JPCERT-IR-2015-04
Issued: 2015-10-08

JPCERT/CC Incident Handling Report
[July 1, 2015 – September 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 July 1, 2015 through September 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 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]	1543	1215	1370	4128	5187
Number of Incidents [*3]	1626	929	1193	3748	4188
Cases Coordinated [*4]	979	554	525	2058	2593

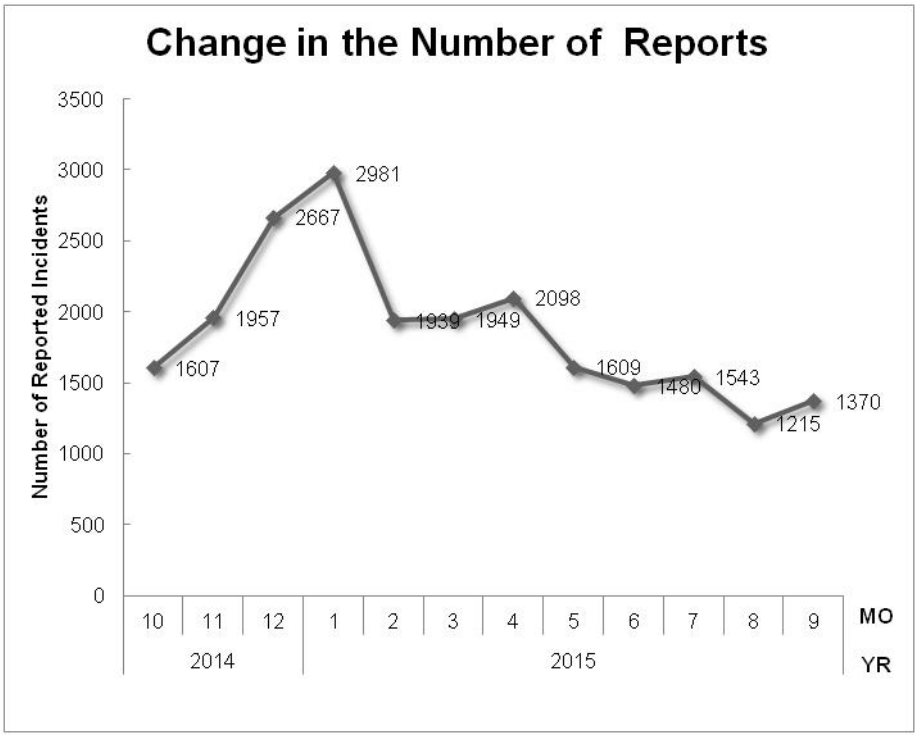
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

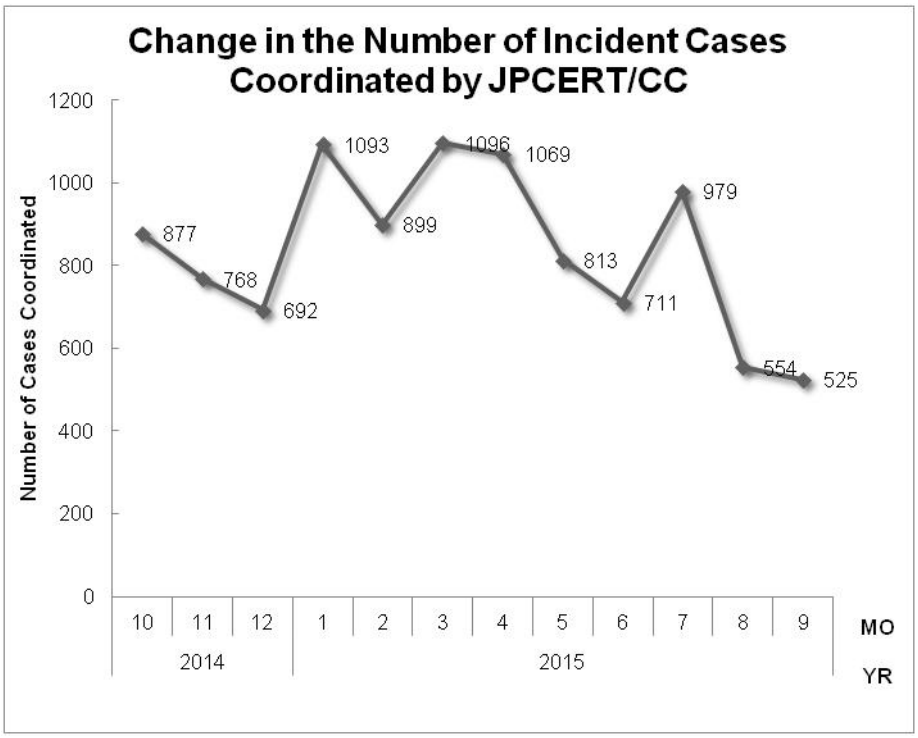
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,128. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,058. When compared with the previous quarter, the total number of reports decreased by 20%, and the number of cases coordinated decreased by 21%. When compared with the same quarter of the previous year, the total number of reports decreased by 11%, and the number of cases coordinated decreased by 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 Reports]



