JPCERT-IR-2016-03

Issued: 2016-10-12

JPCERT/CC Incident Handling Report
[July 1,2016 — September 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 July 1, 2016 through September 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]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports [*2]	908	1192	1037	3137	4686
Number of Incident [*3]	1012	873	916	2801	3791
Cases Coordinated [*4]	761	625	736	2122	2559

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

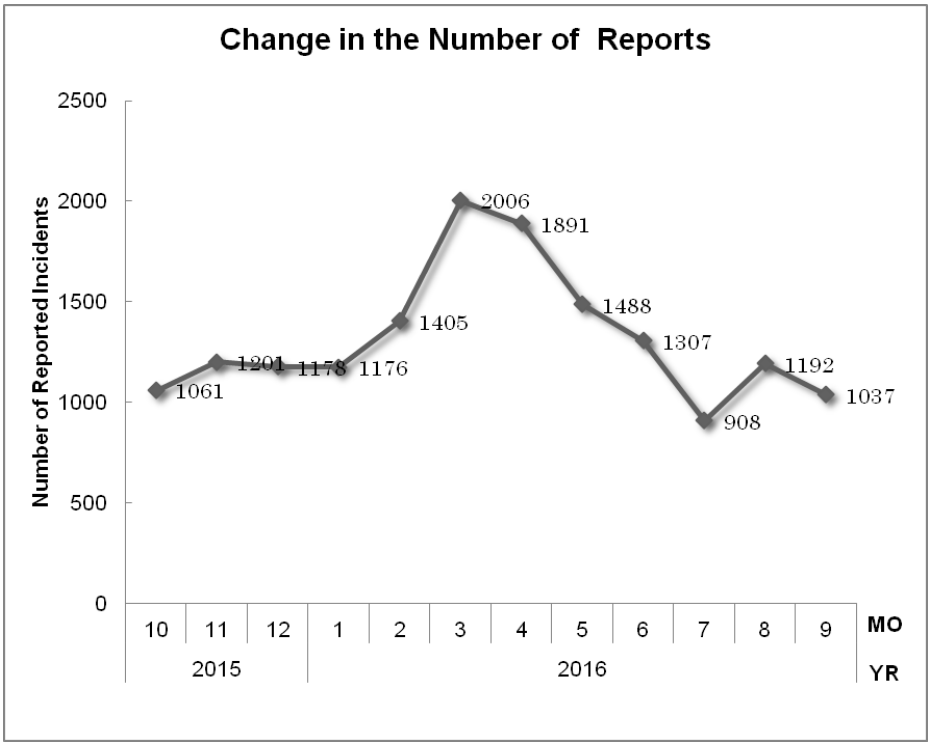
[*3] "Number of Incidents" refers to the number of incidents contained in each report.
Multiple reports on the same incident are counted as 1 incident.

