JPCERT/CC Incident Handling Report

April 1, 2023 ～ June 30, 2023

JPCERT Coordination Center

July 13, 2023

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, 2023 through June 30, 2023.

[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 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]

	April	May	June	Total	Last Qtr. Total
Number of Reports [2]	3,449	6,623	16,836	26,908	11,720
Number of Incident [3]	2,416	2,867	2,642	7,925	8,459
Cases Coordinated [4]	1,500	1,553	1,551	4,604	4,326

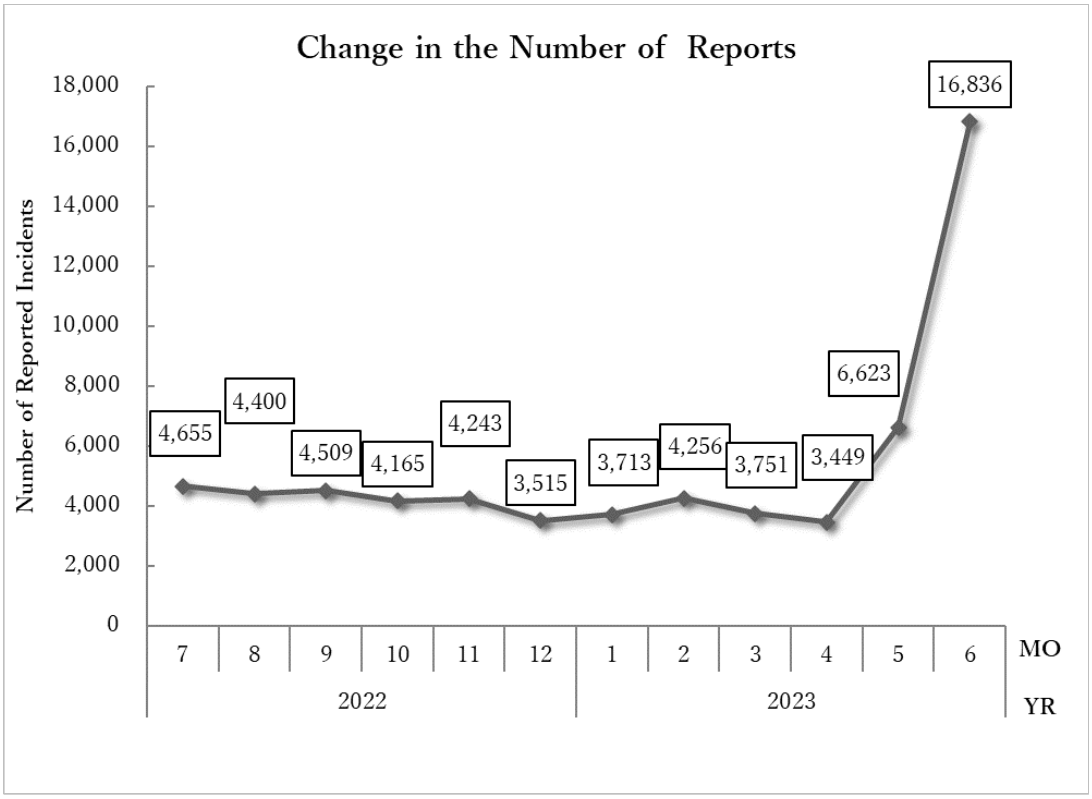
[2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

