JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IR-2017-02

Issued: 4/13/2017

JPCERT/CC Incident Handling Report
[January 1, 2017 - March 31, 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 January 1, 2017 through March 31, 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]

	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports *2	1360	1253	1482	4095	4036
Number of Incident *3	1405	1848	1603	4856	4122
Cases Coordinated *4	800	1307	970	3077	2883

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

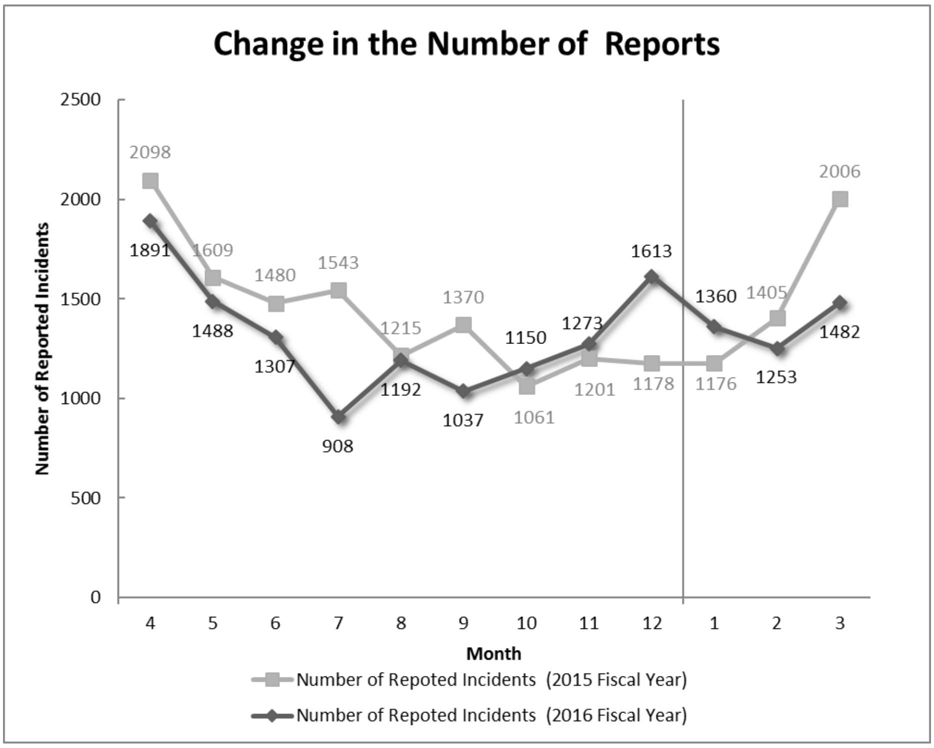
[*3] "Number of Incidents" refers to the number of incidents contained in each report.
Multiple reports on the same incident are counted as 1 incident.

[*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

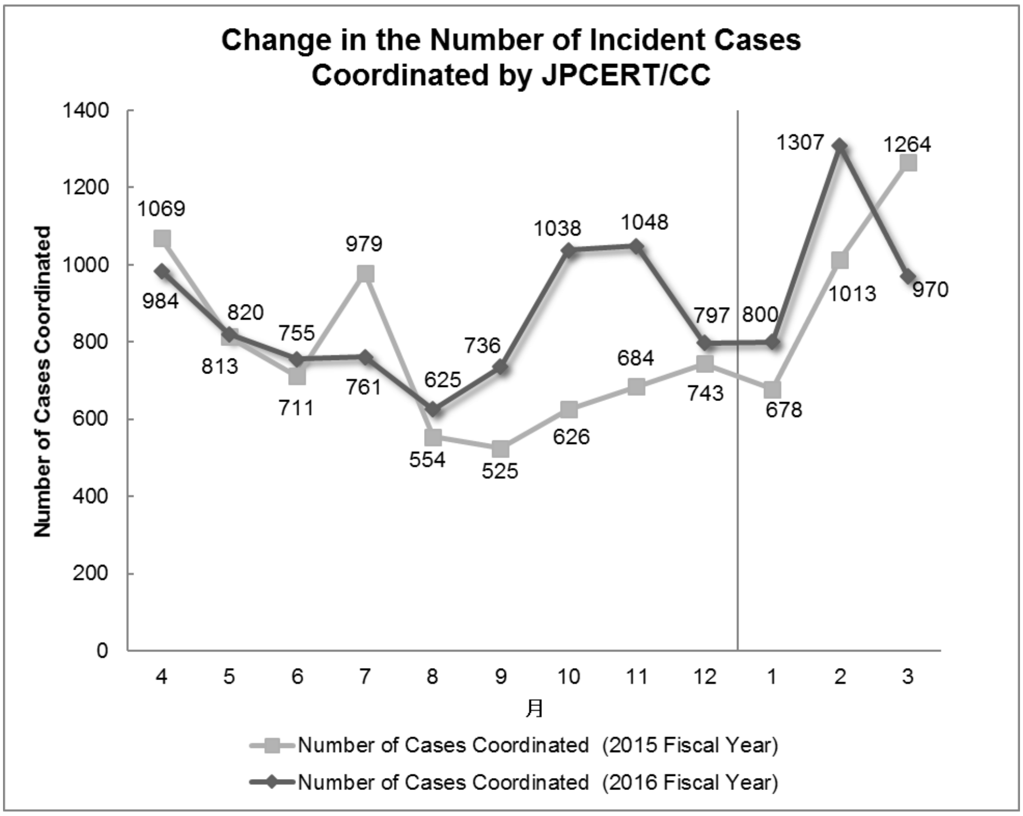
address any issues.

