JPCERT-IR-2018-03
Issued: 2018-07-12

JPCERT/CC Incident Handling Report
[April 1, 2018 - June 30, 2018]

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, 2018 through June 30, 2018.

[*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 (a new method is used to tally ICS-related incident reports starting in this quarter).

[Chart 1: Number of incident reports]

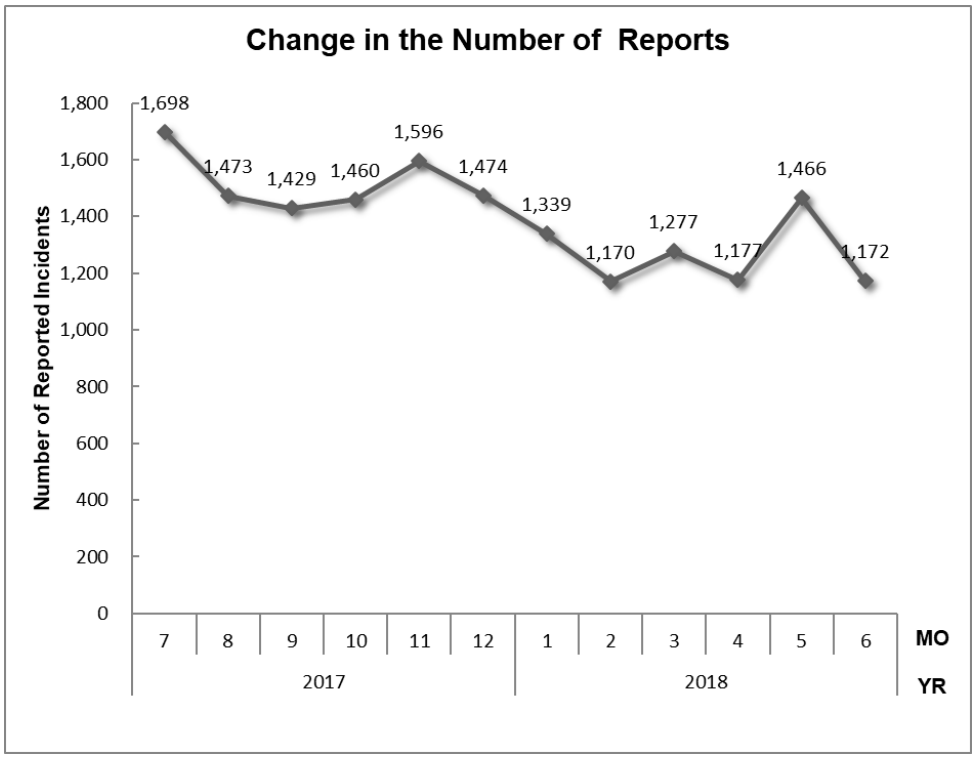
	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports *2	1,177	1,466	1,172	3,815	3,786
Number of Incident *3	1,131	1,425	1,039	3,595	3,857
Cases Coordinated *4	592	795	737	2,124	2,203

[*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.