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

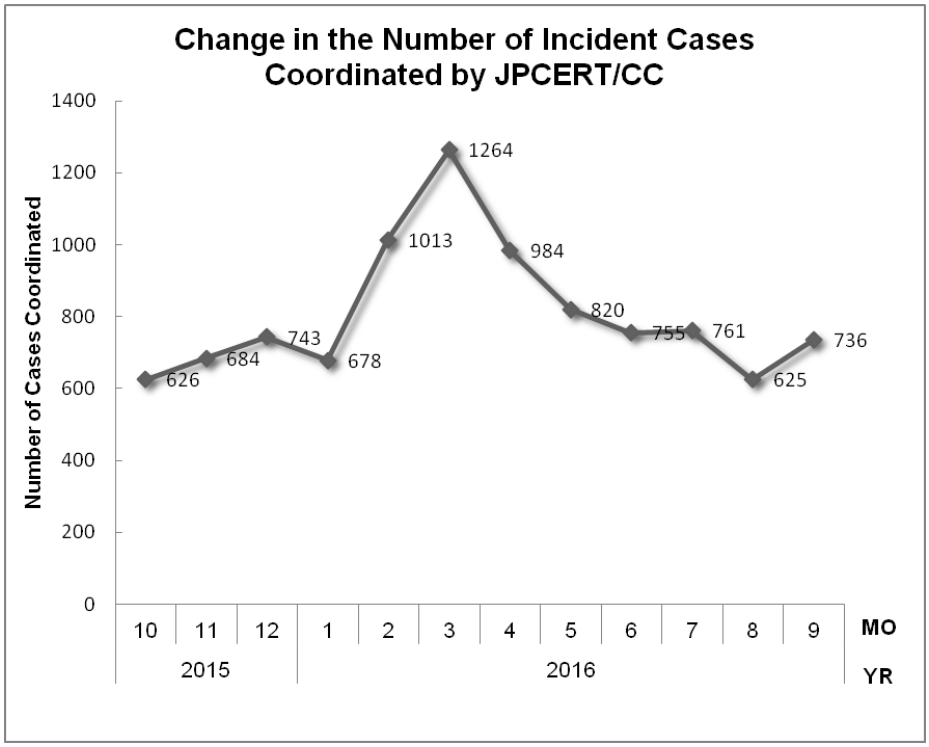
prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 3,137. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,122. When compared with the previous quarter, the total number of reports decreased by 33%, and the number of cases coordinated decreased by 17%. When compared with the same quarter of the previous year, the total number of reports decreased by 24%, and the number of cases coordinated increased by 3%.

[Figure 2] and [Figure 3] 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]



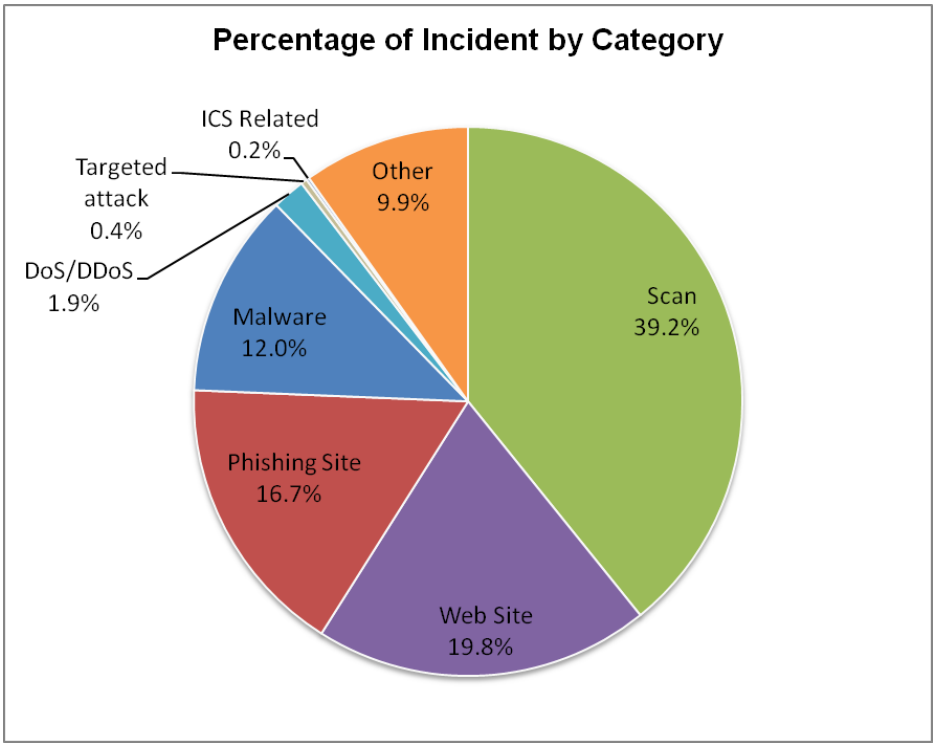
[Figure 2: Change in the Number of Incident Cases Coordinated]

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 per Category]

