JPCERT-IR-2017-04

Issued: 2017-10-12

JPCERT/CC Incident Handling Report
[July 1, 2017 - September 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 July 1, 2017 through September 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]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports *2	1698	1473	1429	4600	5225
Number of Incident *3	1771	1587	1453	4811	5365
Cases Coordinated *4	725	759	750	2234	2553

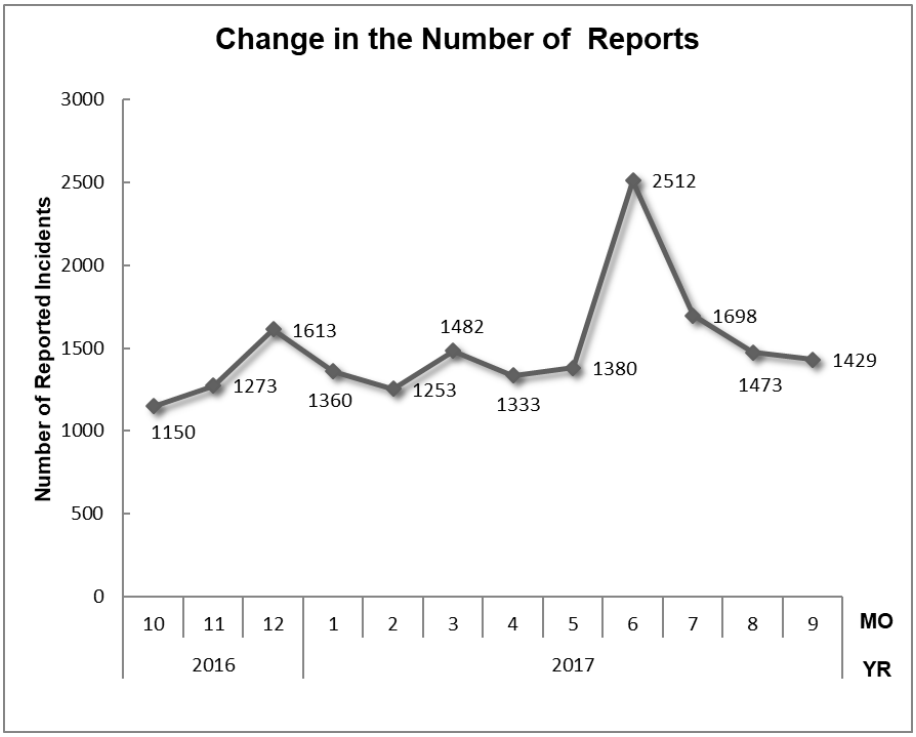
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

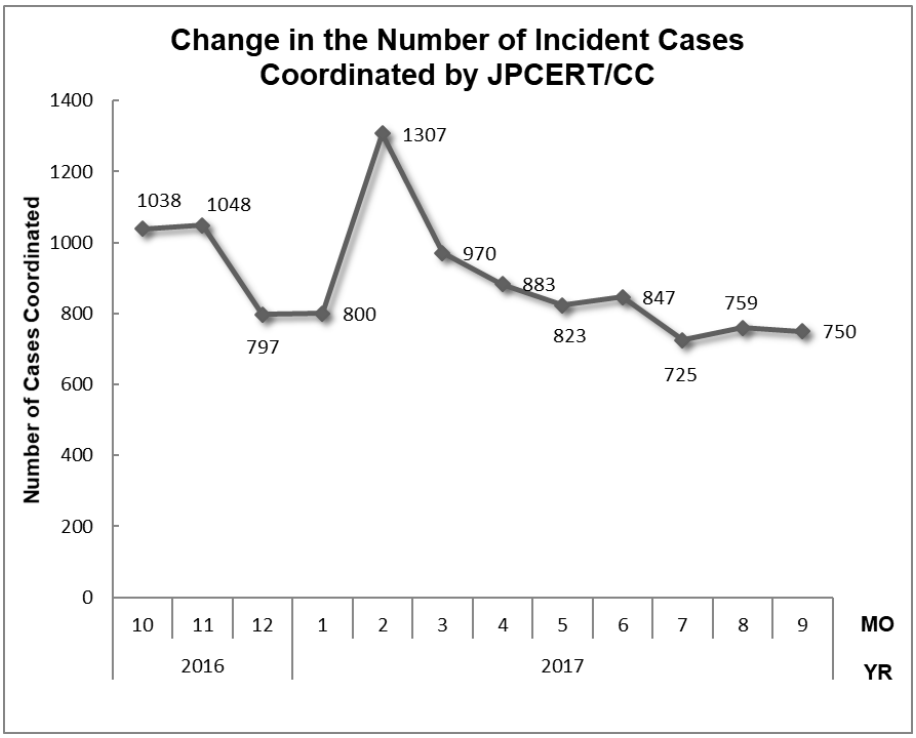
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,600. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,234. When compared with the previous quarter, the total number of reports decreased by 12%, and the number of cases coordinated decreased by 12%. Year on year, the number of reports increased by 47%, and the number of cases coordinated increased by 5%.