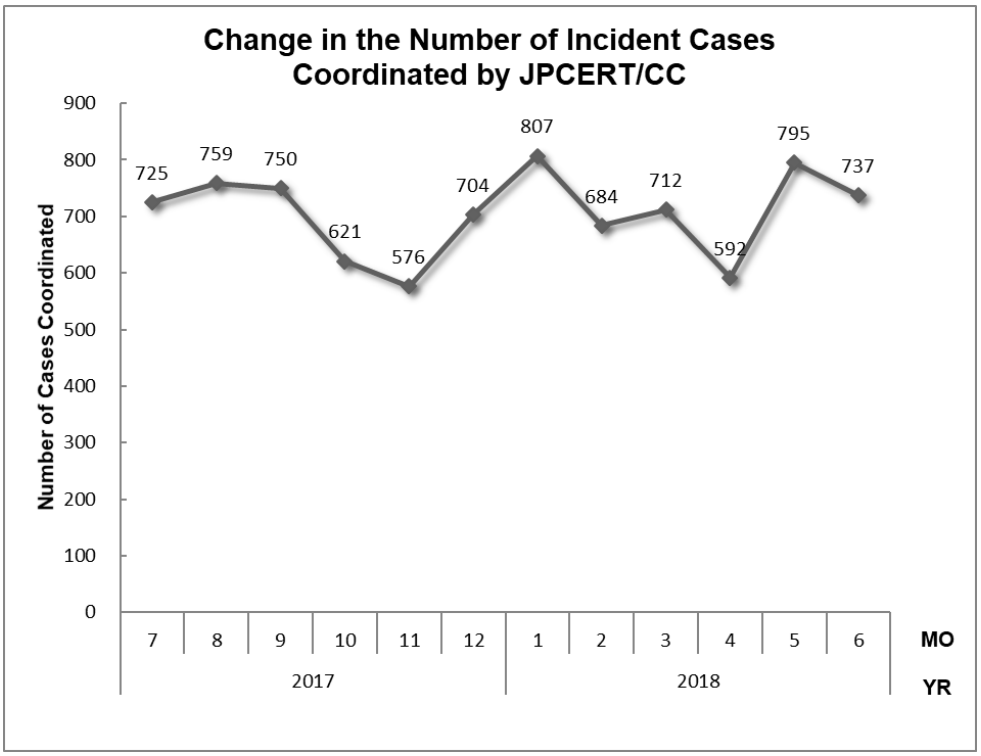
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 3,815. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,124. When compared with the previous quarter, the total number of reports increased by 1%, and the number of cases coordinated decreased by 4%. When compared with the same quarter of the previous year, the total number of reports decreased by 27%, and the number of cases coordinated decreased by 17%.

[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]



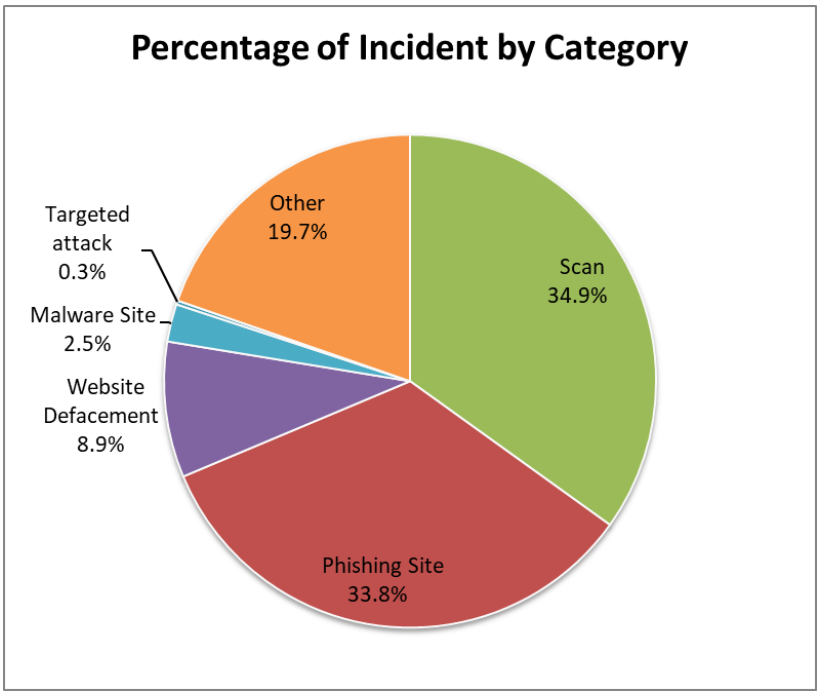
[Figure 2 Change in the number of incident cases coordinated]

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]