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

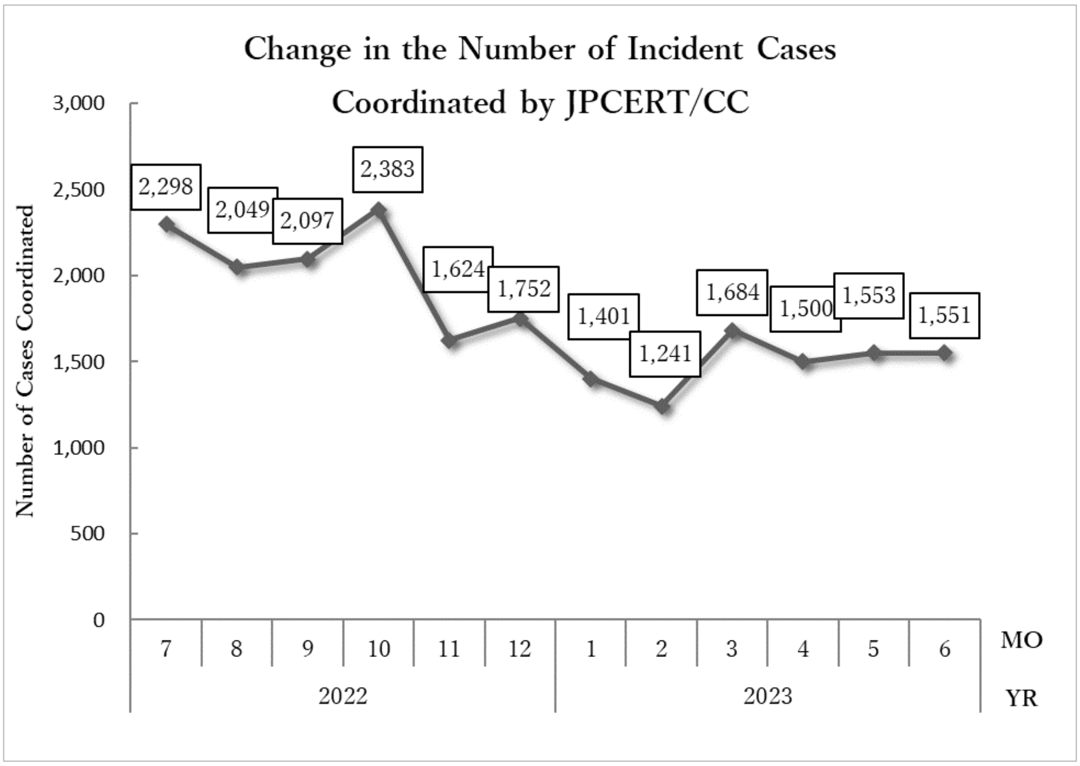
[4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 26,908. Of these, the number of cases that JPCERT/CC coordinated was 4,604. When compared with the previous quarter, the total number of reports increased by 130%, and the number of cases coordinated increased by 6%. Year on year, the number of reports increased by 61%, and the number of cases coordinated decreased by 42%.

[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]