The total number of reports received in this quarter was 4,095. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 3,077. When compared with the previous quarter, the total number of reports increased 1%, and the number of cases coordinated increased 7%. When compared with the same quarter of the previous year, the total number of reports decreased by 11%, and the number of cases coordinated increased by 4%.

[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]

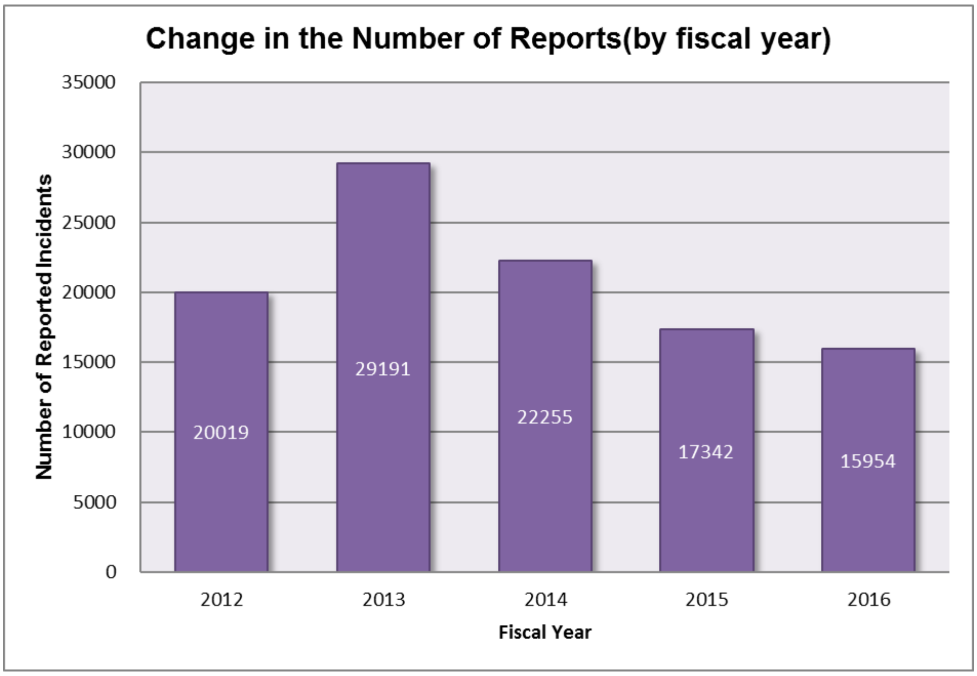
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2016. Each fiscal year begins on April 1 and ends on March 31 of the following year.

[Chart 2: Change in the total number of reports]

FY	2012	2013	2014	2015	2016
Number of Reports	20019	29191	22255	17342	15954

The total number of reports received in FY2016 was 15,954. This marked an 8% decrease from the 17,342 reports received in the previous fiscal year. [Figure 3] shows the change in the total number of reports in the past 5 years.