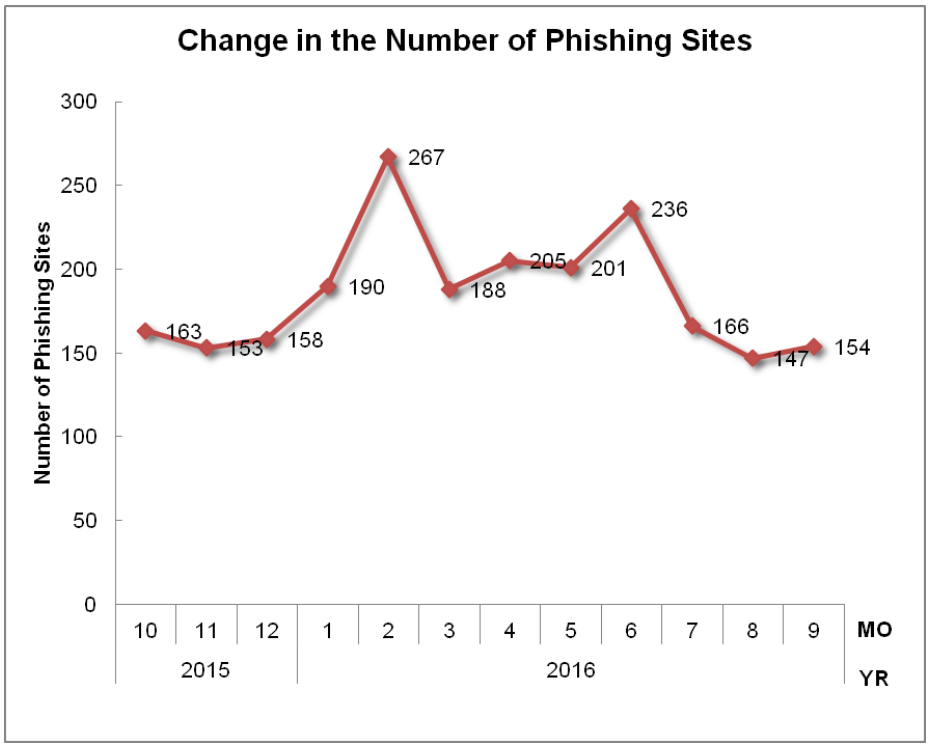
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	166	147	154	467	642
Website Defacement	236	158	160	554	1065
Malware Site	157	49	131	337	181
Scan	371	412	315	1098	1520
DoS/DDoS	5	9	40	54	11
ICS Related	2	2	1	5	15
Targeted attack	1	6	3	10	15
Other	74	90	112	276	342

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 39.2%, and incidents categorized as website defacement made up 19.8%. Also, incidents categorized as phishing sites represented 16.7% of the total.