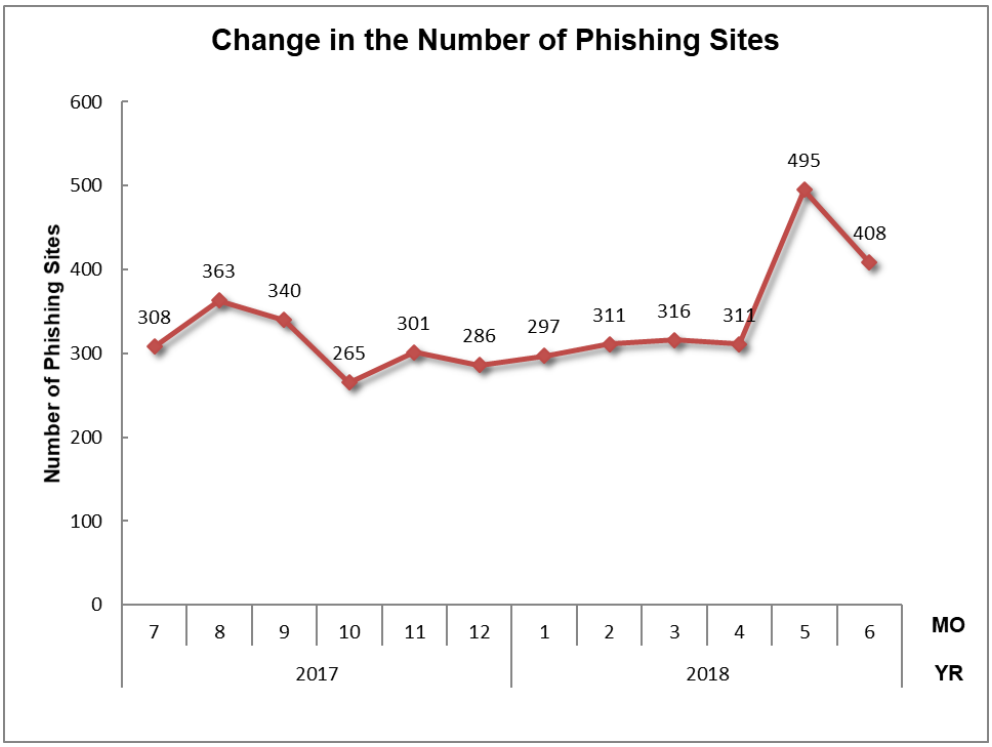
Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	311	495	408	1,214	924
Website Defacement	103	105	112	320	268
Malware Site	29	28	32	89	63
Scan	481	596	178	1,255	1,845
DoS/DDoS	0	0	0	0	1
ICS Related	0	0	0	0	7
Targeted attack	2	3	4	9	6
Other	205	198	305	708	743

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 34.9%, and incidents categorized as phishing sites made up 33.8%.