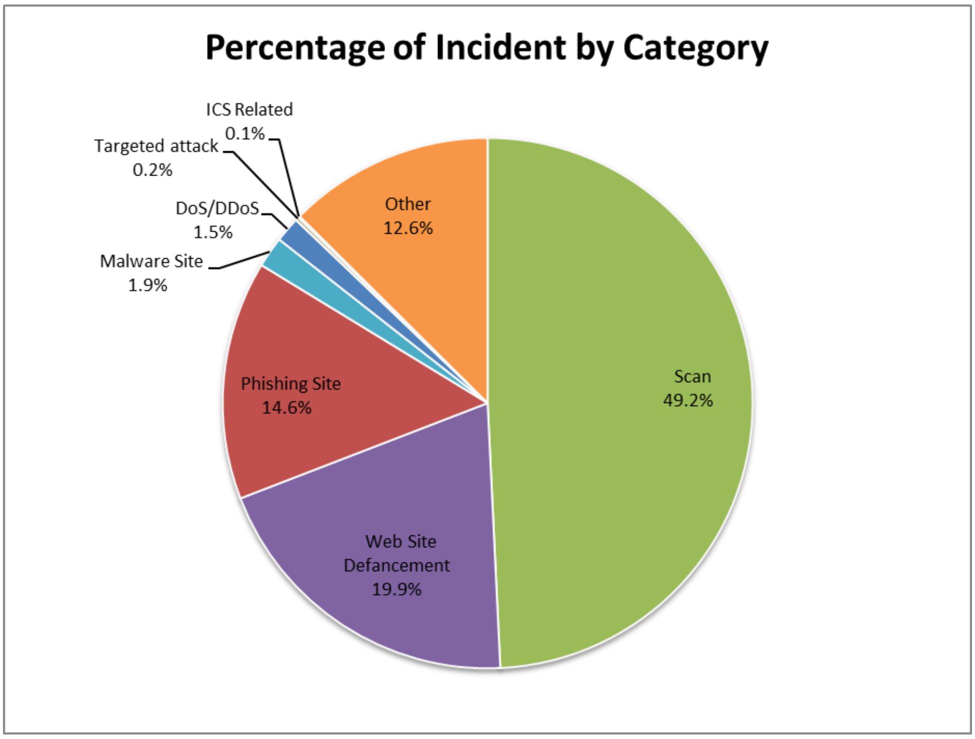
[Figure 3: Change in the total number of reports (by fiscal year)]

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 3] shows the number of incidents received per category in this quarter.

[Chart 3: Number of incidents by category]

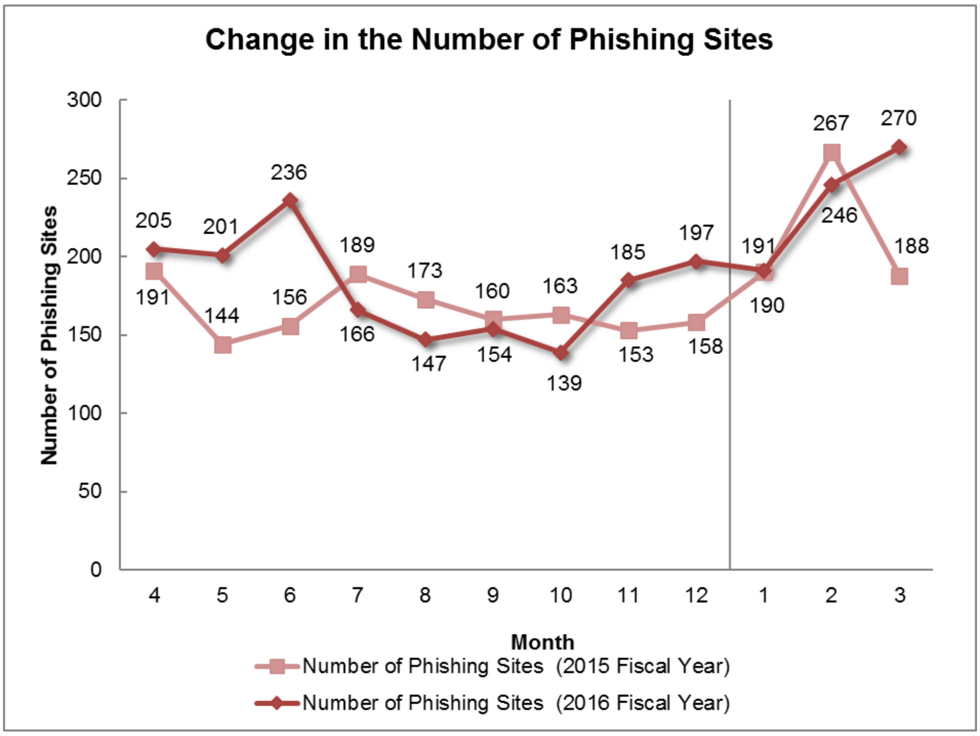
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	191	246	270	707	521
Website Defacement	143	590	234	967	688
Malware Site	35	24	32	91	376
Scan	869	682	840	2391	2177
DoS/DDoS	16	58	1	75	61
ICS Related	3	0	1	4	24
Targeted attack	4	6	1	11	15
Other	144	242	224	610	260

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 4]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 49.2%, and incidents categorized as website defacement made up 19.9%. Also, incidents categorized as phishing sites represented 14.6% of the total.