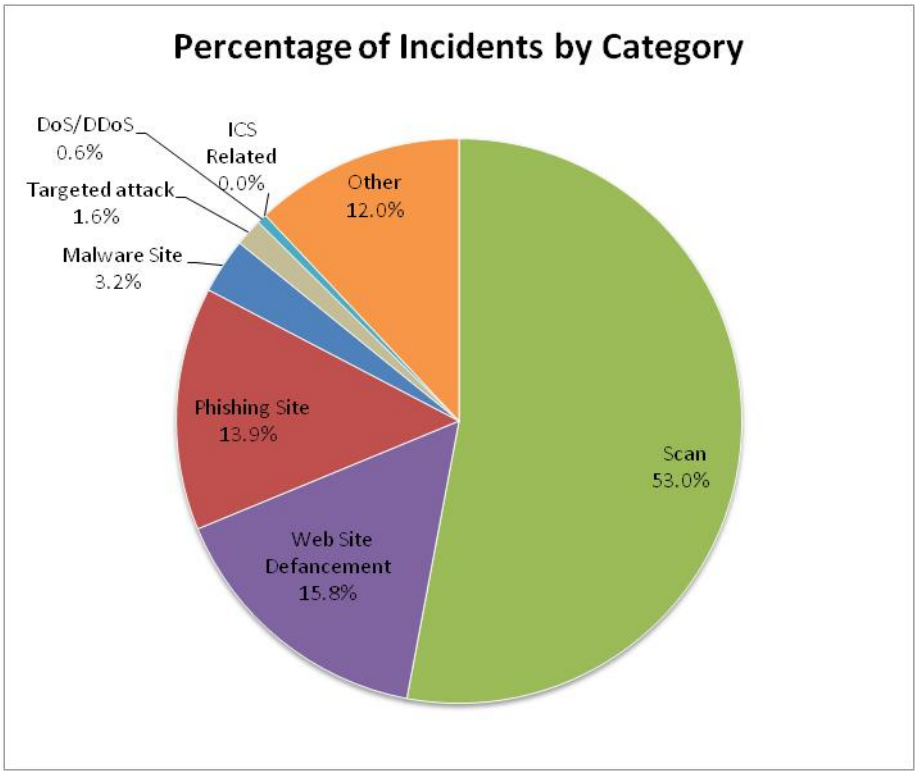
[Figure 2: Change in the Number of Incident Cases Coordinated]

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]