[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]



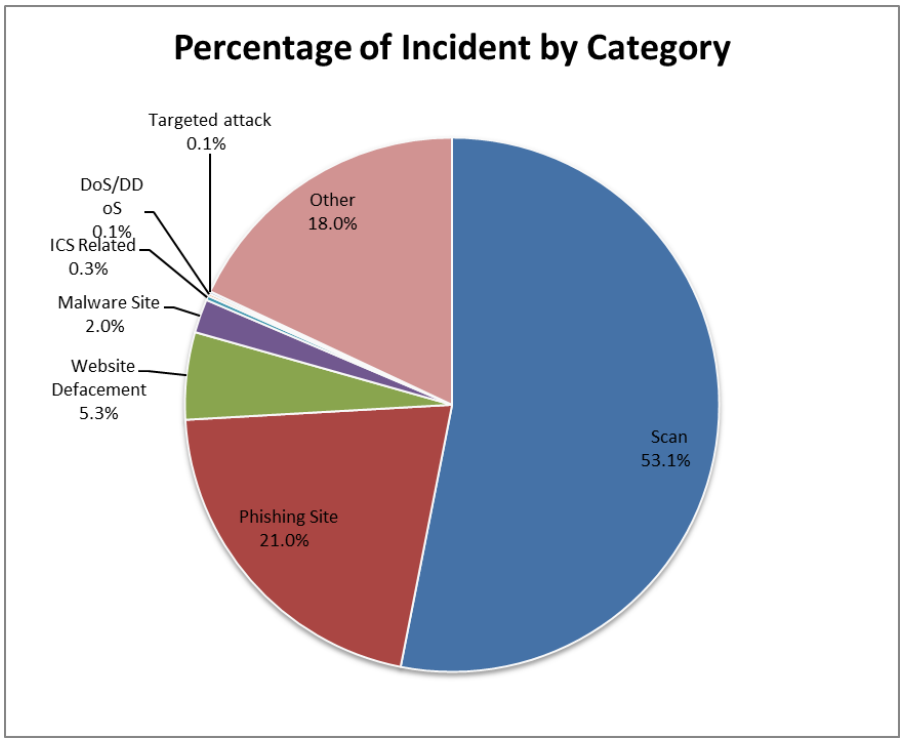
[Figure 2 Change in the number of incident cases coordinated]

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]

