JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IR-2017-03

Issued: 2017-07-13

JPCERT/CC Incident Handling Report
[April 1, 2017 – June 30, 2017]

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, 2017 through June 30, 2017.

[*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	1333	1380	2512	5225	4095
Number of Incident *3	1376	1388	2601	5365	4856
Cases Coordinated *4	883	823	847	2553	3077

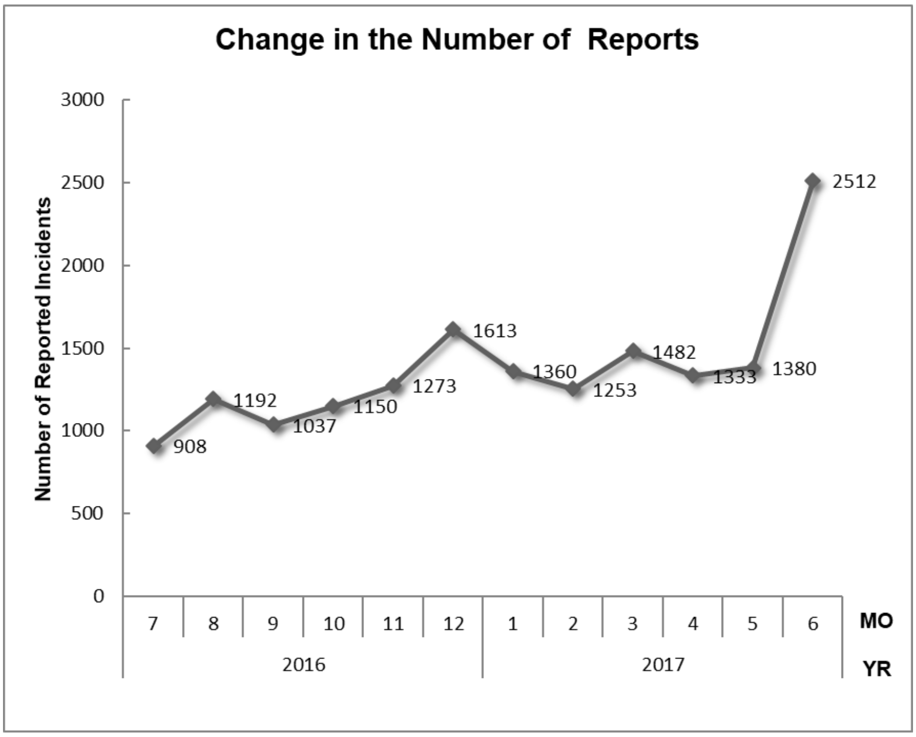
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

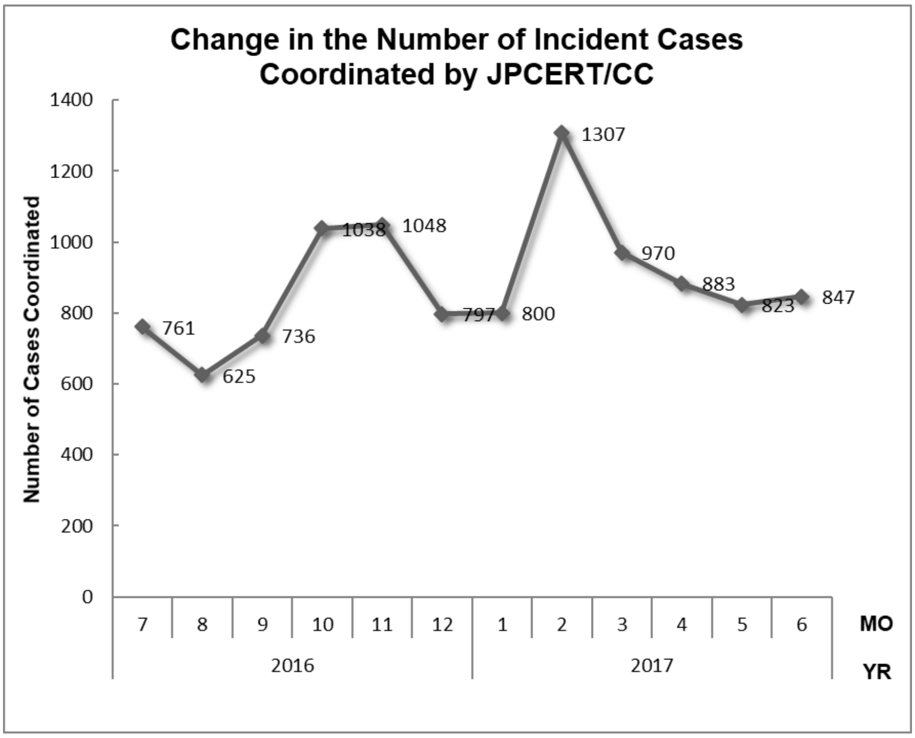
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 5,225. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,553. When compared with the previous quarter, the total number of reports increased by 28%, and the number of cases coordinated decreased by 17%. Year on year, the number of reports increased by 12%, and the number of cases coordinated decreased by 0.3%.