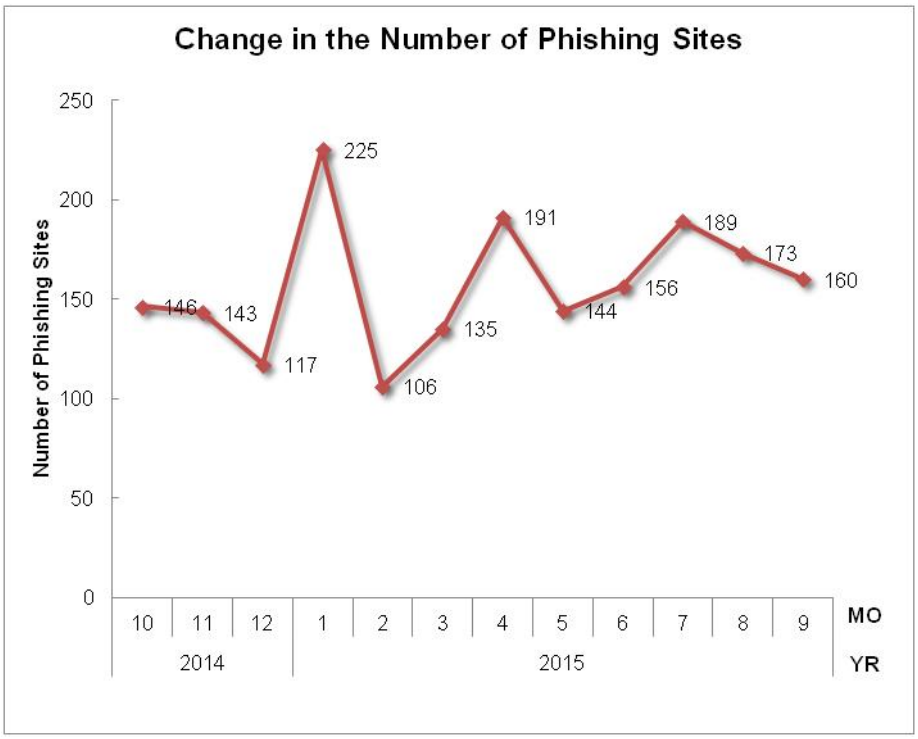
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	189	173	160	522	491
Website Defacement	244	133	215	592	649
Malware Site	51	30	38	119	197
Scan	751	534	700	1985	2442
DoS/DDoS	13	1	7	21	71
ICS Related	0	0	0	0	4
Targeted attack	26	22	11	59	60
Other	352	36	62	450	274

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 53.0%, and incidents categorized as website defacement made up 15.8%. Also, incidents categorized as phishing sites represented 13.9% of the total.

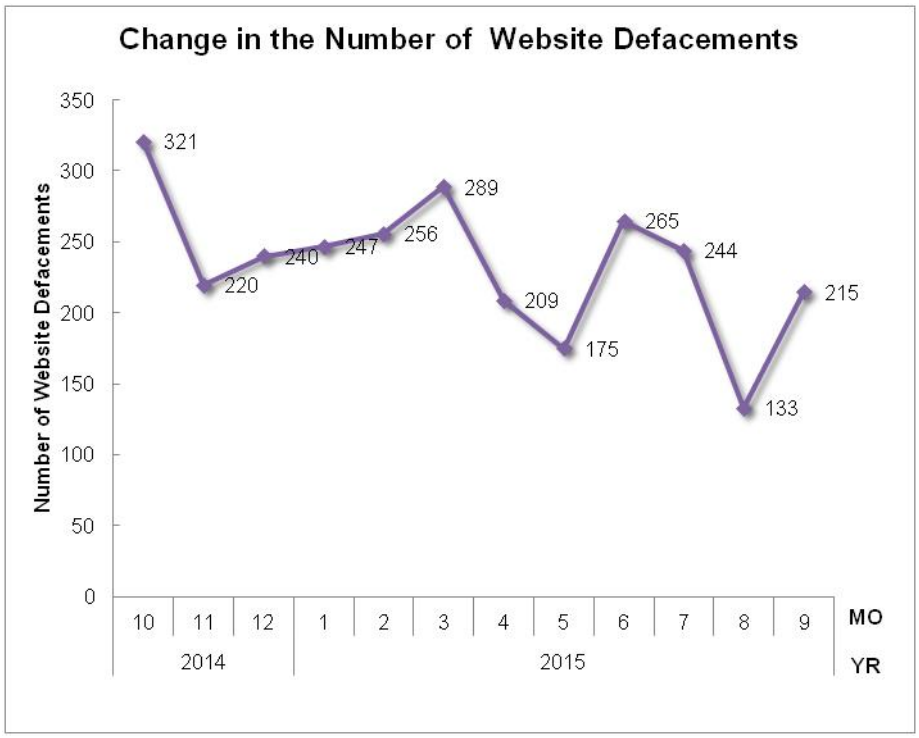


[Figure 3: Percentage of incidents by category]