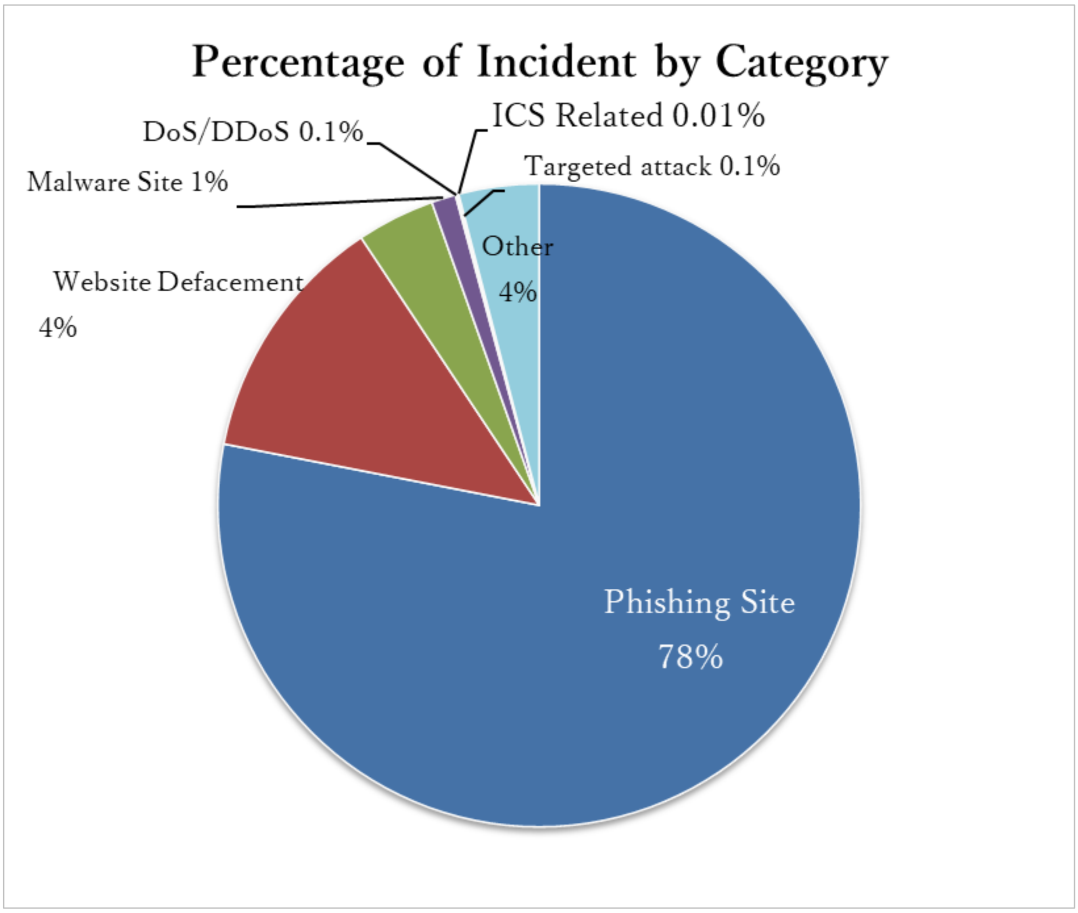


[Figure 2: Change in the number of incident cases coordinated]

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]

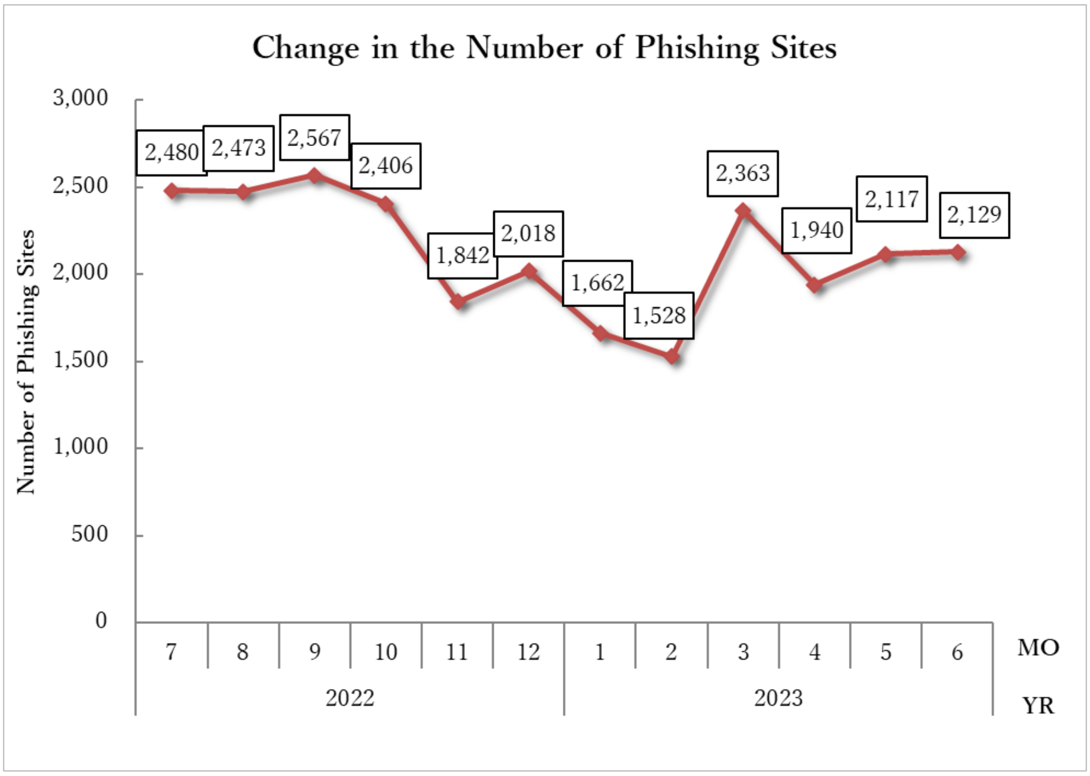
Incident Category	April	May	June	Total	Last Qrt. Total
Phishing Site	1,940	2,117	2,129	6,186	5,553
Website Defacement	104	165	42	311	362
Malware Site	39	38	20	97	154
Scan	251	418	329	998	2,059
DoS/DDoS	0	7	1	8	9
ICS Related	0	0	1	1	0
Targeted attack	1	1	2	4	3
Other	81	121	118	320	319