[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]



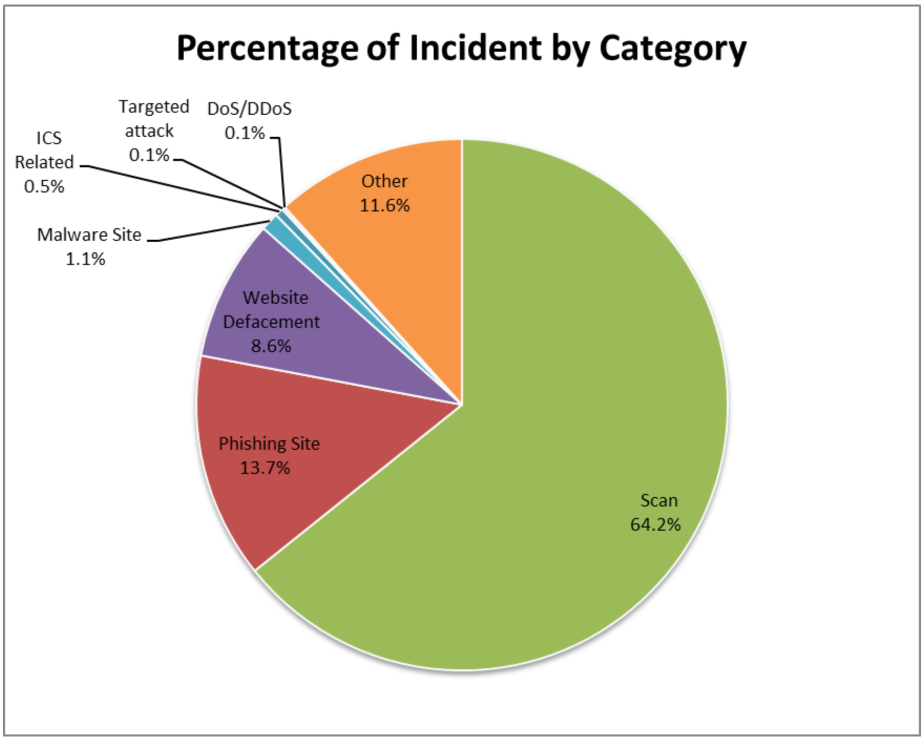
［Figure 2 Change in the number of incident cases coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of 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]