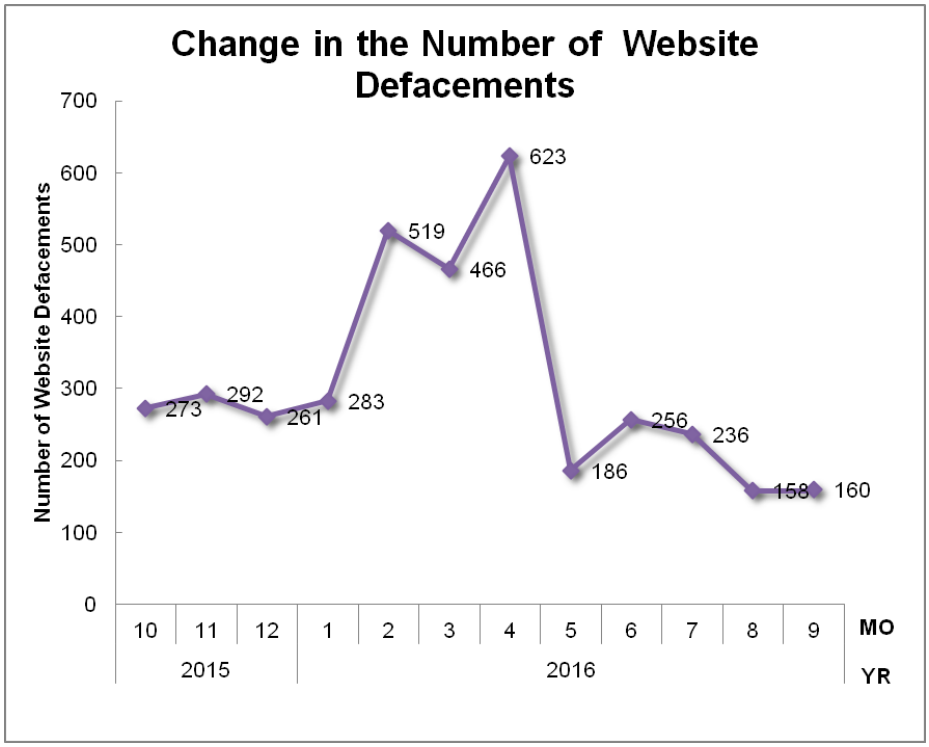


[Figure 3: Percentage of incidents by category]

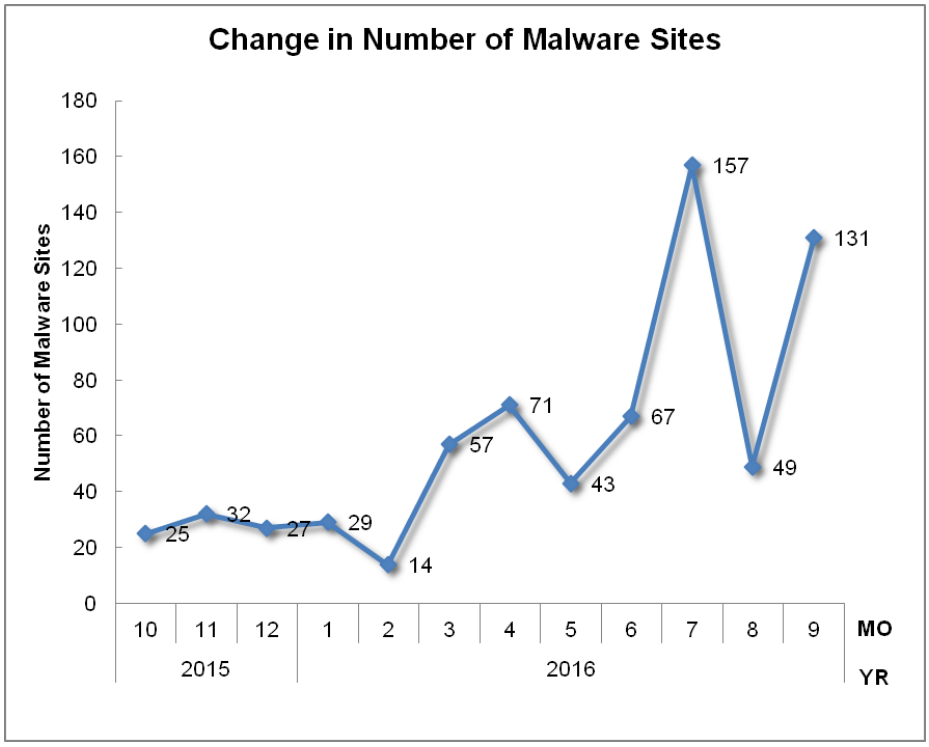
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