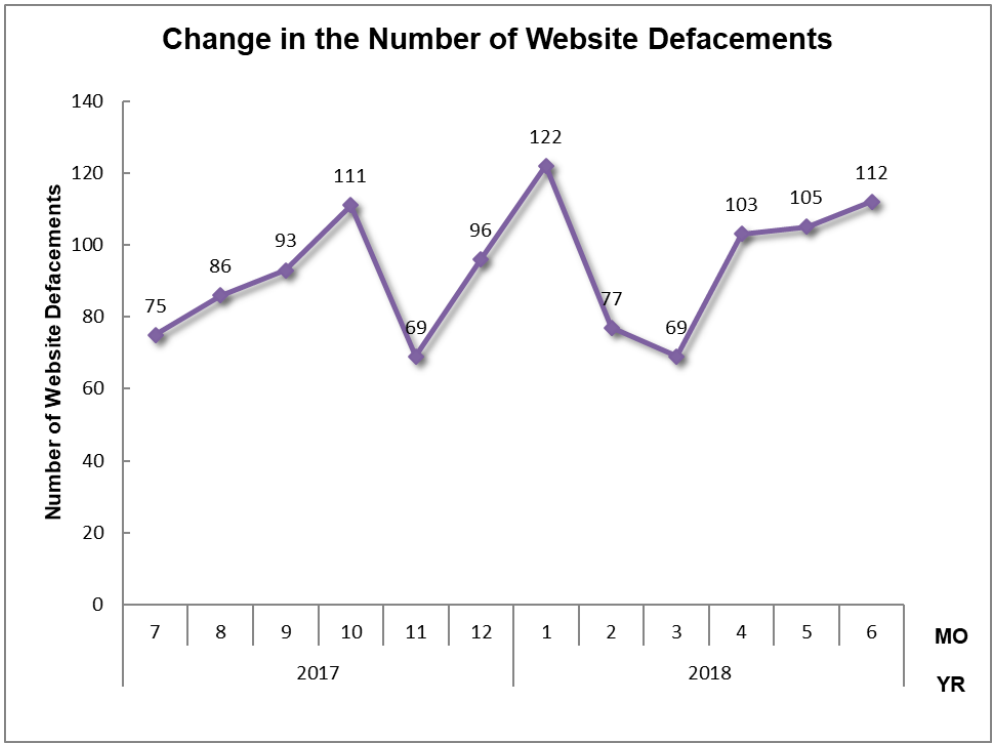


[Figure 3 Percentage of incidents by category]

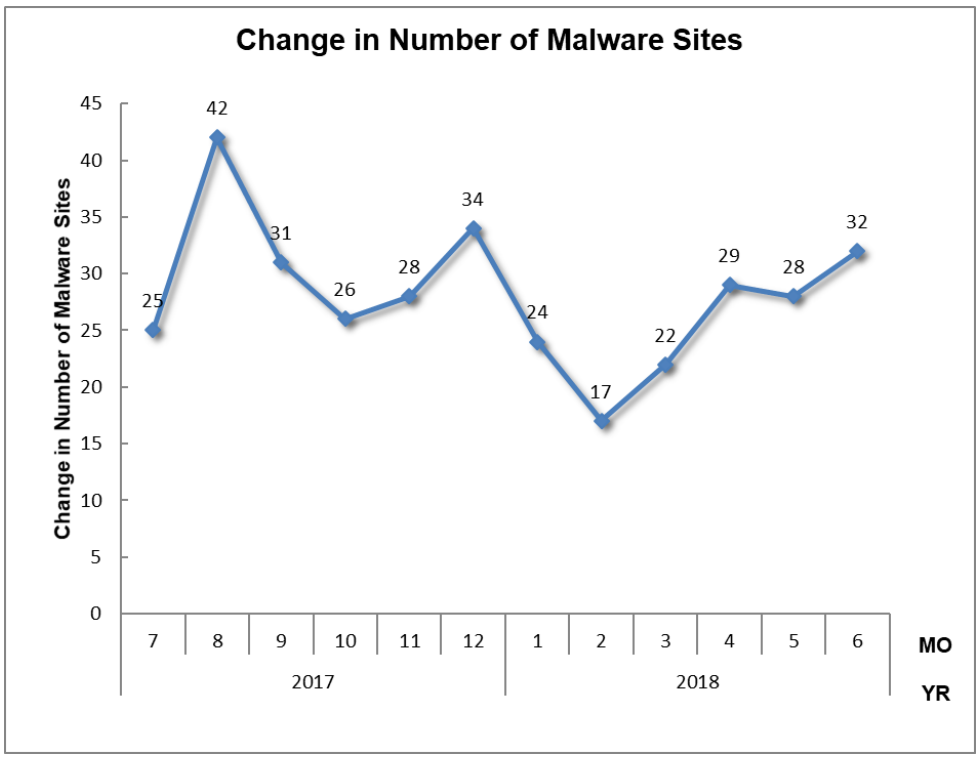
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