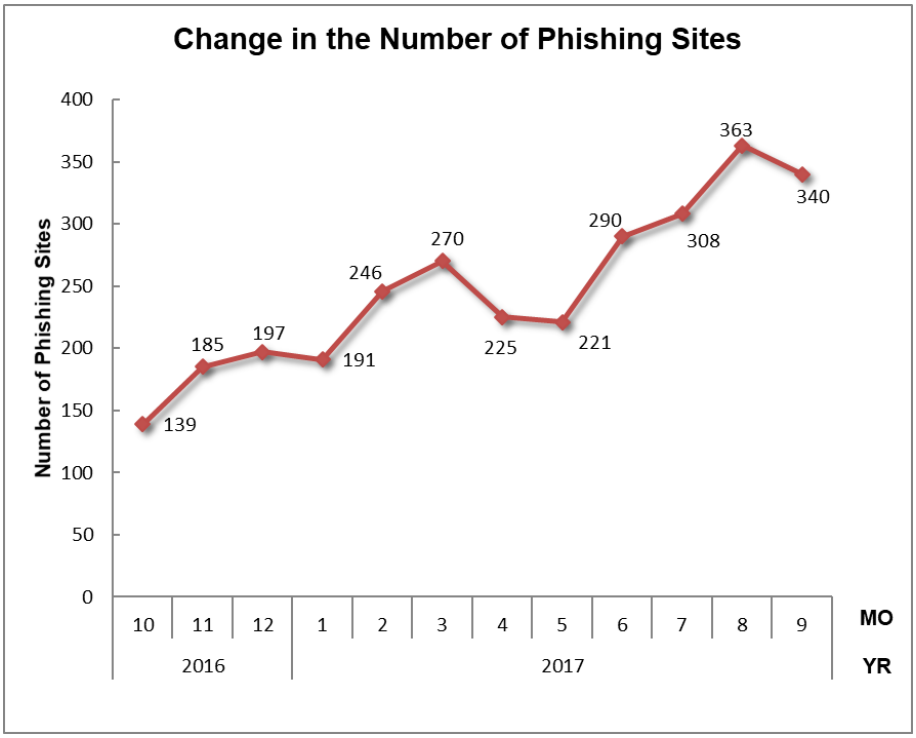
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	308	363	340	1011	736
Website Defacement	75	86	93	254	461
Malware Site	25	42	31	98	59
Scan	1097	827	630	2554	3447
DoS/DDoS	1	0	6	7	3
ICS Related	0	9	4	13	27
Targeted attack	3	0	4	7	9
Other	262	260	345	867	623

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 53.1%, and incidents categorized as phishing sites made up 21.0%.