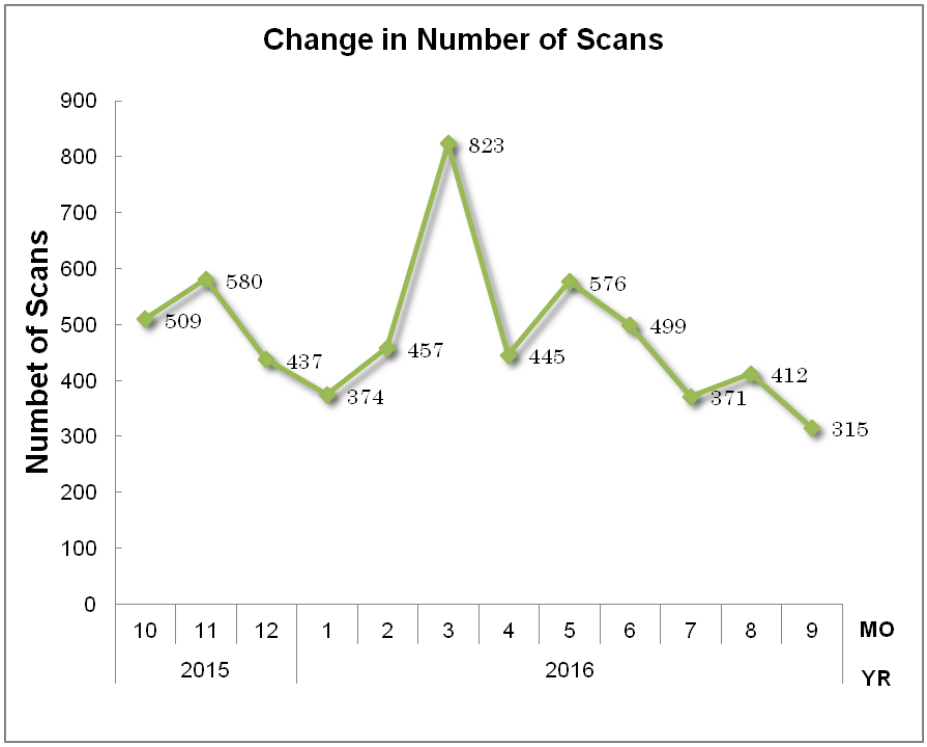
[Figure 4: Change in the number of phishing sites]