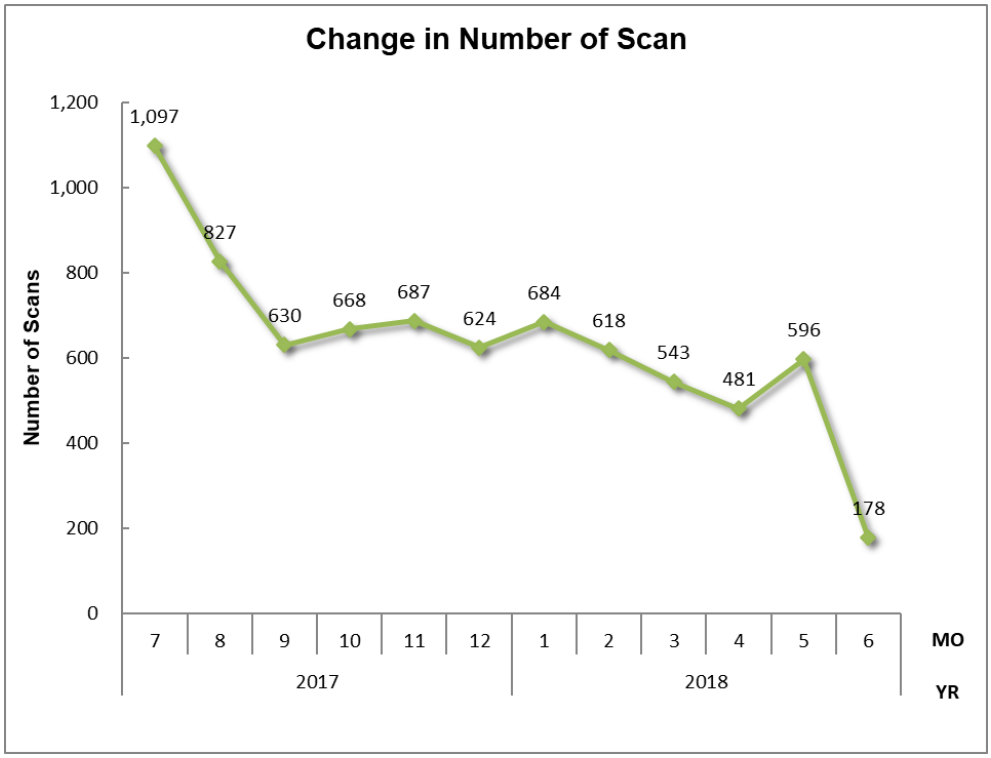
[Figure 4 Change in the number of phishing sites]



[Figure 5 Change in the number of website defacements]