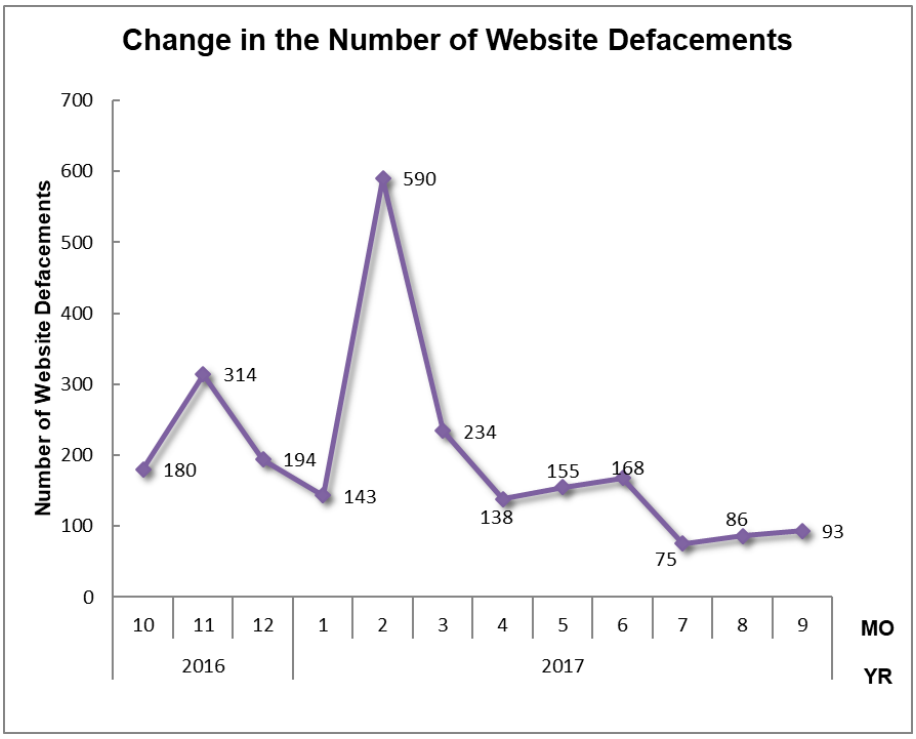


[Figure 3 Percentage of incidents by category]

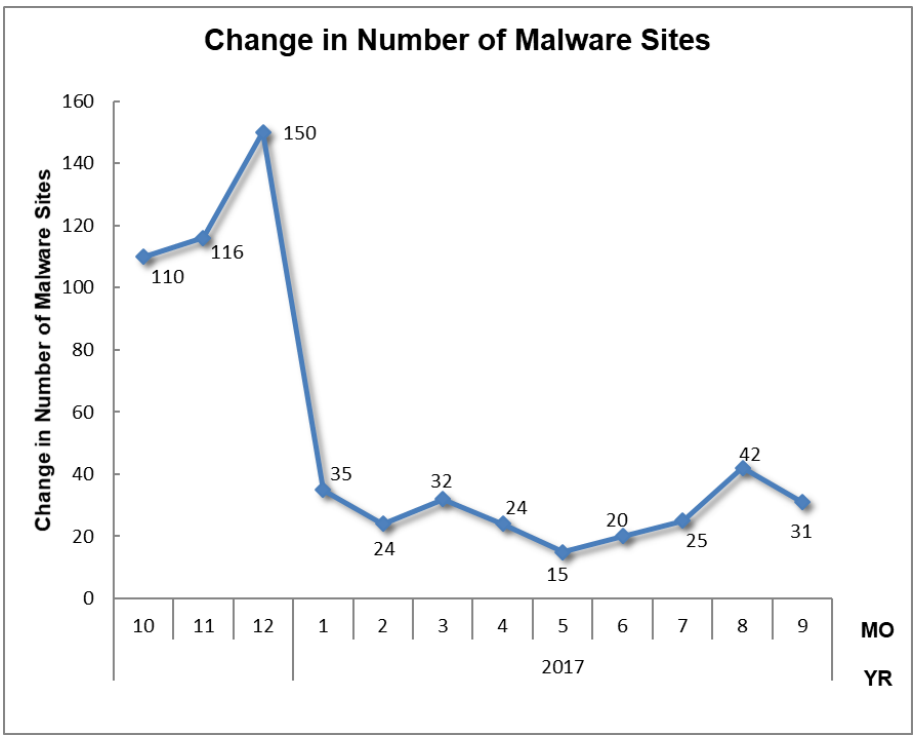
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