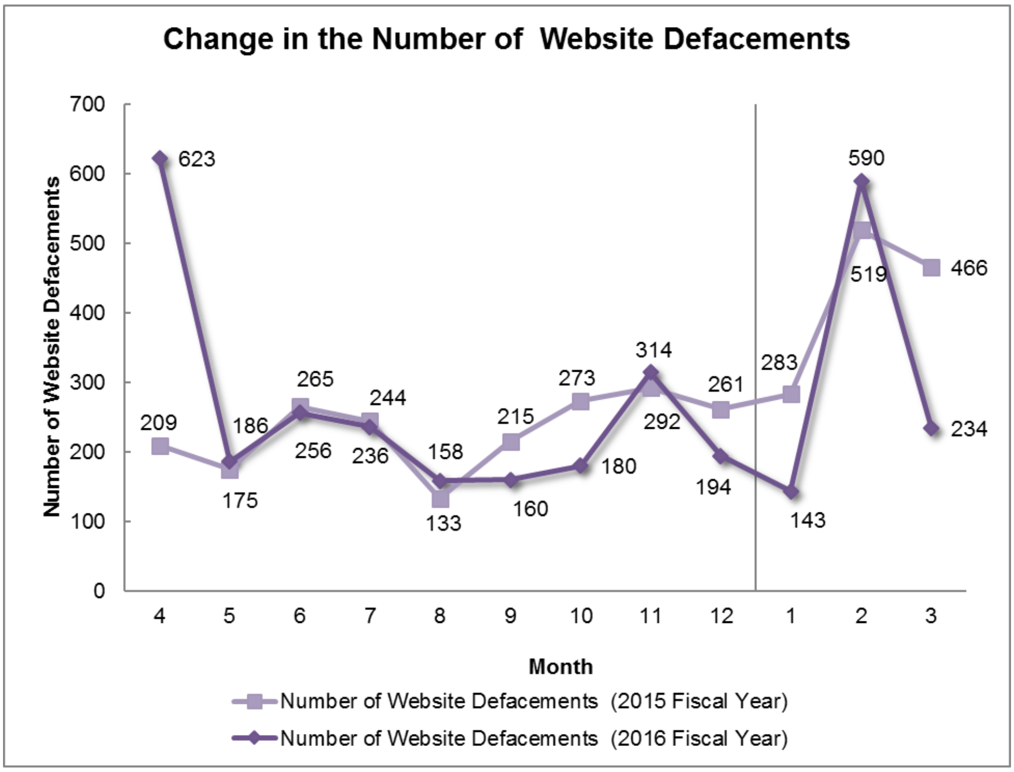


[Figure 4 Percentage of incidents by category]

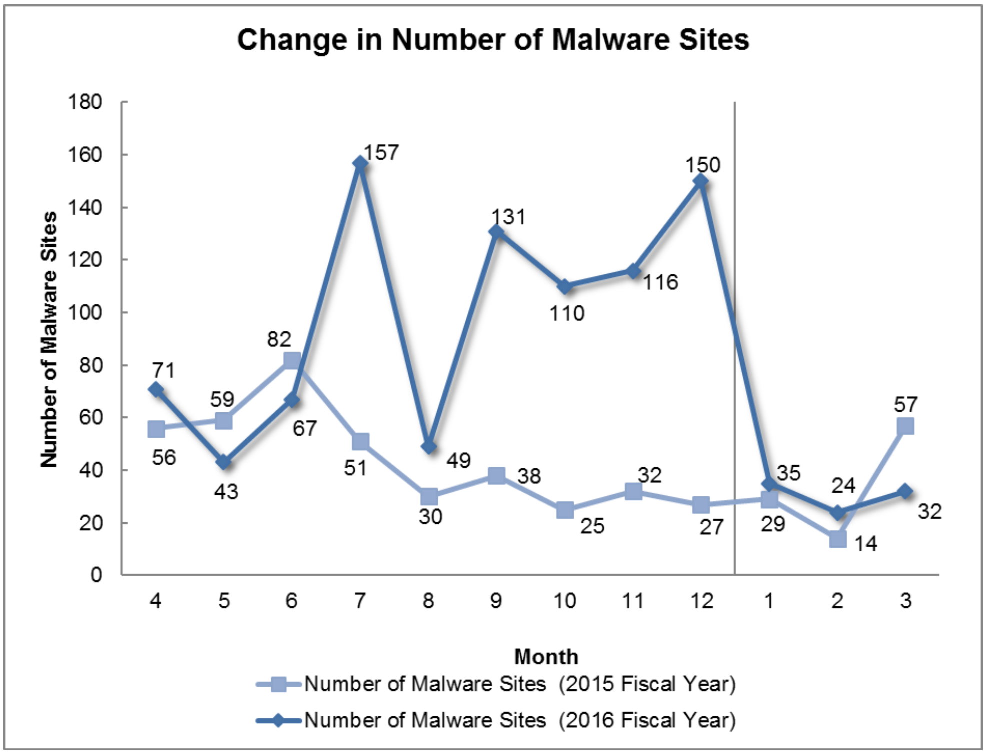
[Figure 5] through [Figure 8] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