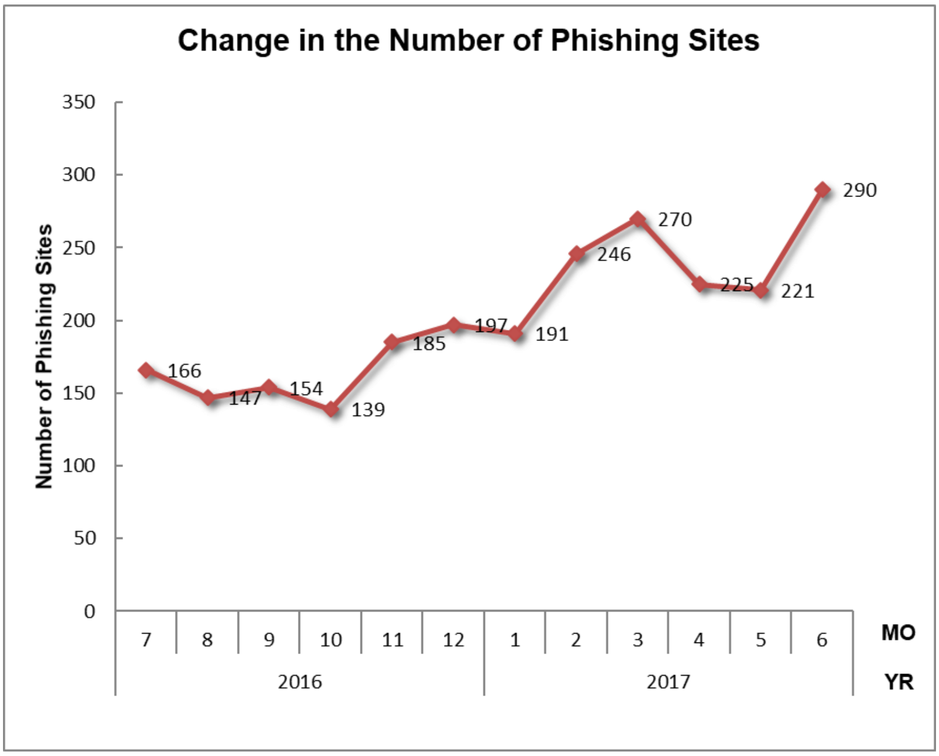
Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	225	221	290	736	707
Website Defacement	138	155	168	461	967
Malware Site	24	15	20	59	91
Scan	751	812	1884	3447	2391
DoS/DDoS	1	1	1	3	75
ICS Related	25	2	0	27	4
Targeted attack	6	1	2	9	11
Other	206	181	236	623	610

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 64.2%, and incidents categorized as phishing sites made up 13.7%.

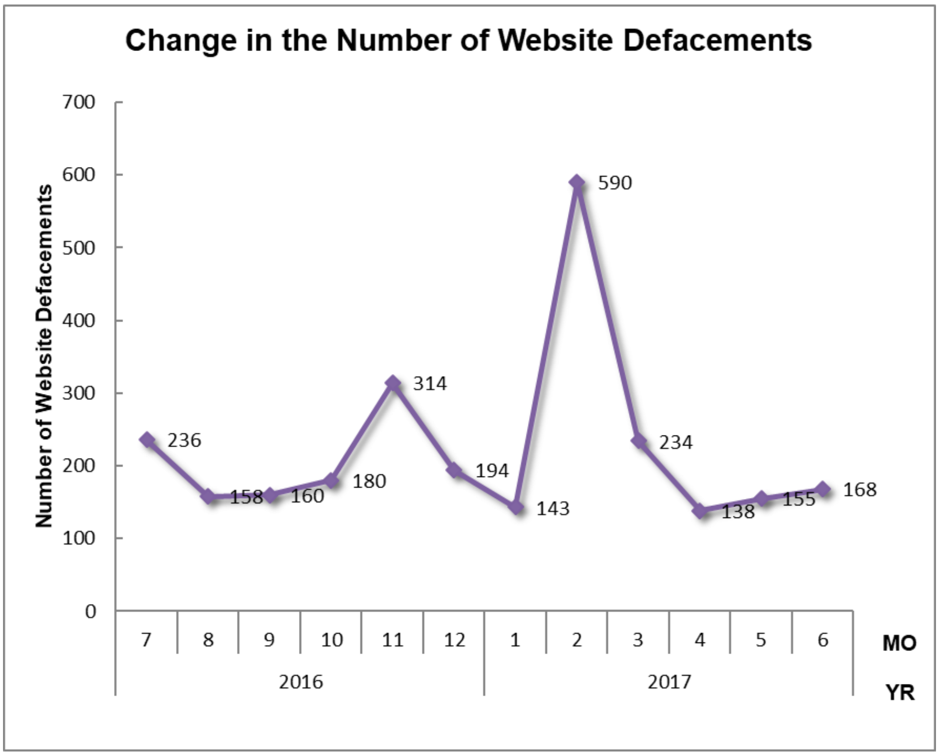


[Figure 3 Percentage of incidents by category]