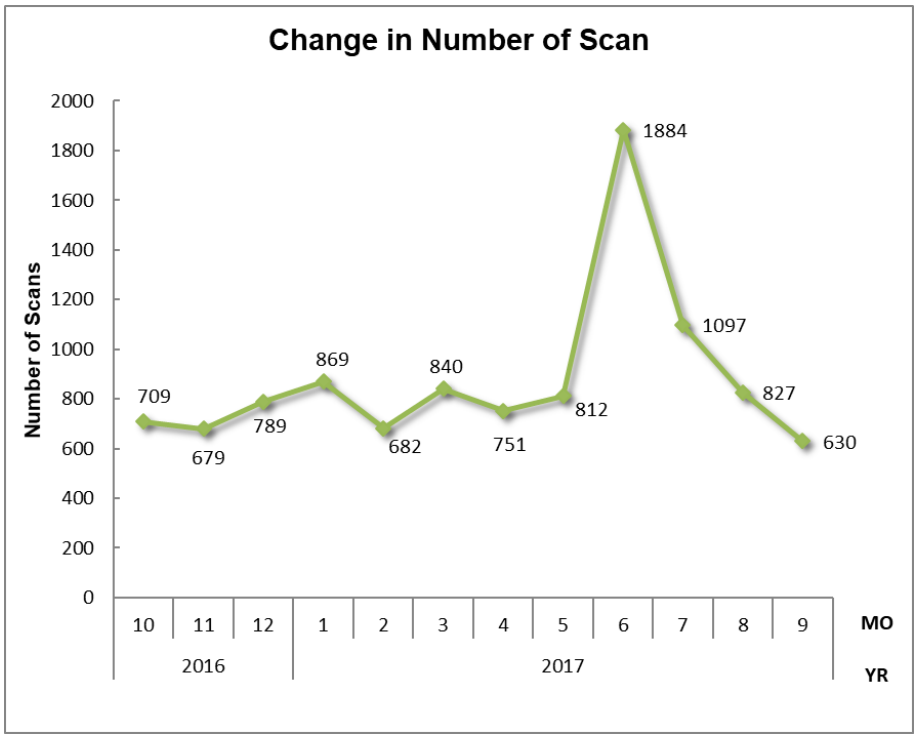
[Figure 4 Change in the number of phishing sites]



[Figure 5 Change in the number of website defacements]