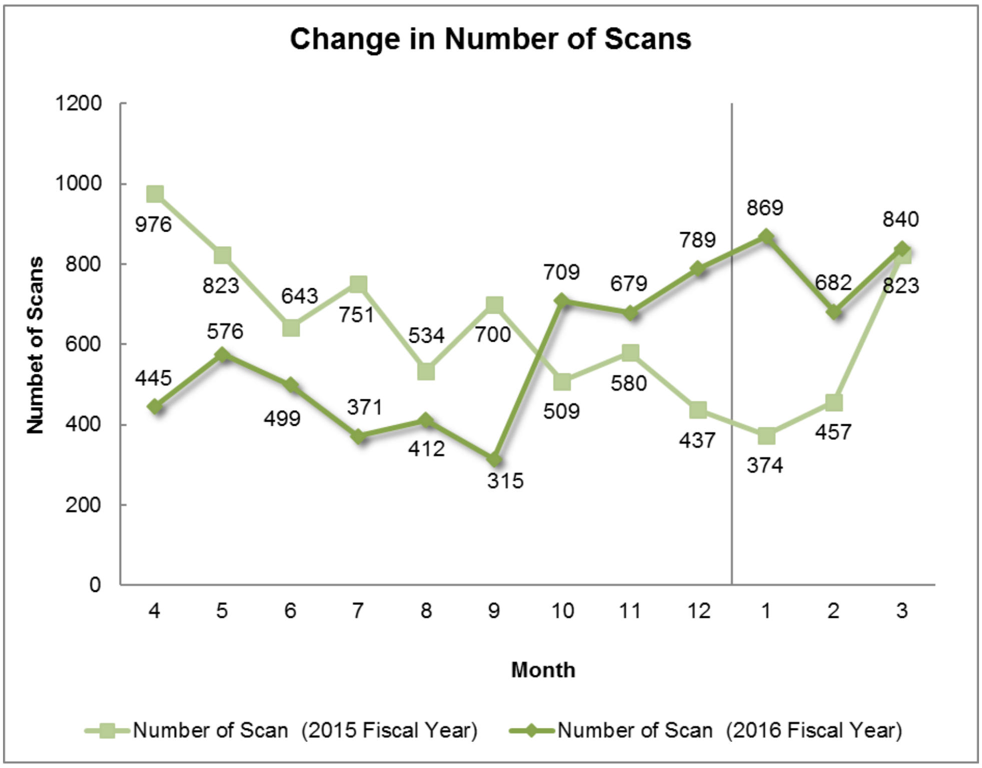
[Figure 5 Change in the number of phishing sites]



[Figure 6 Change in the number of website defacements]