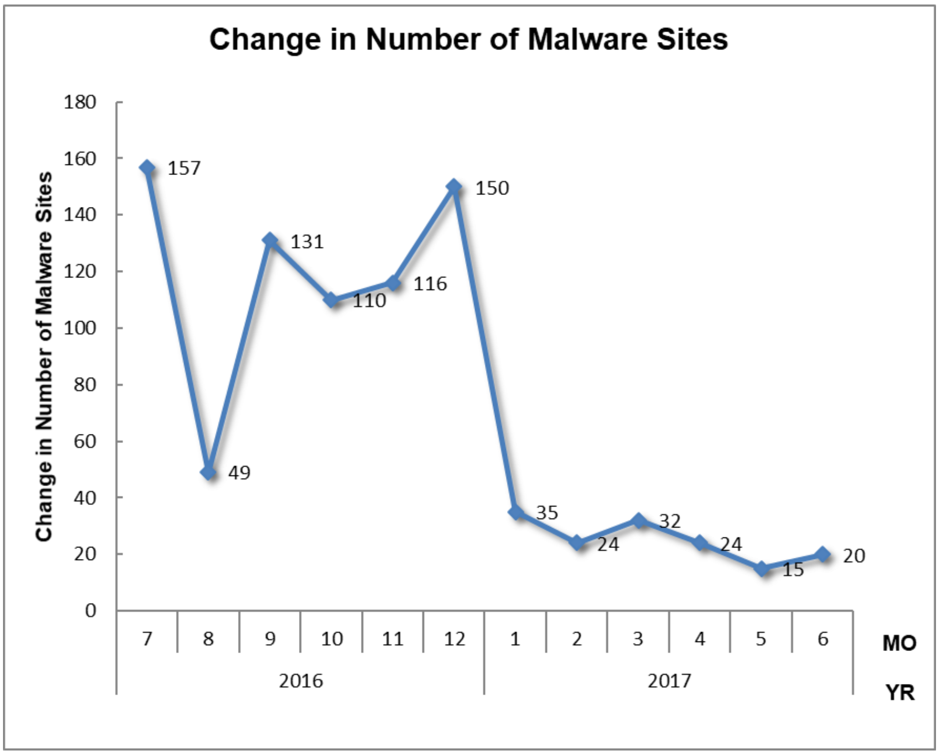
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



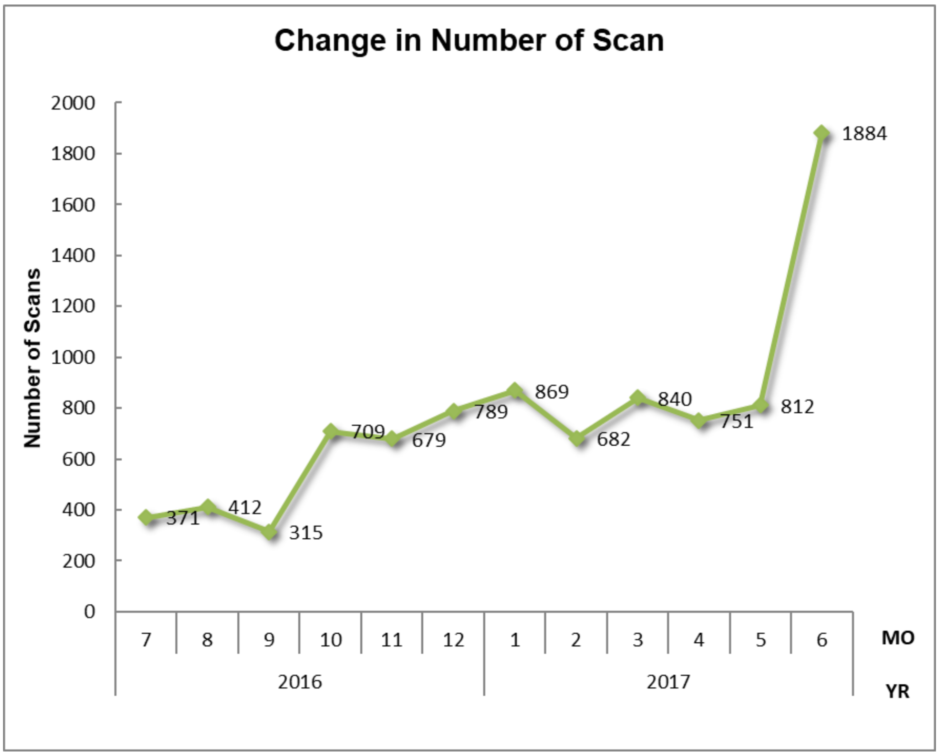
[Figure 4 Change in the number of phishing sites]