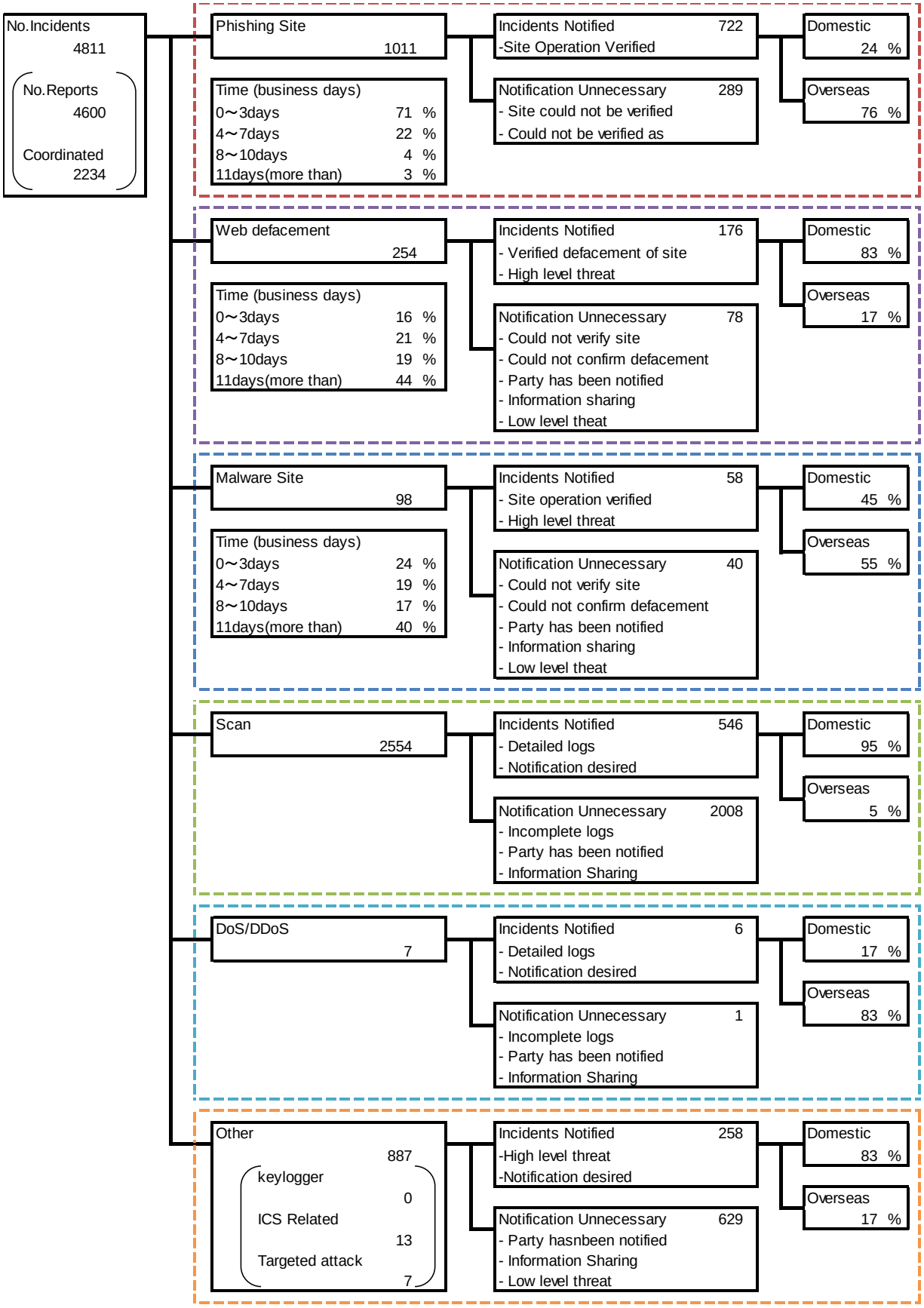


[Figure 6 Change in the number of malware sites]



