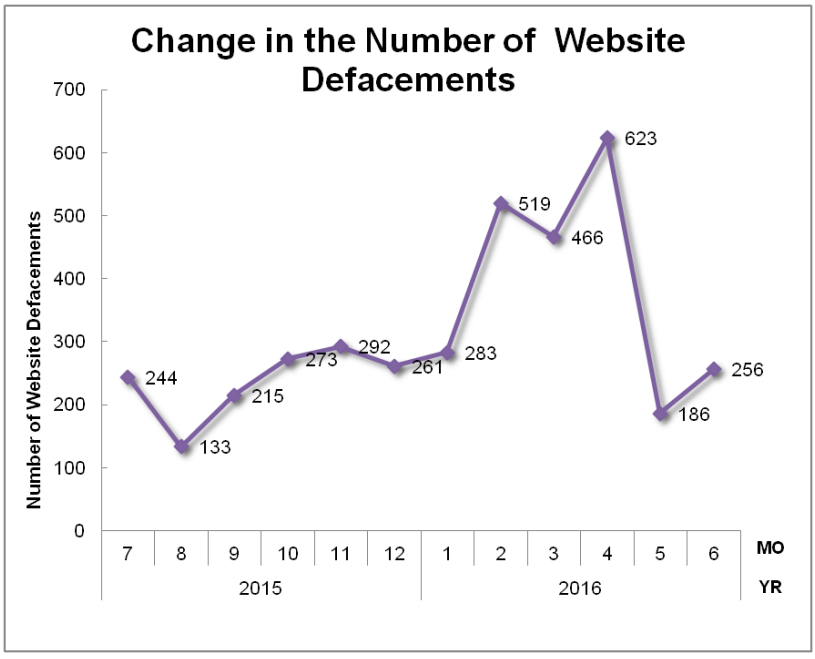


[Figure 3 :Percentage of incidents by category]

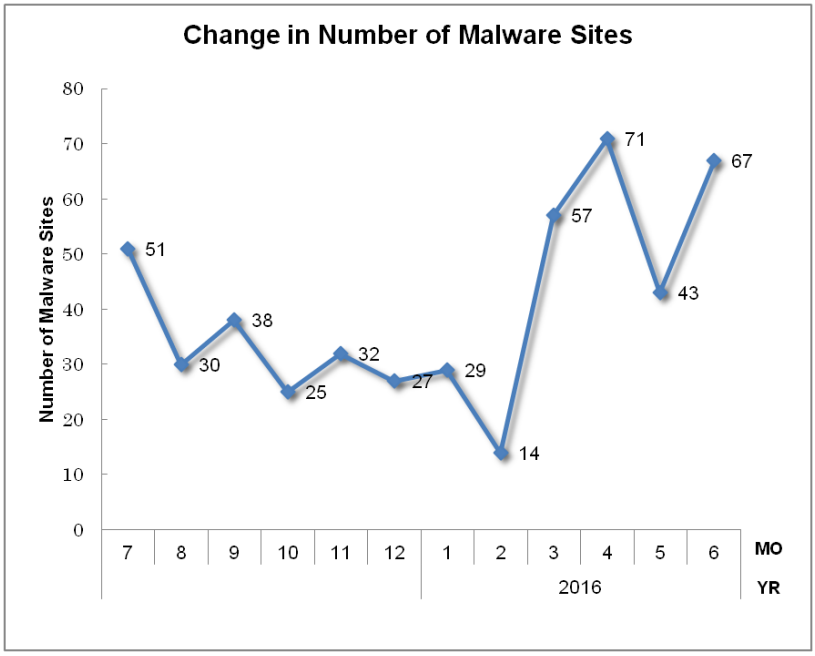
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