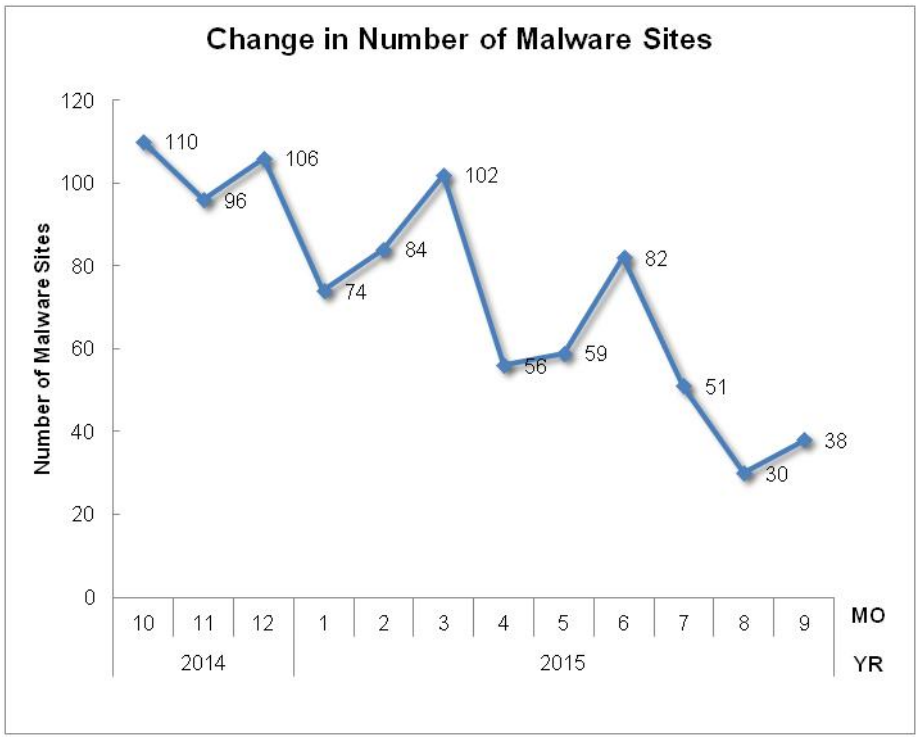
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



[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]