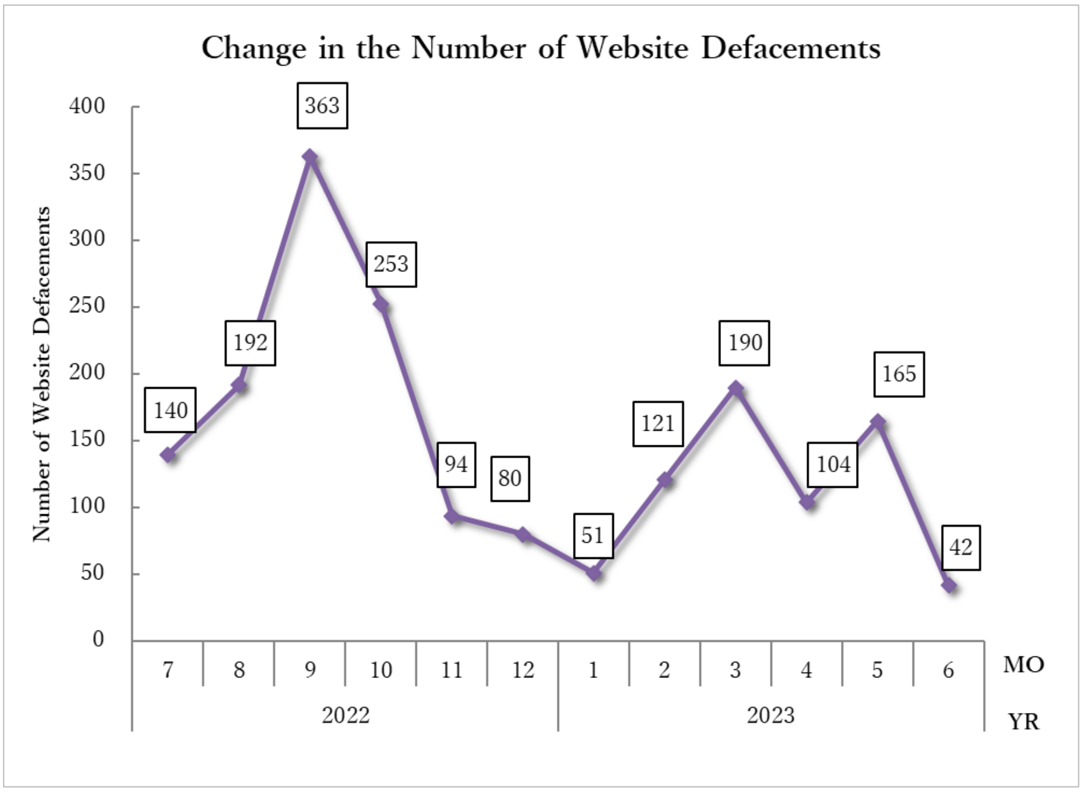
[Figure 3：Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 78%, and those categorized as scans, which search for vulnerabilities in systems, made up 13%.