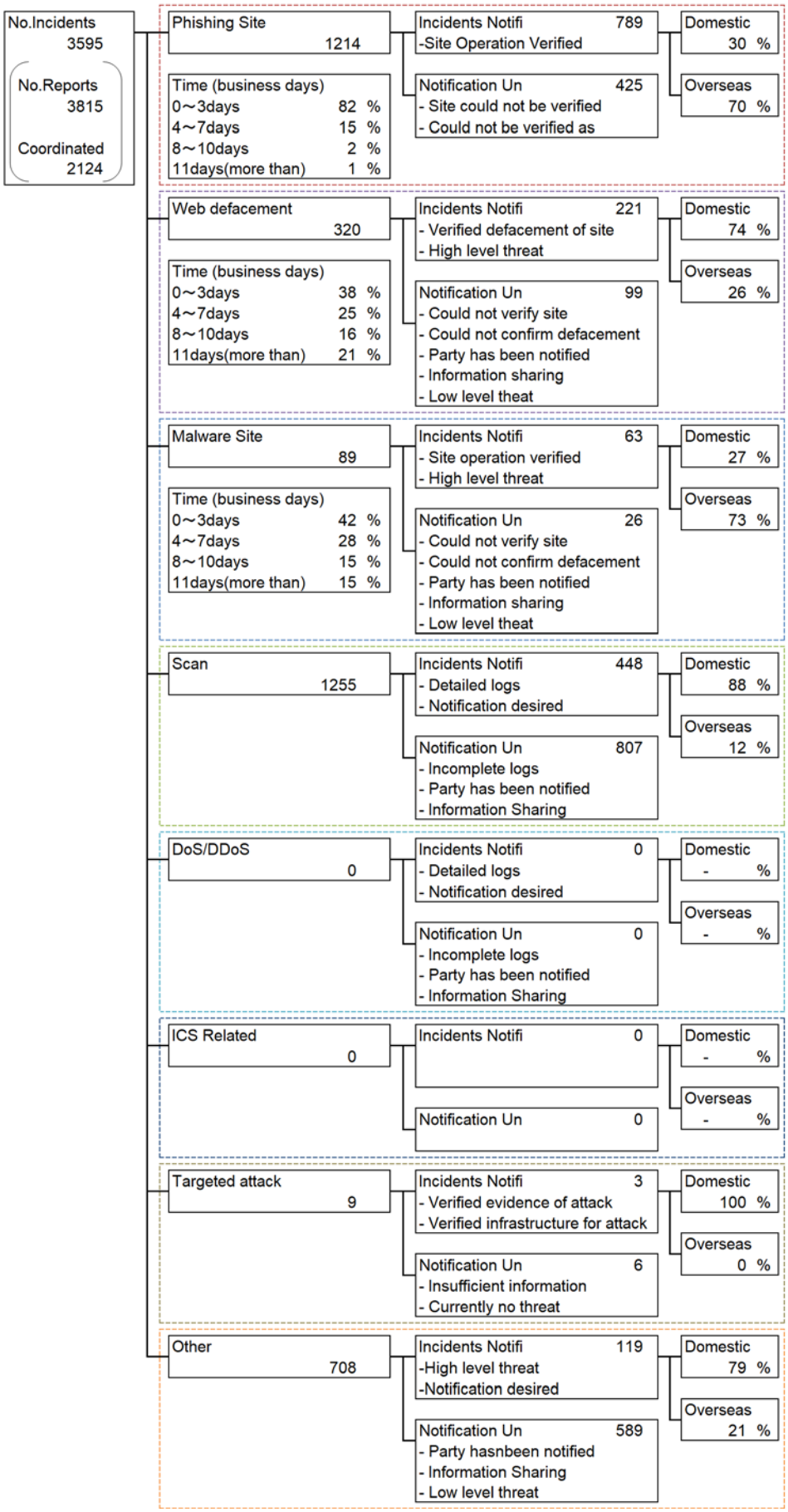


[Figure 6 Change in the number of malware sites]



[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 (the chart has been restructured for this quarter's report).



[Figure 8 Breakdown of incidents coordinated/handled]