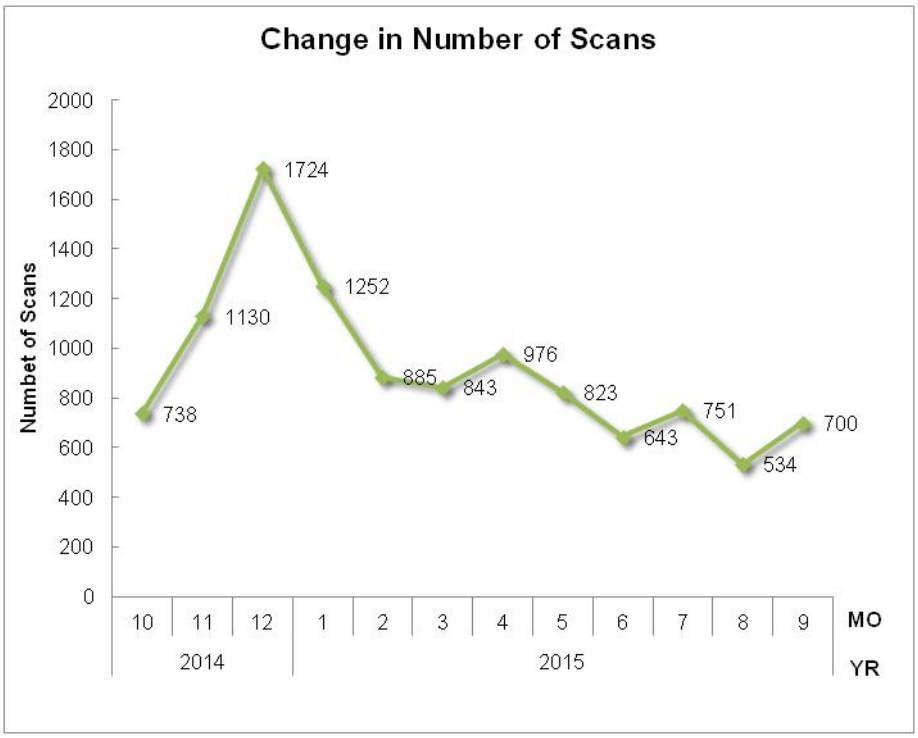
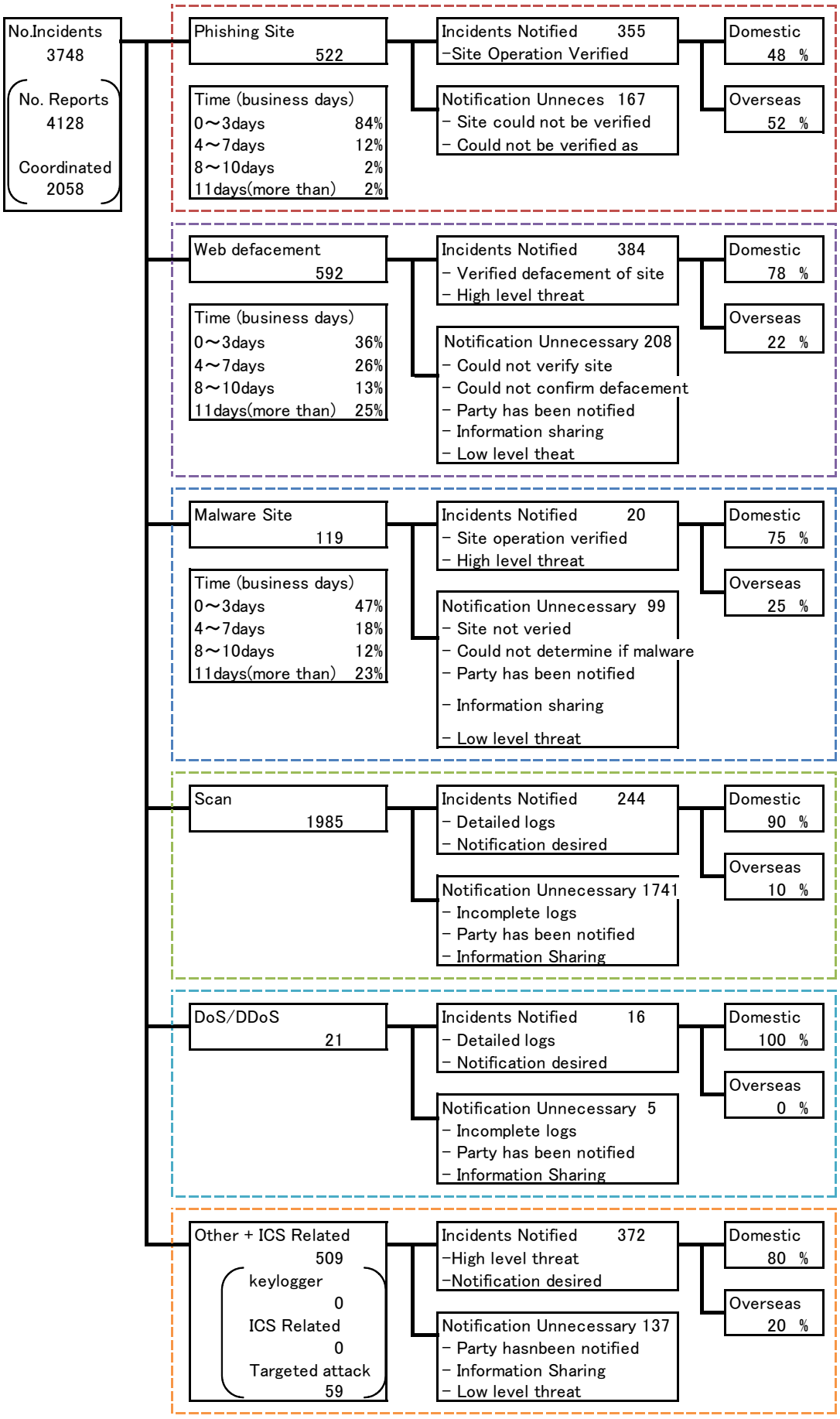