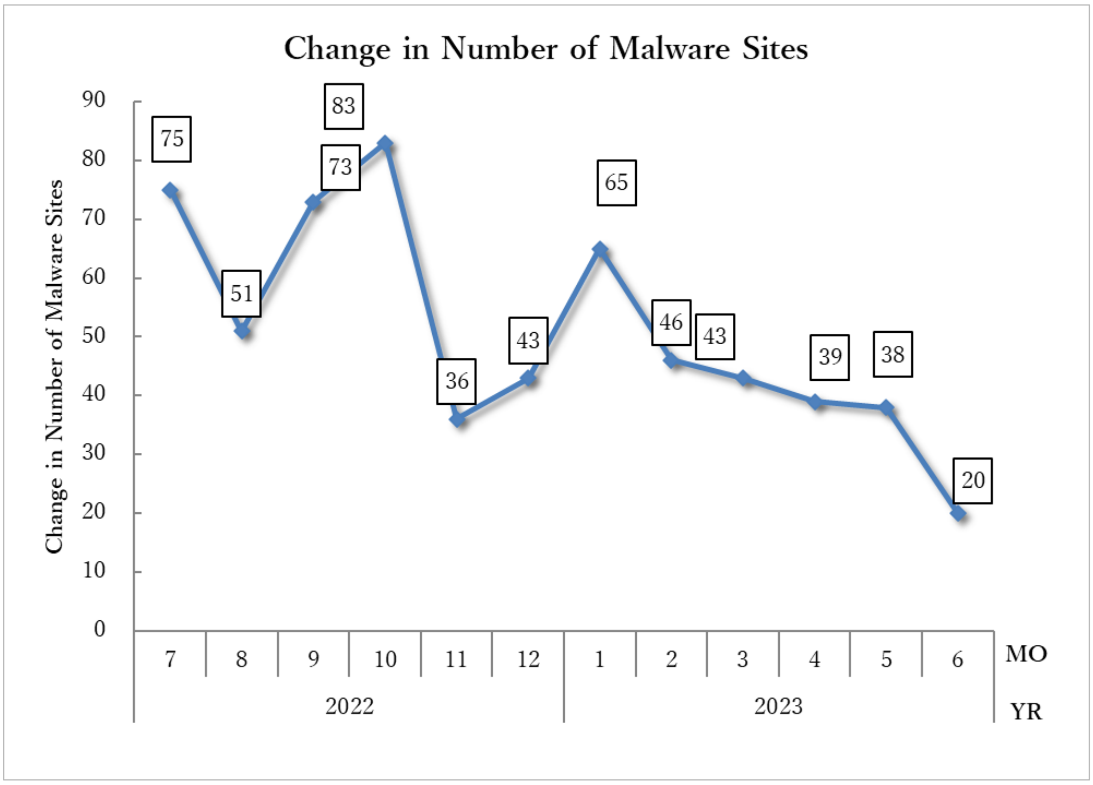
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