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

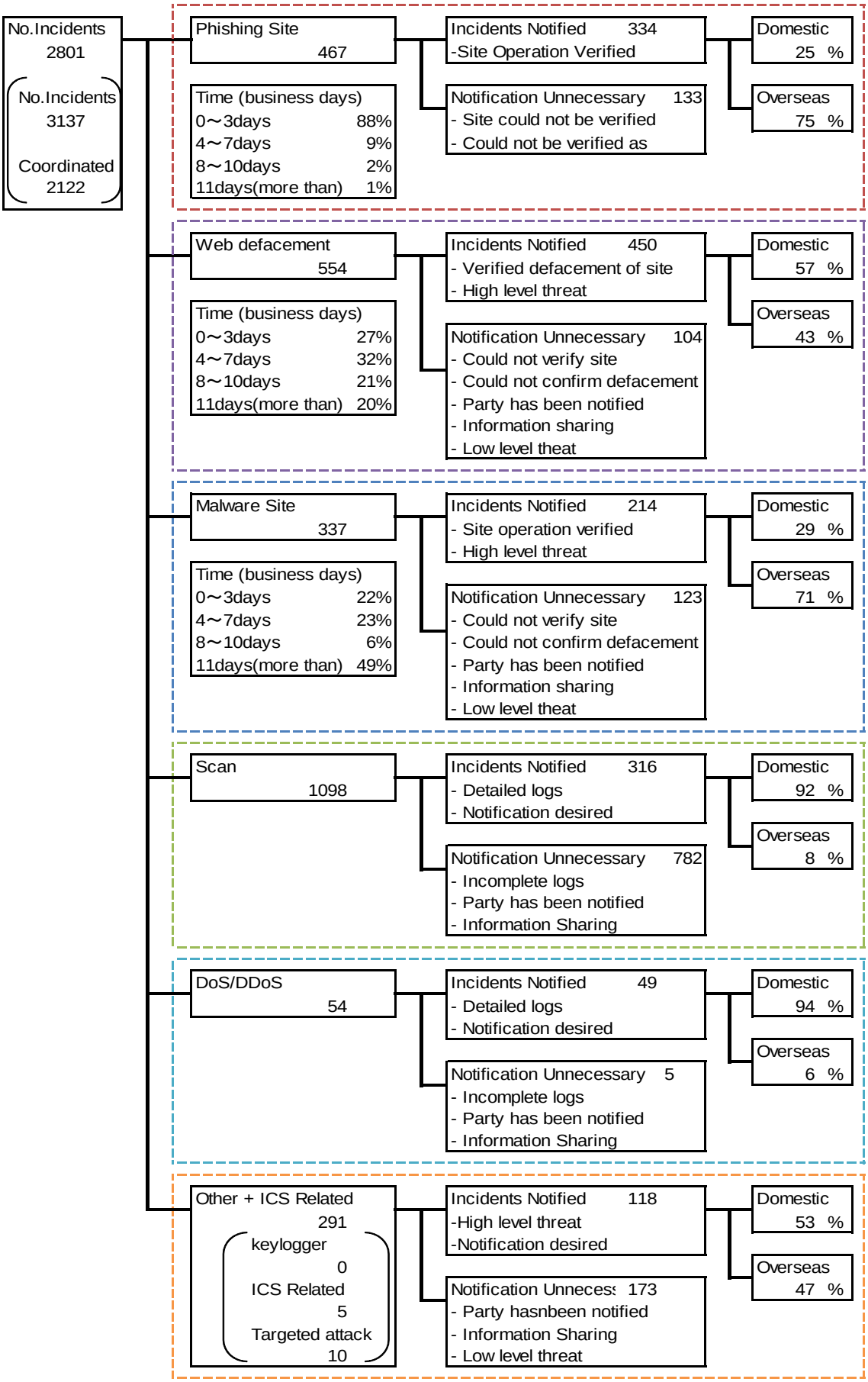


[Figure 6: Change in the number of malware sites]



[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

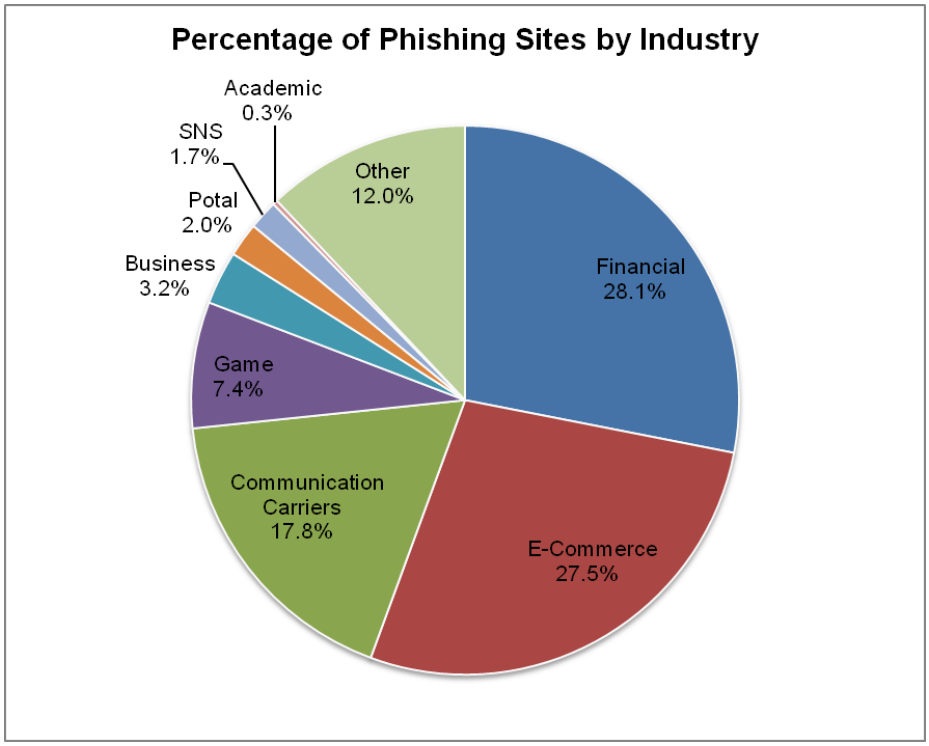
3.1 Phishing Site Trends

467 reports on phishing sites were received in this quarter, representing a 27% decrease from 642 of the previous quarter. This marks an 11% decrease from the same quarter last year (522). 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 [Chart 9].