Figure 7: Change in the number of scans]

[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

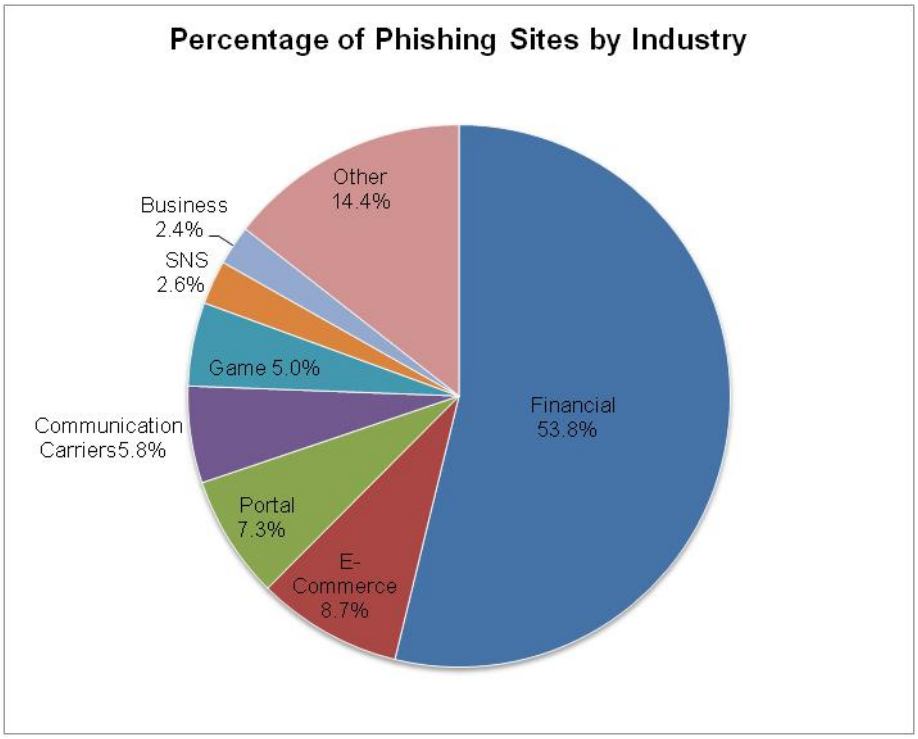
3.1. Phishing Site Trends

522 reports on phishing sites were received in this quarter, representing a 6% increase from 491 of the previous quarter. This marks a 25% increase from the same quarter last year (417). 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	Jul	Aug	Sep	Domestic/ Overseas Total (%)
Domestic Brand	51	32	30	113 (22%)
Overseas Brand	96	97	75	268 (51%)
Unknown Brand (*5)	42	44	55	141 (27%)
Monthly Total	189	173	160	522 (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 113 phishing sites that spoofed domestic brands, decreasing 14 % from 132 of the previous quarter. And there were 268 phishing sites that spoofed overseas brands, increasing 12% from 239 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 53.8% spoofed websites of financial institutions, and 8.7% spoofed e-commerce sites. In both Japanese and overseas brands, financial institutions accounted for most of the spoofed brands.

An investigation of phishing sites spoofing domestic financial institutions and domestic online gaming services found that a large number of .com domains were being used, and most of them had Hong Kong IP addresses. While phishing sites spoofing financial institutions often used domain names that contained a string resembling the target brand name, phishing sites spoofing online gaming services often used domain names consisting of random strings. Further, phishing sites using relatively new gTLDs such as "xyz," "top," and "space" were also confirmed.

Hong Kong (43.1%) and the United States (28.5%) combined accounted for over 70% of the IP addresses used by phishing sites spoofing domestic brands

The parties that JPCERT/CC contacted for coordination of phishing sites were 48% domestic and 52% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 52%, overseas: 48%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 592. This was a 9% decrease from 649 of the previous quarter.