[Figure 5 Change in the number of website defacements]

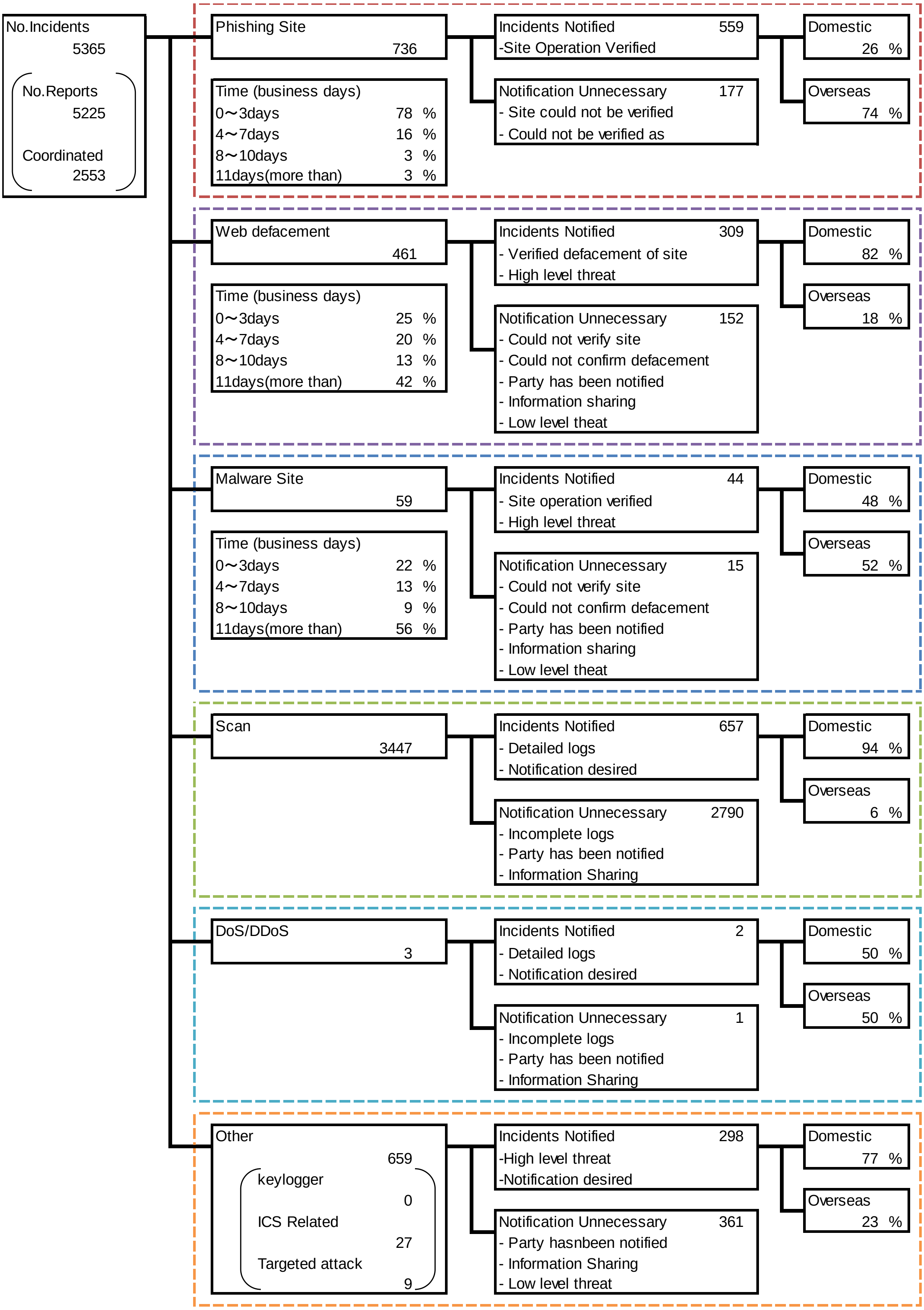


[Figure 6 Change in the number of malware sites]



[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.