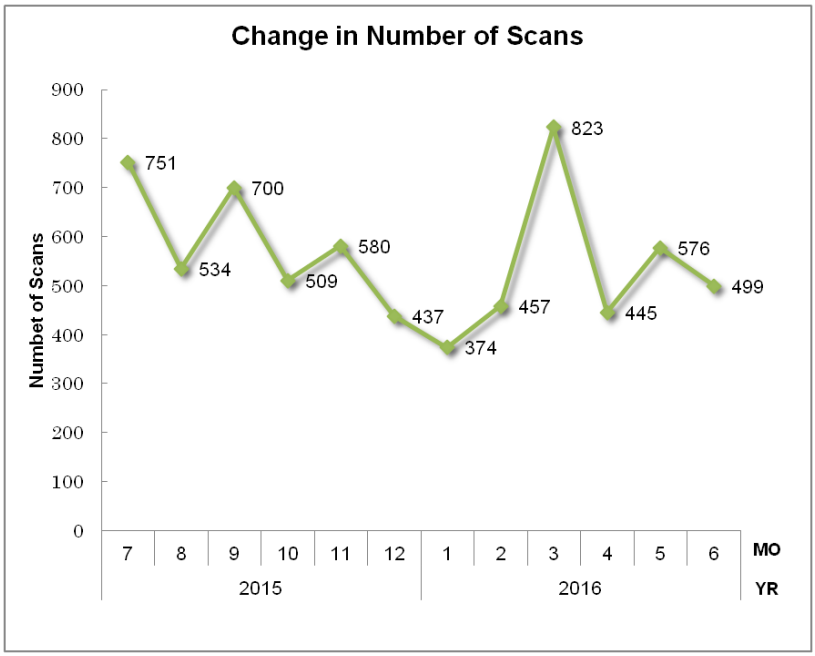
[Figure 4 :Change in the number of phishing sites]



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

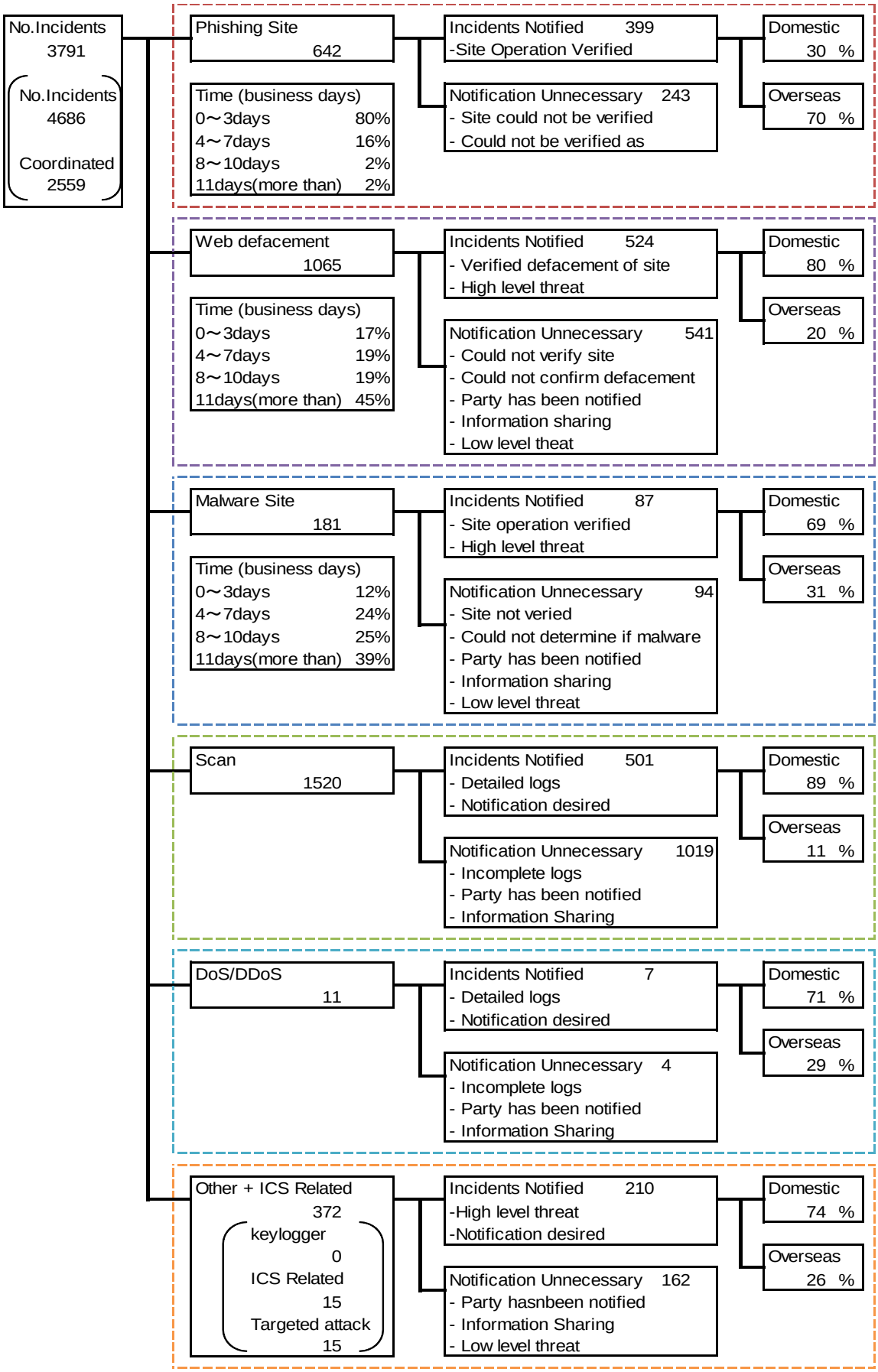


[Figure 6 :Change in the number of malware sites]