[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

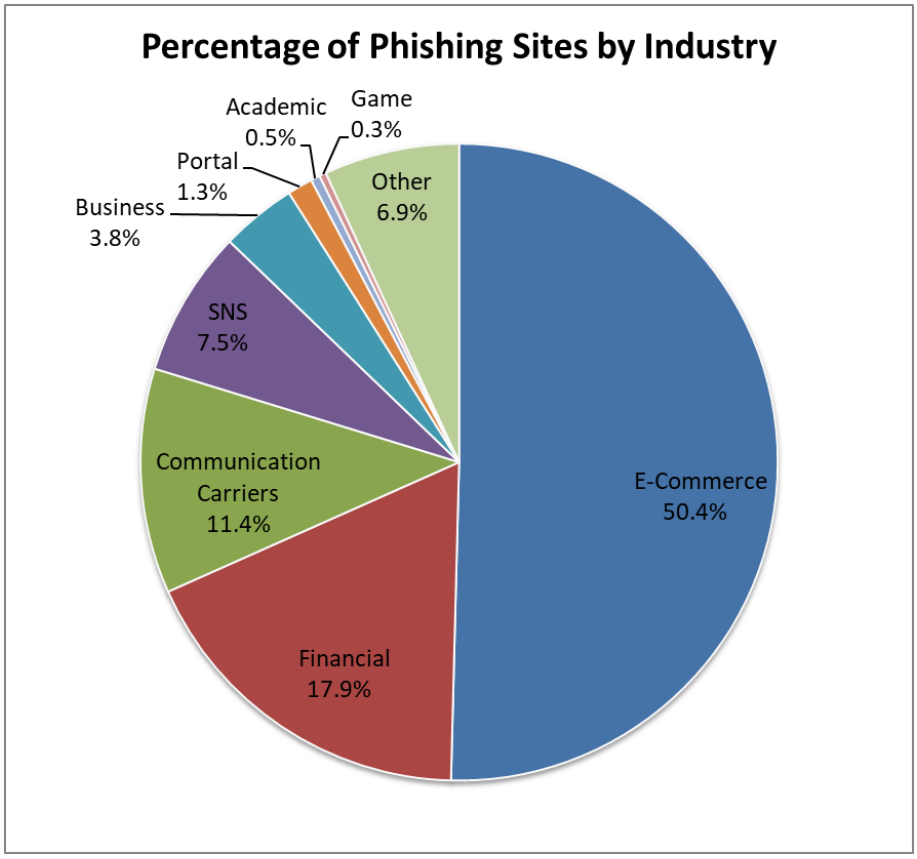
3.1. Phishing Site Trends

During this quarter, 1,011 reports on phishing sites were received, representing a 37% increase from 736 in the previous quarter. This marks a 116% increase from the same quarter last year (467). 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	Jul	Aug	Sep	Domestic/ Overseas Total (%)
Domestic Brand	69	58	46	173(17%)
Overseas Brand	196	253	237	686(68%)
Unknown Brand [*5]	43	52	57	152(15%)
Monthly Total	308	363	340	1011(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 173 phishing sites that spoofed domestic brands, decreasing 17% from 209 in the previous quarter. There were 686 phishing sites that spoofed overseas brands, increasing 17% from 586 in the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 50.4% spoofed e-commerce websites, 17.9% websites of financial institutions, and 11.4% websites of telecommunications carriers.

During this quarter, JPCERT/CC observed many phishing sites where the attackers seem to have newly obtained a domain or rented a server to use specifically for phishing, and many of these phishing sites used a free SSL server certificate to enable HTTPS connections.

Previously, most phishing sites were created by planting phishing content on common websites that did not use a server certificate, and there were not many phishing sites that used HTTPS. Due to the availability of services offering free certificates as well as website creation services and CDN services that provide certificates, attackers can now easily set up HTTPS phishing sites by taking advantage of such services or hacking into websites that use such services. As such, while it used to be possible to identify phishing sites by checking the browser address bar to see whether the site used an HTTPS URL, this is no longer a reliable discerning method.

With respect to domestic brands, there were many reports regarding phishing sites spoofing the web-based e-mail services of domestic telecommunications carriers and phishing sites spoofing SNS sites, as in the previous quarter. Many of the phishing sites spoofing domestic telecommunications carriers were set up using free overseas website creation services, and directed victims to the site by using a shortened URL. Also, most of the phishing sites spoofing an SNS site used a .cn domain name disguised as a legitimate site.

The parties that JPCERT/CC contacted for coordination of phishing sites were 24% domestic and 76% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 26%, overseas: 74%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 254. This was a 45% decrease from 461 in the previous quarter.

There were far fewer reports of website defacements this quarter, compared to the previous quarter. This decrease may be attributable to the absence of new vulnerabilities that facilitate website defacements, as

well as a shift from drive-by download attacks using compromised websites to sending e-mails with an attachment as the primary method of distributing malware.
Starting in late August, JPCERT/CC has been observing cases where victims were directed to a support scam website by means of a malicious script embedded at the end of a web page using CMS. The support scam website displayed a fake alert indicating that the computer has been infected with malware. Victims were then prompted to call the number shown to receive instructions on how to remove the malware.

3.3. Targeted Attack Trends

There were 7 incidents categorized as a targeted attack. This was a 22% decrease from 9 in the previous quarter. JPCERT/CC asked 7 organizations to take action this quarter.

Around late July, a number of organizations reported incidents of e-mail spoofing that appeared to be a targeted attack. These cases all used the same attack method and similar file names.

One of the spoofed e-mails reported had a ZIP file attachment that contained a shortcut file (LNK file) disguised as a text file, and an RTF document file. These files were designed to download and execute a PowerShell script from an overseas server when opened. The RTF file contained a code that downloads and executes the script exploiting the vulnerability in a Microsoft product that was fixed in April 2017 (CVE-2017-0199). The script that gets downloaded in the end was designed to manipulate the compromised computer, and its code resembled a tool that is used to diagnose vulnerabilities.

Another spoofed e-mail that was reported contained a link to download a ZIP file that also contained an RTF file and LNK file. While the RTF file in this case was harmless, the LNK file was designed to download and execute a PowerShell script from a host it specified.