No.Incidents 5365

No.Reports 5225

Coordinated 2553

Phishing Site 736

Time (business days)
0～3days 78 %
4～7days 16 %
8～10days 3 %
11days(more than) 3 %

Incidents Notified 559
-Site Operation Verified

Notification Unnecessary 177
- Site could not be verified
- Could not be verified as

Domestic 26 %

Overseas 74 %

Web defacement 461

Time (business days)
0～3days 25 %
4～7days 20 %
8～10days 13 %
11days(more than) 42 %

Incidents Notified 309
- Verified defacement of site
- High level threat

Notification Unnecessary 152
- Could not verify site
- Could not confirm defacement
- Party has been notified
- Information sharing
- Low level theat

Domestic 82 %

Overseas 18 %

Malware Site 59

Time (business days)
0～3days 22 %
4～7days 13 %
8～10days 9 %
11days(more than) 56 %

Incidents Notified 44
- Site operation verified
- High level threat

Notification Unnecessary 15
- Could not verify site
- Could not confirm defacement
- Party has been notified
- Information sharing
- Low level theat

Domestic 48 %

Overseas 52 %

Scan 3447

Incidents Notified 657
- Detailed logs
- Notification desired

Notification Unnecessary 2790
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 94 %

Overseas 6 %

DoS/DDoS 3

Incidents Notified 2
- Detailed logs
- Notification desired

Notification Unnecessary 1
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 50 %

Overseas 50 %

Other 659

keylogger 0

ICS Related 27

Targeted attack 9

Incidents Notified 298
-High level threat
-Notification desired

Notification Unnecessary 361
- Party hasnbeen notified
- Information Sharing
- Low level theat

Domestic 77 %

Overseas 23 %

[Figure 8 Breakdown of incidents coordinated/handled]

3. Incident Trends

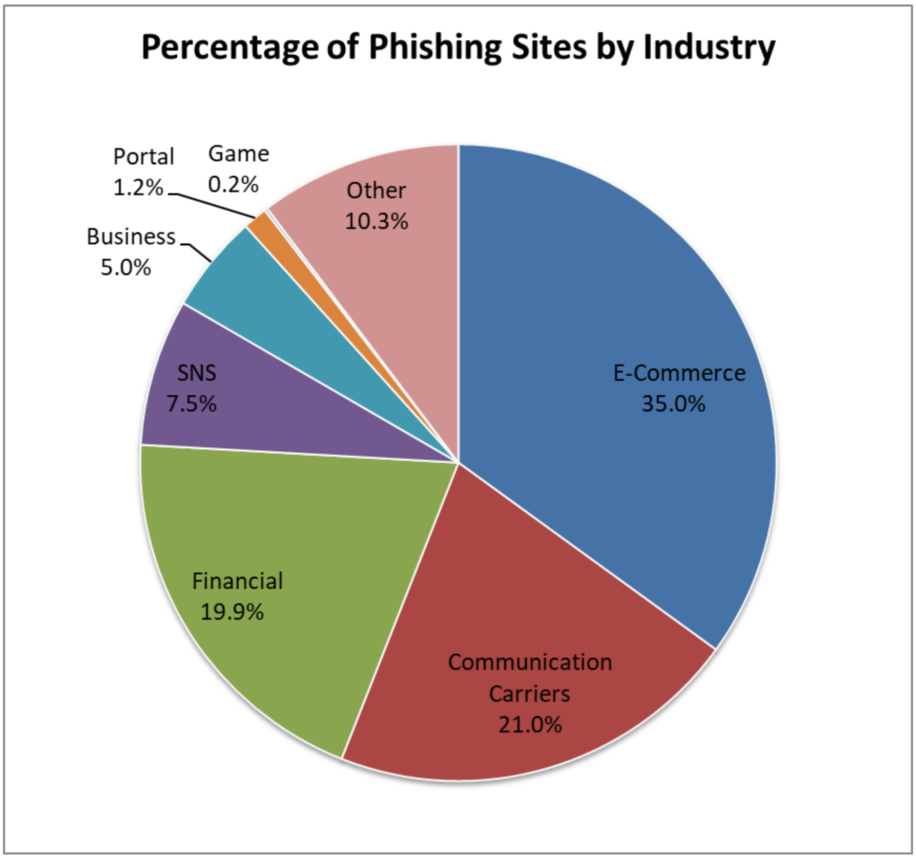
3.1. Phishing Site Trends

736 reports on phishing sites were received in this quarter, representing a 4% increase from 707 in the previous quarter. This marks a 15% increase from the same quarter last year (642). 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 reported phishing sites by domestic/overseas brand]