In July, information about a number of vulnerabilities in Adobe Flash Player was released. Shortly afterward, JPCERT/CC confirmed a case of domestic website defacement in which site visitors were redirected to an attack site exploiting those vulnerabilities. JPCERT/CC subsequently received numerous reports of domestic websites defaced for the purpose of the same attack, and a number of defacement patterns have been identified.

During this quarter, JPCERT/CC also confirmed cases in which the Emdivi malware used in attacks targeting domestic organizations was downloaded by accessing a defaced domestic website. The defaced website had a malicious code embedded in a legitimate js file, and this code was redirecting site visitors to a fraudulent page created on the website where an swf file that exploits the above vulnerabilities is loaded.

From around early September, JPCERT/CC has been receiving reports of incidents in which the victims

were presumably redirected to a malware distribution site by an ad embedded in a website. Based on the reports, JPCERT/CC periodically obtained and observed ads on the website, and confirmed that a js file embedded in the ads occasionally contained a malicious code.

3.3. Other Incident Trends

The number of malware sites reported in this quarter was 119. This was a 40% decrease from 197 of the previous quarter.

The number of scans reported in this quarter was 1,985. This was a 19% decrease from 2,442 of the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were HTTP (80/TCP), SMTP (25/TCP), and SSH (22/TCP).

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

Port	Jul	Aug	Sep	Total
80/tcp	352	233	390	975
25/tcp	96	99	145	340
22/tcp	126	84	80	290
21/tcp	63	23	9	95
31385/udp	20	14	11	45
2632/udp	16	17	12	45
61222/udp	17	16	10	43
16358/udp	17	7	5	29
445/tcp	11	10	7	28
1433/tcp	3	10	13	26
3389/tcp	8	11	3	22
443/tcp	0	0	20	20
23/tcp	9	5	6	20
/udp	0	0	17	17
110/tcp	6	2	0	8
3306/tcp	1	1	3	5
8080/tcp	2	0	2	4
5900/tcp	0	0	3	3
8621/tcp	0	0	2	2
19/udp	2	0	0	2
Other	4	4	17	25
Monthly Total	753	536	755	2044

The number of incidents categorized as Other was 450. This was a 64% increase from 274 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 sophisticated attacks targeting domestic organizations]
This quarter, JPCERT/CC contacted 67 organizations regarding targeted attacks. Of these, 52 organizations were contacted regarding remote control malware called Emdivi. In addition, JPCERT/CC also contacted affected organizations and organizations managing servers used as infrastructure in relation to remote control malware called PlugX, a JavaScript tool called Scan Box, which collects information about accessed devices, etc.

In July, a number of cases in which defaced domestic websites were used as Emdivi's infection route were confirmed. Since August, cases in which targeted attack e-mail are sent with Emdivi attached have also been confirmed.

Attackers use devices infected with Emdivi as a springboard to gain access to AD servers or other devices on the same internal network, and attempt to spread the malware or steal information. Attacks were generally conducted in the following steps.

(1) Infect a PC with malware by means of spoofed e-mail or website defacement to create a springboard for attacks within an organization.
(2) Execute standard OS commands such as ipconfig and netstat on the infected device, and obtain device and network information.
Send the information obtained to the C&C server of the malware.
(3) On the infected device, download the following tools to be used to carry out attacks.

- A legitimate Microsoft tool for obtaining AD information
- A malicious tool for stealing login account passwords
- A tool for increasing permissions by exploiting a vulnerability (MS14-068) in Kerberos KDC
- A remote shell client and server used for remote control
- A file compression tool

(4) Obtain an AD administrator account in some way. Tools such as those listed above are probably used to steal an AD administrator account, but no revealing traces can be found in most cases.(5) Use an AD administrator account to register a task to install malware on an AD server, and infect the AD server with malware. Infect devices on the internal network with malware.
(6) Collect document files and other data from devices and servers on the internal network, and use a file compression tool to create a password-protected file for transmission. Files may be sent to an online storage site.

JPCERT/CC will continue to assist affected organizations in responding to attacks and cooperate with investigations, in addition to contacting organizations that are potentially affected, and preventing the spread of damages through cooperation with investigations and other activities.

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

付録-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 specialy 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 2015 Fiscal Year".