3. Incident Trends

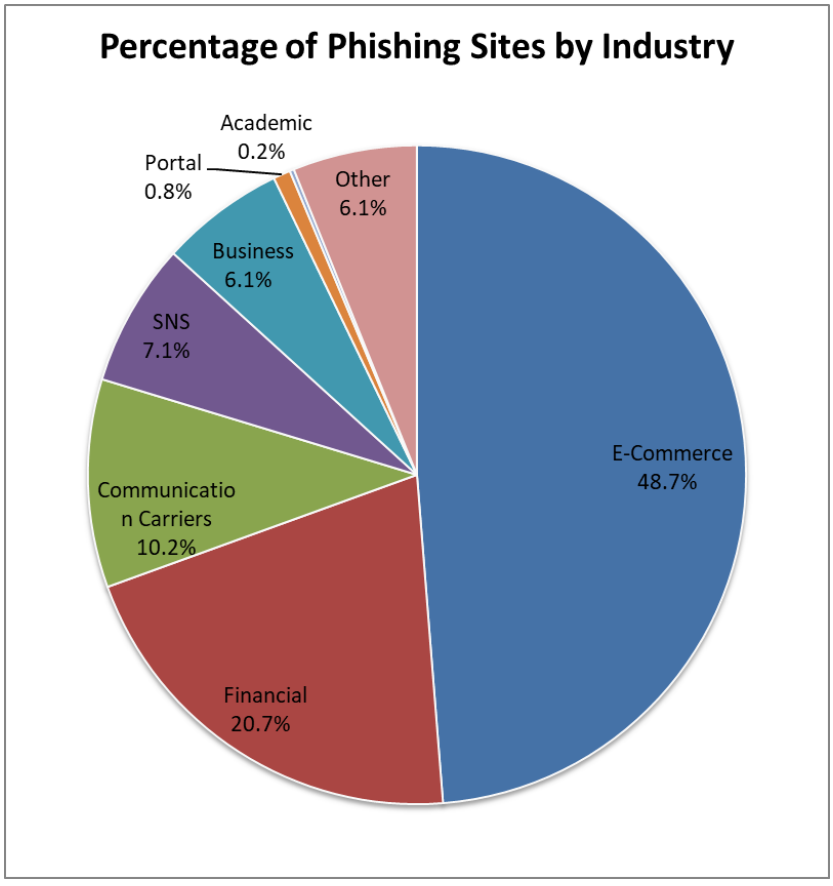
3.1. Phishing Site Trends

1,214 reports on phishing sites were received in this quarter, representing a 31% increase from 924 in the previous quarter. This marks a 65% increase from the same quarter last year (736). 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	67	85	76	228(19%)
Overseas Brand	166	298	258	722(59%)
Unknown Brand [*5]	78	112	74	264(22%)
Monthly Total	311	495	408	1,214(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 228 phishing sites that spoofed domestic brands, increasing 10% from 208 in the previous quarter. There were 722 phishing sites that spoofed overseas brands, increasing 28% from 564 in the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 48.7% spoofed e-commerce websites, 20.7% websites of financial institutions, and 10.2% websites of telecommunications carriers.

Continuing the trend seen in the previous quarter, there were considerable numbers of reports regarding phishing sites designed to steal account information of specific overseas brands, accounting for more than half of the phishing sites involving overseas brands reported during this quarter.

On phishing sites of domestic brands, there were many reports regarding phishing sites spoofing telecommunications carriers, social media and financial institutions, as in the previous quarter. As for phishing sites spoofing telecommunications carriers, JPCERT/CC has confirmed the existence of websites spoofing multiple brands of leading mobile carriers, and that the domains of these websites were all registered using the same e-mail address. Phishing sites spoofing social media used .cn domains, whereas those spoofing two different brands of financial institutions used .club, .top and .xyz domains.

Many of these phishing sites spoofing overseas and domestic brands used domain names resembling legitimate brand names; numerous versions of these domain names, with parts of the names replaced, were obtained from a specific registrar. Since this type of registration pattern clearly indicates that the domain names are obtained for phishing purposes, it is desired that registrars detect and decline such domain registration requests.

The parties that JPCERT/CC contacted for coordination of phishing sites were 30% domestic and 70% overseas, unchanged from the previous quarter.

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 320. This was a 19% increase from 268 in the previous quarter.

During this quarter, JPCERT/CC confirmed numerous cases in which users accessed a compromised website and were redirected to another website that tried to trick them into entering their credit card numbers by saying they won a gift, or one that displayed a fake message saying malware was detected. These cases of redirection were often made via a URL with a .tk domain. Although a number of different methods were identified for redirecting users, such as embedding JavaScript code at the top of a web page or obfuscated JavaScript code within a web page, common patterns were seen in the paths of the URLs to which users were redirected. JPCERT/CC also confirmed many cases in which users were

redirected to a fake survey site with a .loan domain, only when a compromised website was accessed for the first time from the search results of a search service.

3.3. Targeted Attack Trends

There were 9 incidents categorized as a targeted attack. This was a 50% increase from 6 in the previous quarter. JPCERT/CC asked 3 organizations to take action this quarter.

In early April 2018, JPCERT/CC received reports regarding suspicious e-mails with a ZIP file attachment containing a Word document. The Word document was embedded with a macro that creates and executes a VBS file. Executing the macro downloads malware and in the end installs remote desktop tool Ammyy Admin and malware that downloads files from the server it communicates with. The suspicious e-mails were possibly sent from hacked e-mail accounts via mail servers in Japan. The host portions of the URLs accessed by the VBS file and the malware that users get infected with in the end all pointed to a website, apparently hacked and misused, with a domestic IP address. Cases in which Ammyy Admin gets installed by opening a Word document attached to a suspicious e-mail were identified in April 2017 as well. File names of the Word document used for the recent attacks and the method of executing the VBS file created with a macro were the same as in the previous attacks.