Phishing Site	Apr	May	Jun	Domestic/ Overseas Total (%)
Domestic Brand	52	69	88	209(28%)
Overseas Brand	143	115	176	434(59%)
Unknown Brand [*5]	30	37	26	93(13%)
Monthly Total	225	221	290	736(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 209 phishing sites that spoofed domestic brands, increasing 14% from 183 in the previous quarter. And there were 586 phishing sites that spoofed overseas brands, increasing 38% from 424 in the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 35.0% spoofed e-commerce websites, 21.0% websites of telecommunications carriers, and 19.9% websites of financial institutions.

More than 80% of the domestic brand phishing sites identified during this quarter consisted of those spoofing telecommunications carriers or SNS. As for phishing sites spoofing domestic financial institutions, only those spoofing credit card number ID registration sites were identified; other types, such as those spoofing Internet banking, were not found.

Many of the phishing sites spoofing the login screen of web-based e-mail services of domestic telecommunications carriers were set up on overseas websites that appear to have been breached. Phishing attacks spoofing specific brands commonly used the method of directing victims from a shortened URL to a phishing site set up using a legitimate service for creating web forms.

Most of the phishing sites spoofing SNS used a .cn domain. From April to early May, domain names consisting of five to six random alphabets were used, whereas since mid-May, domain names consisting of the targeted brand name appended with two to four alphabets have been used. Moreover, many of the phishing sites used an IP address in Hong Kong.

The parties that JPCERT/CC contacted for coordination of phishing sites were 26% domestic and 74% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 27%, overseas: 73%).

3.2.Website Defacement Trends

The number of website defacements reported in this quarter was 461. This was a 52% decrease from 967 in the previous quarter.

As in the previous quarter, website defacements were observed in which a malicious script gets embedded at the end of a page only when accessed for the first time. As for scripts that are embedded in defaced websites, JPCERT/CC has confirmed those that display a pop-up message prompting the visitor to update fonts, and those that redirect the visitor to a website where an attack using a vulnerability in Adobe Flash Player is performed. In both cases, ransomware is downloaded at the end.

Defacements in which a malicious script is embedded only when accessed for the first time are often found in websites using a CMS. Also, from around early June, many websites were identified in which image files appear to have been planted using a vulnerability in the WordPress plugin WP Job Manager. Vulnerabilities in CMSs and their plugins could be exploited to perform defacements and other types of attack, so it is important to always use the latest versions and to remove these programs if they are not needed.

3.3.Targeted Attack Trends

There were nine incidents categorized as a targeted attack. This was an 18% decrease from 11 in the previous quarter. JPCERT/CC asked two organizations to take action this quarter.

During this quarter, JPCERT/CC received a number of reports concerning targeted attacks using an HTTP bot called Daserf, a downloader called wali and other malware. Reports of similar types of targeted attack have been coming in since August of last year.

One of the confirmed infection routes for malware used in attacks is a certain vulnerability in asset management software. There is a possibility that attackers have been exploiting this vulnerability to carry out attacks continually since around June of last year. When a version of the asset management software with the vulnerability receives attack packets on a computer that has a global IP address assigned, the computer becomes infected with a downloader which then downloads and executes an HTTP bot.

The HTTP bot receives commands from the attacker's C&C server and sends information collected from the infected computer. JPCERT/CC has confirmed many cases in which web servers in Japan have been hacked and used as a C&C server for HTTP bots to communicate with. HTTP bots encrypt data when they send information collected from an infected computer to a C&C server. However, since the data is embedded in an HTTP request parameter, the encrypted data can be taken out from the HTTP request and decrypted, which sometimes offers revealing information about operations performed on the computer by the attacker to collect information.