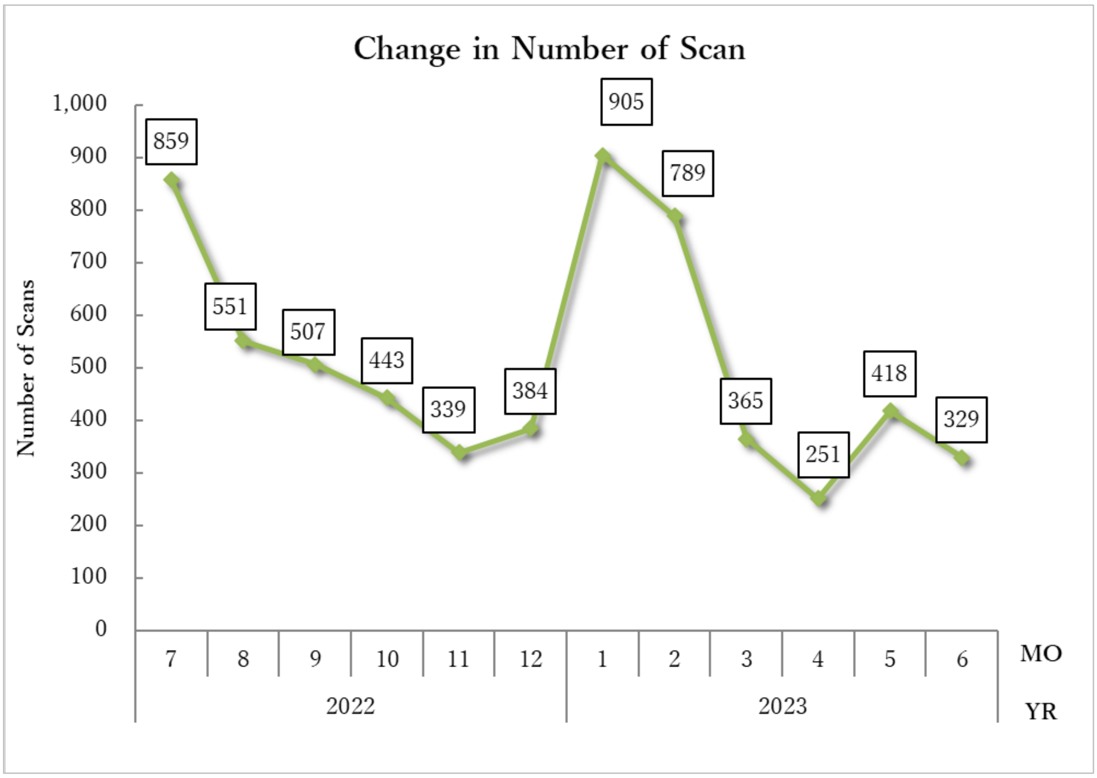
[Figure 4：Change in the number of phishing sites]