In late May, JPCERT/CC received reports of e-mail spoofing that appeared to be a targeted attack. The ZIP file attached to the e-mails was password-protected, and a password for opening the file was provided in a separate e-mail. When the Word document contained in the ZIP file is opened, attack code designed to exploit a vulnerability in the Windows VBScript engine (CVE-2018-8174) gets downloaded to execute malware. CVE-2018-8174 was fixed in Microsoft's security update in May 2018, meaning that the vulnerability was exploited to carry out the attacks shortly after it was announced. The malware that is executed in the final stage of attack was a bot that operates based on commands received from a C&C server via HTTP.

With the aim of preventing the spread of infection and determining the scope of attack, JPCERT/CC shares information identified through analysis of malware provided by the reporting party, such as the URL of the server the malware communicates with, with permission from the relevant party.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 89. This was a 41% increase from 63 in the previous quarter.

The number of scans reported in this quarter was 1,255. This was a 32% decrease from 1,845 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 4: Number of scans by port]

Port	Apr	May	Jun	Total
22/tcp	244	256	63	563
25/tcp	88	142	2	232
80/tcp	22	77	52	151
23/tcp	51	16	14	81
21/tcp	1	42	0	43
443/tcp	0	3	29	32
2323/tcp	9	6	6	21
81/tcp	5	6	8	19
8080/tcp	8	5	3	16
7001/tcp	13	2	0	15
445/tcp	8	5	2	15
5555/tcp	3	4	6	13
3389/tcp	5	4	4	13
82/tcp	4	4	3	11
8000/tcp	0	3	8	11
8888/tcp	0	5	3	8
85/tcp	0	5	3	8
84/tcp	0	5	3	8
8081/tcp	0	3	5	8
53/udp	7	0	1	8
6379/tcp	2	3	1	6
9000/tcp	1	3	1	5
Unknown	787	730	22	1,539
Monthly Total	1,258	1,329	239	2,826

There were 708 incidents categorized as other. This was a 5% decrease from 743 in the previous quarter.

4. Incident Handling Case Examples

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

Coordination for vulnerability in Cisco Smart Install Client

At the end of March 2018, information about a vulnerability in Cisco Smart Install Client (CVE-2018-0171) was published, and a security company made the proof-of-concept exploit code publicly available. Immediately after the vulnerability information and the PoC code were published, JPCERT/CC's Internet threat monitoring system (TSUBAME) detected an increase in the number of scans targeting the port used by Cisco Smart Install Client (4786/TCP).

In mid-April, a number of domestic sources provided information about attacks exploiting the vulnerability in Cisco Smart Install Client. Organizations that were attacked reported damages such as network devices getting restarted and settings being changed. Since there was a possibility that attacks were being carried out on a large scale, JPCERT/CC contacted organizations that manage the IP addresses concerned based on information provided by overseas security organizations about domestic IP addresses whose port 4786/TCP was accessible from the Internet, and asked them to check the settings of network devices.

Coordination for hijacking of network device DNS settings and related malware

In mid-March 2018, JPCERT/CC learned from published information that DNS settings of routers were being hijacked, and when devices connected to the compromised routers accessed particular websites, a suspicious APK file got downloaded.

In mid-April, it was found that a DNS server with an IP address in Japan was set in a similar case of hijacking. JPCERT/CC confirmed that when this DNS server was set and a particular website was accessed, an APK file got downloaded. JPCERT/CC analyzed the APK file and found that it resembled the APK file identified in March, but it also found that the file came with a new function for sending e-mail to a specific e-mail address. The subject line of the e-mail that is sent contains the phrase "connection error" written in simplified Chinese and the language setting of the device, and its body contains phone numbers, execution results of the ping command and other data, presumably intended to provide the attackers with information about the infected device. JPCERT/CC contacted the hosting operator that manages the IP address of the rogue DNS server, and later received a reply saying the server had been shut down.

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 2018 Fiscal Year".