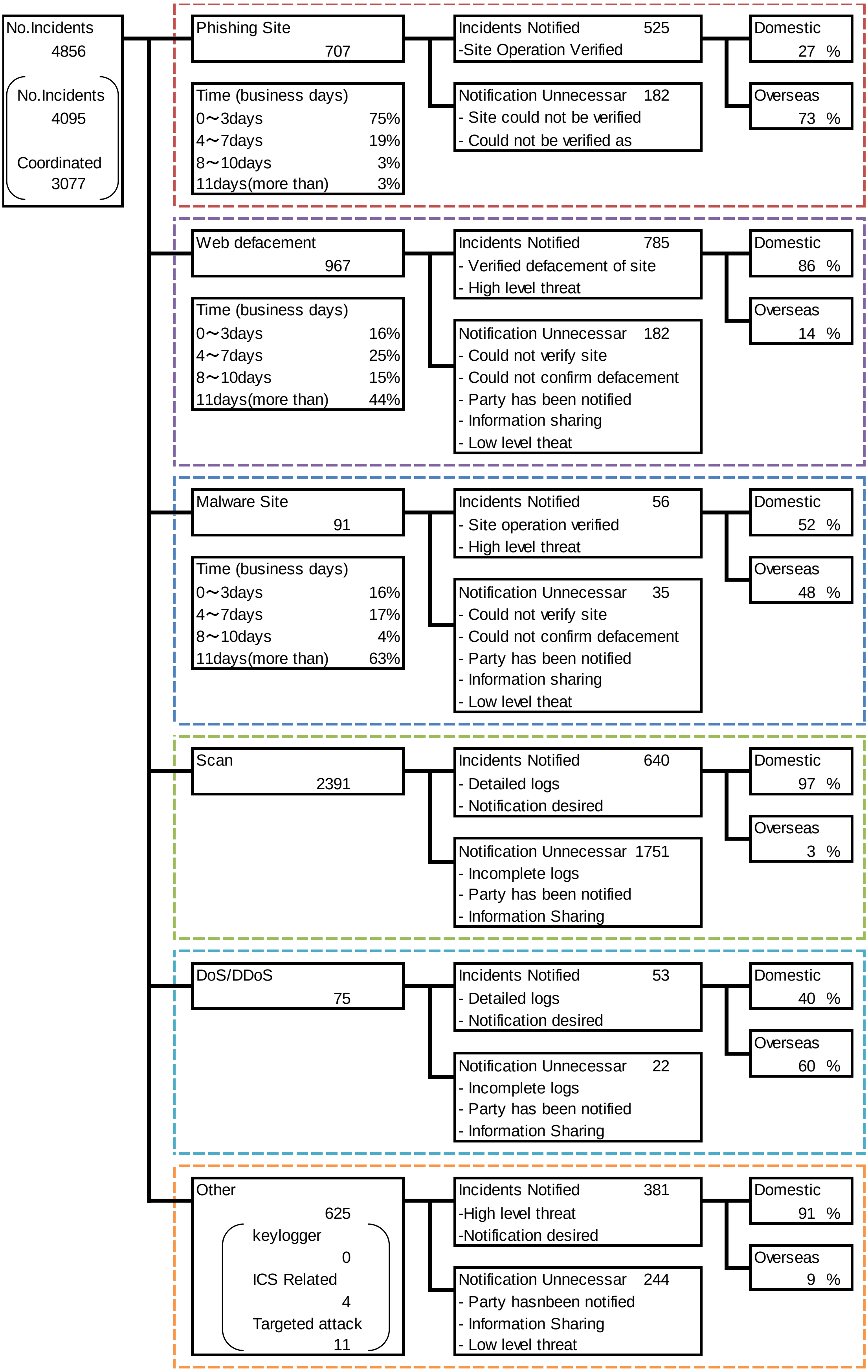


[Figure 7 Change in the number of malware sites]



[Figure 8 Change in the number of scans]

[Figure 9] provides an overview as well as a breakdown of the incidents that were coordinated / handled.



[Figure 9 Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1.Phishing Site Trends