[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

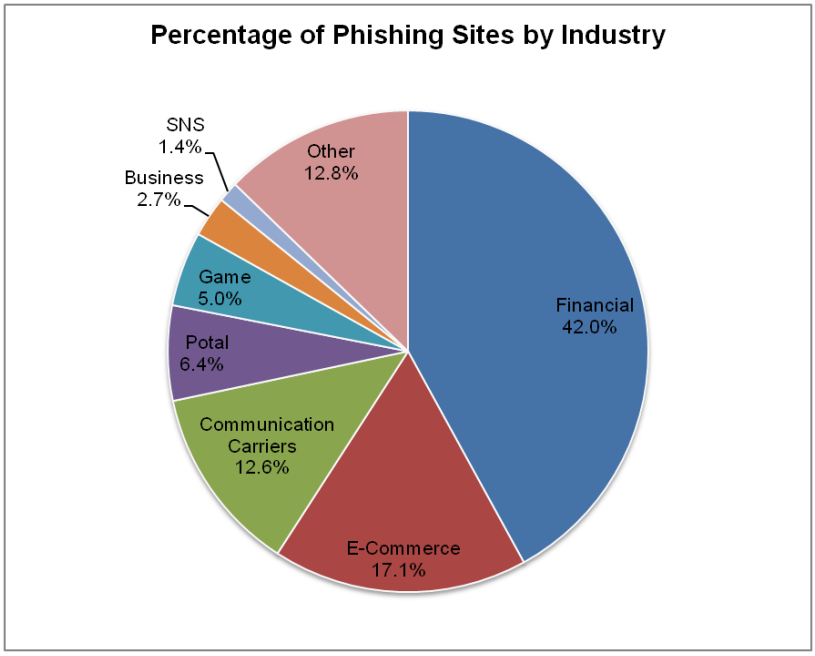
3.1. Phishing Site Trends

642 reports on phishing sites were received in this quarter, representing a 0.5% decrease from 645 of the previous quarter. This marks a 31% increase from the same quarter last year (491). 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].

[Chart3 :Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Apr	May	Jun	Domestic/ Overseas Total (%)
Domestic Brand	44	38	44	126(20%)
Overseas Brand	115	108	89	312(49%)
Unknown Brand [*5]	46	55	103	204(32%)
Monthly Total	205	201	236	642(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 reported phishing sites by industry]

During this quarter, there were 126 phishing sites that spoofed domestic brands, decreasing 33% from 189 of the previous quarter. And there were 312 phishing sites that spoofed overseas brands, increasing 16% from 270 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 42.0% spoofed websites of financial institutions, and 17.1% spoofed e-commerce websites. In Japan, telecommunications carriers accounted for most of the spoofed brands, whereas overseas, most of the spoofed brands were found among financial institutions.

During this quarter, there were many reports regarding phishing sites spoofing web-based e-mail services of domestic telecommunications carriers. Many of these phishing sites were set up on overseas websites that appear to have been breached. JPCERT/CC has confirmed phishing sites hosting multiple web pages spoofing different telecommunications carriers. This finding may be a sign that attacks aimed at stealing information of web-based e-mail accounts provided by domestic carriers are on the rise.

While phishing sites spoofing Japanese financial institutions were seen continually between April and late May, no phishing sites with a new IP address were found for about a month until late June, indicating that these attacks may be waning.

Between April and early June, phishing sites spoofing Japanese online gaming services were identified for only one brand. In mid-June, however, JPCERT/CC found phishing sites spoofing a number of different brands. All these phishing sites were using a free .cc domain that was found during the previous quarter as well.

The parties that JPCERT/CC contacted for coordination of phishing sites were 30% domestic and 70% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 35%, overseas: 65%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 1,065. This was a 16% decrease from 1,268 of the previous quarter.

Cases of website defacement in which malicious JavaScript is displayed only when the compromised websites are accessed with a specific browser were found in great numbers during the previous quarter. This trend was still observed during this quarter as well, and JPCERT/CC also found many website defacements in which JavaScript embedded at the end of a head tag redirects site visitors to a URL containing the string "jquery.min.php". Many of the compromised websites were using CMSs, indicating the possibility that they were infiltrated and compromised through an attack exploiting vulnerabilities in CMS themes and plugins, or a breach of authentication in an administration screen.