All of these spoofed e-mails were forwarded from a mail server located in Japan. JPCERT/CC contacted the organization that was administering the source server and was later notified that an account was being used fraudulently.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 98. This was a 66% increase from 59 in the previous quarter. JPCERT/CC received many reports this quarter regarding ransomware that gets downloaded from a script file attached to a suspicious e-mail, and financial malware that gets downloaded by executing a macro-enabled document file or by accessing a link contained in the e-mail body.

The number of scans reported in this quarter was 2,554. This was a 26% decrease from 3,447 in the previous quarter. The ports that the scans targeted are listed in [Chart 4].

[Chart 4: Number of scans by port]

Port	Jul	Aug	Sep	Total
22/tcp	892	438	348	1678
25/tcp	122	185	132	439
80/tcp	63	76	28	167
53/udp	29	51	5	85
23/tcp	24	12	23	59
21/tcp	12	10	14	36
445/tcp	9	5	8	22
2222/tcp	8	10	4	22
3389/tcp	4	5	9	18
2323/tcp	3	3	4	10
9000/tcp	3	0	5	8
443/tcp	1	0	7	8
1433/tcp	2	3	3	8
993/tcp	1	1	4	6
81/tcp	3	1	2	6
4752/udp	1	1	4	6
123/udp	0	1	3	4
8080/tcp	0	2	1	3
7547/tcp	2	0	1	3
5060/udp	1	1	1	3
2375/tcp	0	0	3	3
143/tcp	1	2	0	3
50681/udp	1	0	1	2
3544/udp	2	0	0	2
110/tcp	0	1	1	2
Unknown	548	693	583	1824
Monthly Total	1732	1501	1194	4427

Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP). From mid-June to mid-July, JPCERT/CC received many reports regarding SSH scans performed from an IP address in Japan. JPCERT/CC worked with a domestic Internet service provider to investigate the host that was scanning

SSH ports and found that the host might have been used as a springboard for attacks by an attacker exploiting a vulnerability in a wireless LAN router. JPCERT/CC coordinated with the company that sells the router product in question and published an alert regarding vulnerabilities in router products.

There were 867 incidents categorized as other. This was a 39% increase from 623 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 a server administration tool embedded with malware]
Around mid-August, KrCERT/CC, South Korea's national CSIRT, provided information that a South Korean company distributing a server administration tool had been hacked and the tool was published with malware embedded between late July and early August. KrCERT/CC also provided a list of IP addresses in Japan that accessed the link for downloading the tool during the period when the tool was published with malware embedded.

JPCERT/CC contacted Japanese organizations that may have downloaded the tool to advise them to check that they have not downloaded the version embedded with malware, and to update the tool to the latest version if they are using it. As a result, a number of organizations replied that they actually downloaded and were using the tool. On the other hand, many organizations replied that they could not confirm whether the tool was actually downloaded and used based on the information provided by JPCERT/CC.

[Coordination involving a variant of the WannaCry ransomware]
Around mid-August, multiple organizations in Japan reported that a variant of the WannaCry ransomware was detected on their internal network. WannaCry was identified around mid-May as ransomware that encrypts the files on an infected computer and demands payment of money to have the files decrypted. Then in late June, a variant of the ransomware that does not encrypt files was identified.

According to information provided by an affected organization, while there were no cases of files being encrypted, the computer infected with the malware scanned the internal network using a vulnerability in the SMBv1 protocol (MS17-010), thereby spreading the infection. As a result, the organization experienced increased communication traffic due to newly infected computers performing the scan, and abnormal termination of the operating system on some hosts that were scanned. JPCERT/CC analyzed a malware sample provided by the affected organization and found that it was a WannaCry variant that does not perform file encryption due to a defect in the code that executes encryption.

Overseas security organizations continually provide JPCERT/CC with the IP addresses of computers in Japan that accessed the domain that WannaCry communicates with. Based on this information, JPCERT/CC is contacting domestic organizations that may have infected computers.

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.

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".