[Chart 3: Number of phishing sites by domestic/overseas brand]

Phishing Site	Jul	Aug	Sep	Domestic/ Overseas Total (%)
Domestic Brand	30	43	33	106(23%)
Overseas Brand	94	73	76	243(52%)
Unknown Brand (*5)	42	31	45	118(25%)
Monthly Total	166	147	154	467(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 106 phishing sites that spoofed domestic brands, decreasing 16% from 126 of the previous quarter. There were 243 phishing sites that spoofed overseas brands, decreasing 22% from 312 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 28.1% spoofed websites of financial institutions, and 27.5% spoofed e-commerce websites.

Continuing the trend seen in the previous quarter, there were many reports regarding phishing sites spoofing web-based e-mails of domestic telecommunications carriers during this quarter. Some of these phishing sites were set up on compromised overseas websites while others were set up using free website services. Free website services were also used by phishing sites spoofing web-based e-mails of universities. These findings point to a tendency of free website services to be abused by attackers attempting to steal e-mail credentials.

In the financial institutions segment, there were reports of phishing sites spoofing a number of credit card brands. These phishing sites typically used a free .cc or .online domain.

Many of the phishing sites spoofing domestic online games were found to be using a URL created with a free .cc domain and a subdomain made to look like that of a legitimate website. These phishing sites were assigned an IP address of one of specific hosting service providers in Hong Kong and China.

The parties that JPCERT/CC contacted for coordination of phishing sites were 25% domestic and 75% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 30%, overseas: 70%).

3.2 Website Defacement Trends

The number of website defacements reported in this quarter was 554. This was a 48% decrease from 1,065 of the previous quarter.

As in the previous quarter, JPCERT/CC confirmed many cases of website defacement involving embedded malicious JavaScript that redirects site visitors to a URL containing the string "jquery.min.php". JPCERT/CC received an altered PHP file and investigation results from the administrator of one of the affected websites it coordinated with. The information provided revealed that, in the case of this website, the CMS it uses served as an attack vector in creating a backdoor that the attacker can use to execute codes and in altering the contents of the PHP file.

Many of the affected websites use a CMS, and judging from the fact that CMSs as well as CMS themes and plug-ins are being targeted in extensive scanning activities, there may be more website defacements than the JPCERT/CC is aware of. Website administrators are advised to keep up-to-date any CMS they

use to administer websites, delete any unnecessary themes or plug-ins, and take any other necessary measures.

3.3 Targeted Attack Trends

There were 10 incidents categorized as a targeted attack. This was a 33% decrease from 15 of the previous quarter. JPCERT/CC requested a total of 2 organizations to take action during this quarter.

Since late July, a number of organizations in Japan have reported malware infections that appear to be the result of targeted attacks by a specific group of attackers.

JPCERT/CC obtained files found on infected devices from these organizations and conducted analysis. As a result, malware classified as an HTTP bot, which performs remote control by communicating with the attacker's server via HTTP, and tools that appear to have been used by the attackers to collect information were identified. JPCERT/CC also investigated proxy server logs provided by the affected organizations and found that communication between the devices infected with the HTTP bot and the attackers' servers contained encrypted strings. When decrypted, these strings were found to contain the results of command execution by the attackers to remotely control the infected devices and collect information.

The series of attacks were undertaken on the affected organizations' networks using a single infected device as a springboard, infecting a large number of devices with the malware. The malware was configured to communicate with different servers for each infected device within the same organization, and C2 servers for transmitting the attackers' commands were identified in large numbers. Moreover, many of the servers used to communicate with the malware were compromised web servers located in Japan. Servers used for these communications were installed with a PHP script through which the attackers communicate with the bot. This PHP script was designed to handle such operations as sending the attackers' commands to the bot, saving data sent from the bot, and obtaining and deleting data saved on the servers.