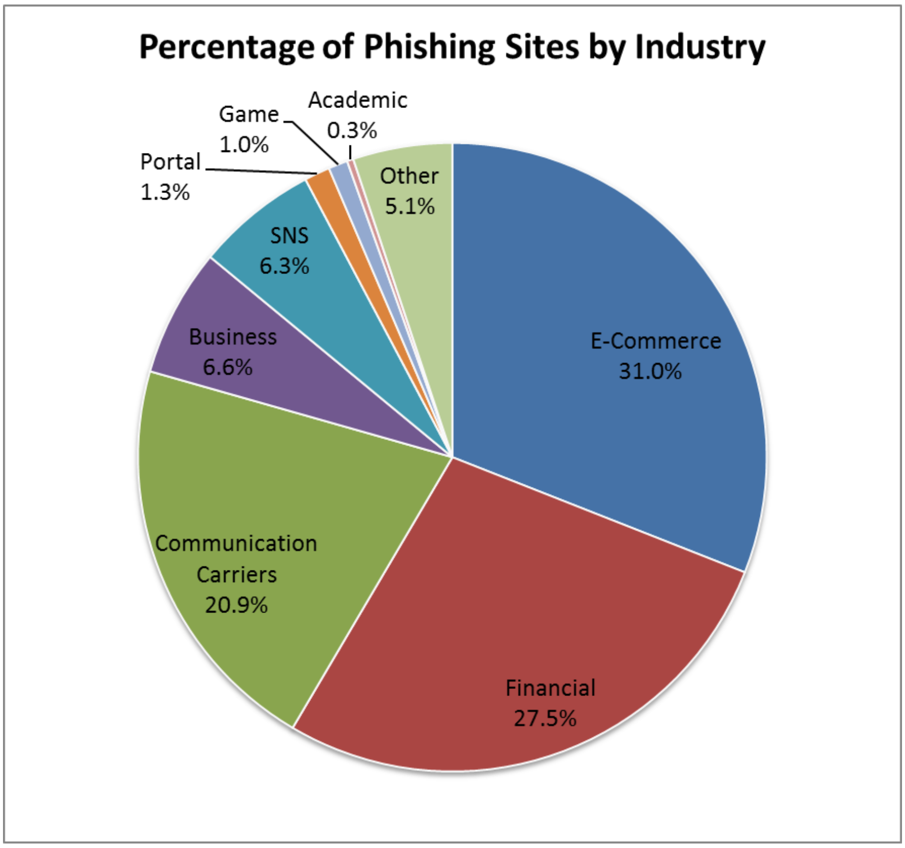
707 reports on phishing sites were received in this quarter, representing a 36% increase from 521 of the previous quarter. This marks a 10% increase from the same quarter last year (645).

The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 4], and a breakdown by industry is shown in [Figure 10].

[Chart 4 Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jan	Feb	Mar	Domestic/ Overseas Total (%)
Domestic Brand	56	42	85	183(26%)
Overseas Brand	111	161	152	424(60%)
Unknown Brand [*5]	24	43	33	100(14%)
Monthly Total	191	246	270	707(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 10 Percentage of reported phishing sites by industry]

During this quarter, there were 183 phishing sites that spoofed domestic brands, increasing 37% from 134 of the previous quarter. And there were 424 phishing sites that spoofed overseas brands, increasing 52% from 279 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 31.0% spoofed e-commerce websites, 27.5% websites of financial institutions, and 20.9% websites of telecommunications carriers.

On phishing sites of domestic brands, there were many reports regarding phishing sites spoofing the login screen of web-based e-mail services of domestic telecommunications carriers. Most of these phishing sites have foreign IP addresses and were created on overseas websites and hosting services that appear to have been hacked. In particular, a specific Russian hosting service was continually used.

Since January, phishing e-mails spoofing Microsoft Japan have been continually observed. These phishing e-mails attempt to lead the recipient to perform authentication from a link contained in the message, saying that the product key of Office software has been illegally copied and that verification needs to be performed. The link directs the recipient to a phishing site designed to steal Microsoft account information, and the host names invariably contained words such as "support," "security" and "microsoft."

The parties that JPCERT/CC contacted for coordination of phishing sites were 27% domestic and 73% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 38%, overseas: 62%).

3.2.Website Defacement Trends

The number of website defacements reported in this quarter was 967.
This was a 41% increase from 688 in the previous quarter.

JPCERT/CC has received a number of reports since around January concerning a website that seems to have been altered to make a pop-up message appear upon access, prompting the visitor to update fonts. When the visitor presses the button on the pop-up, an EXE file is downloaded. It has been confirmed that executing this file will infect the computer with ransomware. The malicious script that displays the pop-up was designed to be embedded in a page only when the referer and user agent of the access source meet certain conditions and at the first access from the access source IP address.

Around early February, large scale attacks exploiting the vulnerabilities of the WordPress REST API were carried out, and numerous cases of defacements apparently caused by the attacks were found among domestic websites. The defacements consisted of a message embedded on a page by a foreign hacker group.

3.3.Targeted Attack Trends

There were 11 incidents categorized as a targeted attack. This was a 27% decrease from 15 of the previous quarter. JPCERT/CC did not ask any organization to take action this quarter.

A number of reports were received in February and March concerning e-mail spoofing that appeared to be a targeted attack. The e-mails analyzed by JPCERT/CC either had a ZIP file attached or contained a link for downloading a ZIP file. In either case, the ZIP file contained a shortcut file with the .lnk extension. This shortcut file was designed to download and execute additional files using PowerShell commands when opened. Downloaded files, which included PowerShell scripts and EXE files, differed with the attack.

In cases where a PowerShell script gets downloaded, executing the .lnk file first initiates an access to a shortened URL, then a PowerShell script disguised as an image file is downloaded from a redirected site. It was confirmed that when the downloaded PowerShell script is executed, malware is executed in the background while a dummy document is opened, resulting in infection with malware (HTTP bot) called ChChes, which communicates with a C&C server through HTTP. A number of C&C servers involved in similar attacks have been identified. Various domain names were used, but there were similarities in their domain registration information.