There were also a number of reports concerning e-mails with malware attached, which appear to be targeted attacks. A targeted attack e-mail reported in late April had an attachment file that carries out an attack exploiting a vulnerability in a Microsoft product (CVE-2017-0199), which was fixed in an update released in April 2017. JPCERT/CC has also confirmed an attack method in which a dummy document file is attached along with a shortcut file which runs malware with bot functions upon execution, causing a PowerShell script to download and execute another malware in the end. This method is similar to the method used in past targeted attack e-mails to infect the recipient's computer with HTTP bots such as Asruex and ChChes.

3.4.Other Incident Trends

The number of malware sites reported in this quarter was 59. This was a 35% decrease from 91 in the previous quarter.

The number of scans reported in this quarter was 3,447. This was a 44% increase from 2,391 in the previous quarter. The ports that the scans targeted are listed in [Chart 4].

[Chart 4: Number of scans by port]

Port	Apr	May	Jun	Total
22/tcp	340	288	1471	2099
25/tcp	198	302	232	732
53/udp	104	35	82	221
80/tcp	34	53	24	111
23/tcp	19	28	10	57
1433/tcp	4	25	3	32
445/tcp	3	23	5	31
21/tcp	5	11	14	30
143/tcp	2	25	0	27
81/tcp	18	3	1	22
110/tcp	4	8	3	15
2222/tcp	3	8	0	11
3389/tcp	2	4	4	10
2323/tcp	4	1	1	6
5060/udp	1	0	3	4
9000/tcp	0	0	3	3
51331/udp	0	1	2	3
4752/udp	2	0	1	3
33442/udp	2	0	1	3
Unknown	144	294	435	873
Monthly Total	889	1109	2295	4293

Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and DNS (53/UDP). From around mid-June, JPCERT/CC has been receiving an increasing number of reports concerning scans targeting SSH, with IP addresses in Japan as attack sources. Possible reasons for the increase in scans include a growing number of network devices infected with malware due to ongoing attacks exploiting vulnerabilities in the devices. JPCERT/CC is currently working to collect information on hosts that serve as attack sources.

There were 623 incidents categorized as other. This was a 2% increase from 610 in the previous quarter.

4. Incident Handling Case Examples

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

[Coordination involving domestic websites affected by a vulnerability in IIS 6.0 WebDAV service]
In early April, a foreign security researcher provided JPCERT/CC with a list of websites in Japan containing a vulnerability (CVE-2017-7269) in the WebDAV service in Microsoft IIS 6.0. CVE-2017-7269, announced on March 27, 2017, is a vulnerability in the WebDAV service in IIS 6.0 in Windows Server 2003 R2, which is no longer supported. A vulnerable server could have arbitrary code executed if it receives a modified request.

JPCERT/CC has contacted the administrators of the websites identified using the provided list and requested them to confirm whether the WebDAV service is running on the server. A number of them have responded that they disabled the server's WebDAV service or took other measures.

[Coordination involving Japanese e-mails designed to infect computers with financial malware]
During this quarter, JPCERT/CC identified many cases in which a Japanese e-mail is sent with a ZIP file attachment containing an execution file or a document file which appears to be designed to infect the recipient's computer with malware. In June, there were also cases in which an e-mail attachment contained a document file that carries out an attack exploiting a vulnerability (CVE-2017-0199) in a Microsoft product, which was fixed in April. When the attached file is opened, malware called Ursnif or DreamBot, which steals Internet banking information, is downloaded and executed in the end. The malware downloads a module for communicating using Tor, which enables anonymous communication, then communicates with a C&C server on a Tor network to configure settings and obtain commands.

A number of domestic websites with a Ursnif execution file planted have been identified. JPCERT/CC has requested the business operators that administer the infected servers to look into the possibility of the servers being abused. JPCERT/CC has also confirmed a number of cases in which IP addresses in Japan were used to send e-mails with the malware attached. JPCERT/CC has requested the telecommunications carriers that manage the source IP addresses.

Request from JPCERT/CC

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

Reporting an ICS Incident
https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

If you would like to encrypt your report, please use JPCERT/CC's PGP public key. The public key can be obtained at the following web page.

PGP Public Key
https://www.jpcert.or.jp/english/ir/pgp.html

JPCERT/CC provides a mailing list to ensure speedy delivery of the information it issues. If you wish to use the mailing list, please refer to the following information.

About the Mailing List
https://www.jpcert.or.jp/announce.html

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 2017 Fiscal Year".

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). For the latest information, please refer to JPCERT/CC's website.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/