JPCERT/CC also confirmed many cases in which an online shopper searching for a product with a web search engine sees suspicious online shopping sites listed among the search results. These suspicious online shopping sites were created by defacing a legitimate third-party website. An investigation of this

legitimate site led to numerous sites spoofing an online shopping site that sells various products unrelated to the legitimate site. When the URL of the legitimate site was accessed directly, the correct pages were displayed with the relevant keywords embedded. However, when it was accessed by specifying the URL of a web search engine as the referer, an iframe tag loaded the pages of suspicious online shopping sites.

3.3. Targeted Attack Trends

There were 15 incidents categorized as a targeted attack. This was a 150% increase from 6 of the previous quarter. JPCERT/CC requested a total of 2 organizations to take action during this quarter.

In early May, JPCERT/CC identified communication from the IP address of a Japanese organization to a destination where an attack framework called Scanbox sends and collects information about the environment of PCs used to access a web page. An investigation conducted by JPCERT/CC revealed that, based on access referer information, the web user interface of a network device used internally by the organization may have been compromised and had a Scanbox code embedded.

In mid-May, an overseas security group provided JPCERT/CC with the IP address information of a domestic terminal communicating with an overseas C&C server where malware sends information collected from infected terminals.

Based on the obtained information, JPCERT/CC requested the relevant organizations to investigate whether such communication was not taking place.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 181. This was an 81% increase from 100 of the previous quarter.

The number of scans reported in this quarter was 1,520. This was an 8% decrease from 1,654 of the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SMTP (25/TCP), HTTP (80/TCP) and SSH (22/TCP).

[Chart 4 :Number of scans by port]

Port	Apr	May	Jun	Total
25/tcp	219	289	270	778
80/tcp	107	82	76	265
22/tcp	47	58	58	163
23/tcp	34	29	51	114
53/udp	16	76	0	92
21/tcp	11	11	13	35
123/tcp	0	0	20	20
445/tcp	7	4	6	17
53413/udp	2	2	7	11
8080/tcp	4	2	2	8
443/tcp	2	6	0	8
3389/tcp	1	4	2	7
143/tcp	6	1	0	7
1433/tcp	3	3	0	6
51331/udp	1	2	2	5
81/tcp	1	0	3	4
53/tcp	0	4	0	4
3306/tcp	3	0	1	4
82/tcp	0	2	1	3
50943/udp	0	2	1	3
5060/udp	1	2	0	3
5001/tcp	0	0	3	3
Unknown	18	139	144	301
Monthly Total	483	718	660	1861

There were 342 incidents categorized as other. This was an 8% decrease from 373 of the previous quarter.

4. Incident Handling Case Examples

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

[Anonymous FTP servers that appear to be network attached storages for personal use]
This quarter, JPCERT/CC received numerous reports concerning anonymous FTP servers operated on a Japanese ISP network. Normally, anonymous FTP servers are set up to be made publicly available, but judging from the characteristics of the reverse lookup name of the IP address and directory names, the reported FTP servers seemed to be network attached storages (NAS) that individuals or companies unintentionally made public. Further, many of these FTP servers had suspicious SCR files, HTML files, etc., with a specific file name, pointing to the possibility that they were being used as a storage location for malware.

JPCERT/CC requested a number of telecommunications carriers to contact relevant subscribers to confirm whether the state of their FTP servers was intended. As a result, a handful of the FTP servers became inaccessible or started requiring authentication to gain access, indicating that countermeasures were taken. However, no change in the state was seen with many of the servers.

[Credentials stolen by Pony information-stealing malware]
In late April, an overseas security group provided JPCERT/CC with the data of credentials that appear to have been stolen by Pony malware. Pony is a type of malware designed to steal credentials from many tools and browsers. It infects computers through an e-mail attachment containing the malware or a drive-by download attack that redirects users from a compromised website to a website that attacks vulnerabilities. The data JPCERT/CC received contained credentials of web-based services and mail servers that appeared to have been stolen from a user terminal infected with Pony.

JPCERT/CC extracted credentials that concern domestic web-based services and users from the received data, and contacted the companies operating each service to notify them of the possibility that service credentials may have been stolen from user terminals infected with the malware.

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 industries are targeted for malware infection or unauthorized access.

JPCERT/CC categorizes the following as a targeted attack.

- Spoofed e-mail with malware attached sent to a specific organization
- Defacement of a website affected to limited organizations
- A fake website accessible to limited organizations and attempting to infect site visitor's computer
- A command and control server that specially crafted malware 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 2016Fiscal Year".