Targeted attack e-mails with a shortcut file attached have been seen continually for some time, but the files that get downloaded by executing the shortcut file and the types of malware differ according to the timing of occurrence. The targeted attack e-mails seen from November 2015 to June 2016 contained a .lnk file attachment that infected the host with malware (downloader) when executed. This malware downloaded an image file, then decoded and executed it, resulting in infection with an HTTP bot called Asruex.

See the following for details on cases where the malware ChChes and PowerShell are used to spread infection.

ChChes – Malware that Communicates with C&C Servers Using Cookie Headers (2017-02-15)
http://blog.jpcert.or.jp/2017/02/chches-malware--93d6.html

Malware Leveraging PowerSploit (2017-03-01)
http://blog.jpcert.or.jp/2017/03/malware-leveraging-powersploit.html

3.4.Other Incident Trends

The number of malware sites reported in this quarter was 91. This was a 76% decrease from 376 in the previous quarter.

The number of scans reported in this quarter was 2,391. This was an 10% increase from 2,177 of the previous quarter.

The ports that the scans targeted are listed in [Chart 5].

Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and DNS (53/UDP).

[Chart 5: Number of scans by port]

Port	Jan	Feb	Mar	Total
22/tcp	469	272	520	1261
25/tcp	147	110	127	384
53/udp	53	124	85	262
80/tcp	69	58	43	170
23/tcp	58	34	17	109
2323/tcp	16	9	4	29
2222/tcp	11	6	4	21
5358/tcp	13	6	1	20
21/tcp	5	1	9	15
3389/tcp	9	4	1	14
7547/tcp	7	4	1	12
23231/tcp	7	1	0	8
5555/tcp	6	0	0	6
53413/udp	1	5	0	6
4752/udp	2	2	2	6
23887/udp	4	1	1	6
123/udp	6	0	0	6
51331/udp	3	1	1	5
33442/udp	4	1	0	5
443/tcp	1	3	0	4
5432/tcp	1	1	1	3
1433/tcp	1	2	0	3
Unknown	199	165	159	523
Monthly Total	1092	810	976	2878

There were 610 incidents categorized as other. This was a 135% increase from 260 in the previous quarter.

4. Incident Handling Case Examples

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

[Attacks exploiting a vulnerability of Apache Struts 2]
In March 2017, information about an Apache Struts 2 vulnerability (S2-045, CVE-2017-5638) was released, and a number of reports concerning attacks that appear to have exploited this vulnerability have subsequently been received. The proof-of-concept (PoC) exploit code was released the day after the vulnerability was announced, and according to reports from affected organizations, there is a possibility that accesses that appear to be attacks were already seen on the same day the code was released.
This means that it probably would not have been possible to prevent attacks unless countermeasures were taken immediately after the vulnerability information was released.

This attack gives the attacker the ability to execute any command with the authority of a user running server applications, and cases where the attacks resulted in files being placed or deleted were actually observed. JPCERT/CC analyzed logs provided by a number of reporters to identify the commands that the attackers tried to execute. Among those identified were a command to gather information such as user names and server OS versions, a command to download from an external source a JSP file that appears to be a backdoor, and a command to download and execute a virtual currency mining tool.

Although it has been reported that dynamic IP addresses managed by domestic ISPs were the attack sources, these could have been hosts used as springboards for the attacks.

[Coordination involving domestic IP addresses communicating with C&C servers in a botnet]
In December 2016, European law enforcement agencies dismantled a large-scale communications infrastructure called Avalanche, which had been used to manage various botnets as well as financial malware and information-stealing malware. Domains used by C&C servers that were hosted on Avalanche have now been rendered harmless, and they are currently used as sinkholes for verifying communication from computers infected with malware.

JPCERT/CC continues to receive lists of domestic IP addresses that communicate with the sinkholes from CERT-Bund, the National CSIRT of Germany. Avalanche served as a communication destination for financial Trojans and information-stealing malware, and according to the lists, about half of the hosts communicating with the sinkholes are infected with malware called Rovnix.
Rovnix, which targets the account information of Internet banking services in Japan, was also found in the attachment contained in e-mails spoofing Japan Post, which were observed around March 2016.
JPCERT/CC is notifying telecommunications carriers that manage the IP addresses concerned and sharing the lists with domestic partners.

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 2016 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/