JPCERT/CC also received reports of other cases, in which the attackers sent PlugX, a type of malware which performs remote control via spoofed e-mails, or malware using a fake extension that downloads and executes a multi-functional bot.

3.4 Other Incident Trends

The number of malware sites reported in this quarter was 337. This was an 86% increase from 181 of the previous quarter.

The number of scans reported in this quarter was 1,098. This was a 28% decrease from 1,520 of the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SMTP (25/TCP), SSH (22/TCP) and HTTP (80/TCP).

[**Chart 4: Number of scans by port**]

Port	Jul	Aug	Sep	Total
25/tcp	167	198	123	488
22/tcp	60	114	73	247
80/tcp	48	40	43	131
23/tcp	43	10	10	63
21/tcp	11	3	6	20
443/tcp	4	4	0	8
3389/tcp	3	1	3	7
6667/tcp	0	5	1	6
53/udp	0	0	6	6
33442/udp	2	2	2	6
4752/udp	3	2	0	5
53413/udp	1	3	0	4
445/tcp	0	2	2	4
1433/tcp	1	0	3	4
8473/udp	0	1	2	3
62374/udp	0	0	3	3
51331/udp	2	1	0	3
5060/udp	1	1	1	3
23887/udp	1	1	1	3
222/tcp	0	3	0	3
143/tcp	0	1	2	3
137/udp	0	0	3	3
8443/tcp	0	2	0	2
8080/tcp	1	0	1	2
5050/tcp	0	1	1	2
441/tcp	2	0	0	2
20472/udp	0	2	0	2
1723/tcp	1	1	0	2
Other	294	104	106	504
Monthly Total	645	502	392	1539

There were 276 incidents categorized as other. This was a 19% decrease from 342 of the previous quarter.

4. Incident Handling Case Examples

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

[Pharming to steal credentials of domestic Internet banking]
Since early August, JPCERT/CC has been receiving numerous reports concerning websites that use an attack method called pharming. In this type of attack, an Internet banking user trying to access a legitimate URL from a web browser will be redirected to a fake website on a server prepared by the attacker, and the credentials entered by the user are stolen.

Some of the servers used by the attackers contain content spoofing domestic Internet banking, and content that appears to be an administration screen used by the attacker. As soon as these servers are identified, JPCERT/CC requests the companies administering the servers to take appropriate steps and undertakes coordination to have these servers suspended.

JPCERT/CC identified and analyzed malware that appears to be related to these cases. The analysis revealed that when a user accesses a specific website, such as that of a domestic financial institution, from an infected PC, the user is redirected to the attacker's server via a proxy embedded in the malware, with specific information added to the HTTP request.

[Coordination involving Japanese e-mails with malware attachment]
During this quarter, many Japanese e-mails with a ZIP file attachment containing malware were found. Many of the e-mails used a sender address, subject and text spoofing a shipping company. They appear to be an attempt to convince the recipient to open the attachment by making it look like a document related to a shipment. There were also other e-mails with a short subject and text that were made to look like a photo or an invoice was attached and urged the recipient to open the attachment.

The attached ZIP files contained malware that is detected by anti-virus software under such names as Shiotob, Bebloh and URLZone. JPCERT/CC analyzed the malware and found that it communicates with a C&C server, then downloads and executes banking malware that is detected under such names as Ursnif and Gozi and that steals the credentials of Internet banking, etc.

JPCERT/CC contacted the telecommunications carriers that manage the domestic IP addresses used to send the reported e-mails with malware attachment, and requested them to confirm relevant facts regarding the delivery of e-mails. With regard to reports that the banking malware that is downloaded was found on an apparently compromised web server with a domestic IP address, JPCERT/CC requested the

hosting service provider to look into the matter and take necessary steps, then subsequently confirmed that the malware has been deleted.

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".