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

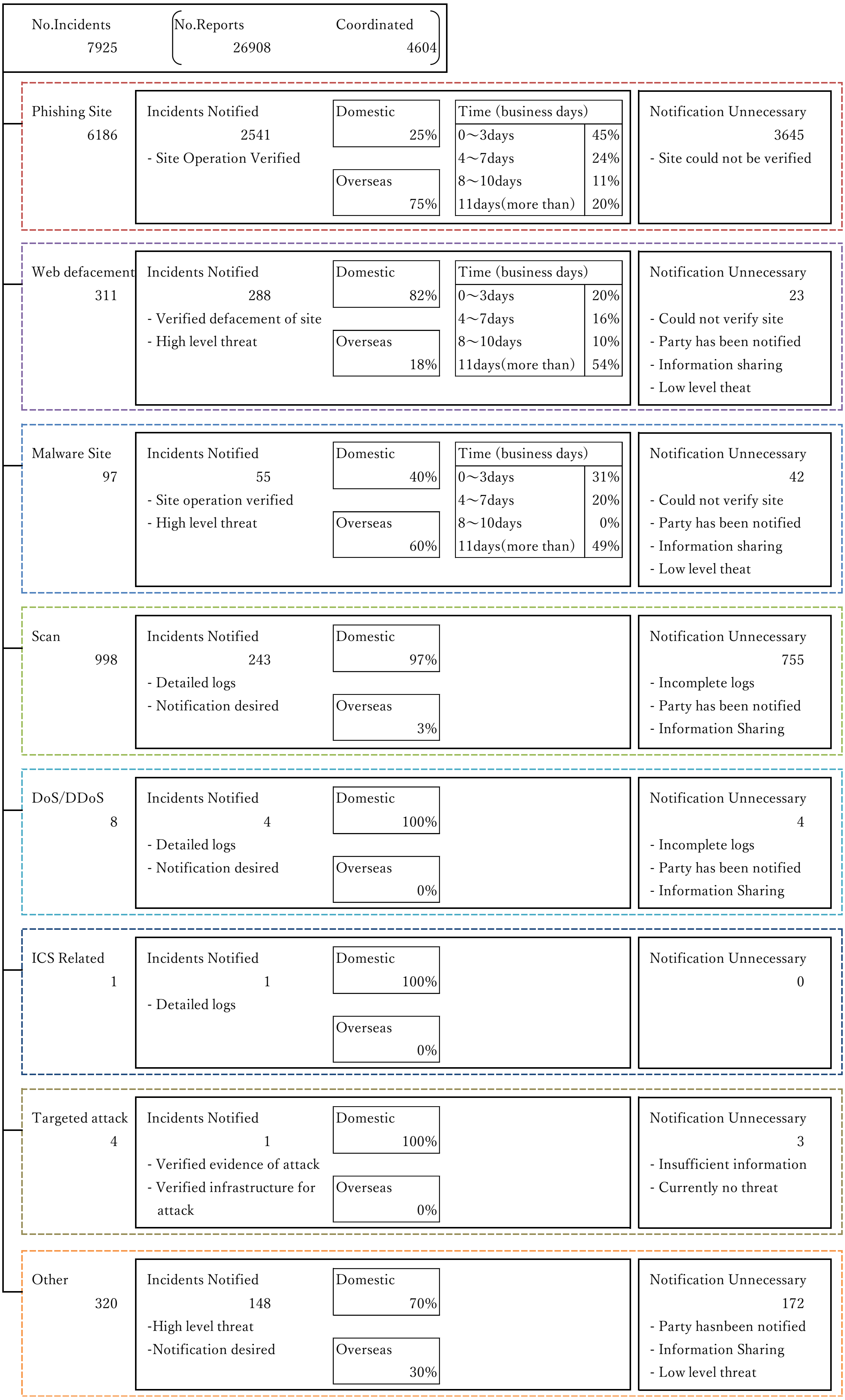


[Figure 6：Change in the number of malware sites]



[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	No.Reports	Coordinated
7925	26908	4604

Phishing Site 6186	Incidents Notified 2541 - Site Operation Verified	Domestic 25% Overseas 75%	Time (business days) 0～3days 45% 4～7days 24% 8～10days 11% 11days(more than) 20%	Notification Unnecessary 3645 - Site could not be verified
Web defacement 311	Incidents Notified 288 - Verified defacement of site - High level threat	Domestic 82% Overseas 18%	Time (business days) 0～3days 20% 4～7days 16% 8～10days 10% 11days(more than) 54%	Notification Unnecessary 23 - Could not verify site - Party has been notified - Information sharing - Low level theat
Malware Site 97	Incidents Notified 55 - Site operation verified - High level threat	Domestic 40% Overseas 60%	Time (business days) 0～3days 31% 4～7days 20% 8～10days 0% 11days(more than) 49%	Notification Unnecessary 42 - Could not verify site - Party has been notified - Information sharing - Low level theat
Scan 998	Incidents Notified 243 - Detailed logs - Notification desired	Domestic 97% Overseas 3%		Notification Unnecessary 755 - Incomplete logs - Party has been notified - Information Sharing
DoS/DDoS 8	Incidents Notified 4 - Detailed logs - Notification desired	Domestic 100% Overseas 0%		Notification Unnecessary 4 - Incomplete logs - Party has been notified - Information Sharing
ICS Related 1	Incidents Notified 1 - Detailed logs	Domestic 100% Overseas 0%		Notification Unnecessary 0
Targeted attack 4	Incidents Notified 1 - Verified evidence of attack - Verified infrastructure for attack	Domestic 100% Overseas 0%		Notification Unnecessary 3 - Insufficient information - Currently no threat
Other 320	Incidents Notified 148 -High level threat -Notification desired	Domestic 70% Overseas 30%		Notification Unnecessary 172 - Party hasbneen notified - Information Sharing - Low level threat

[Figure 8：Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

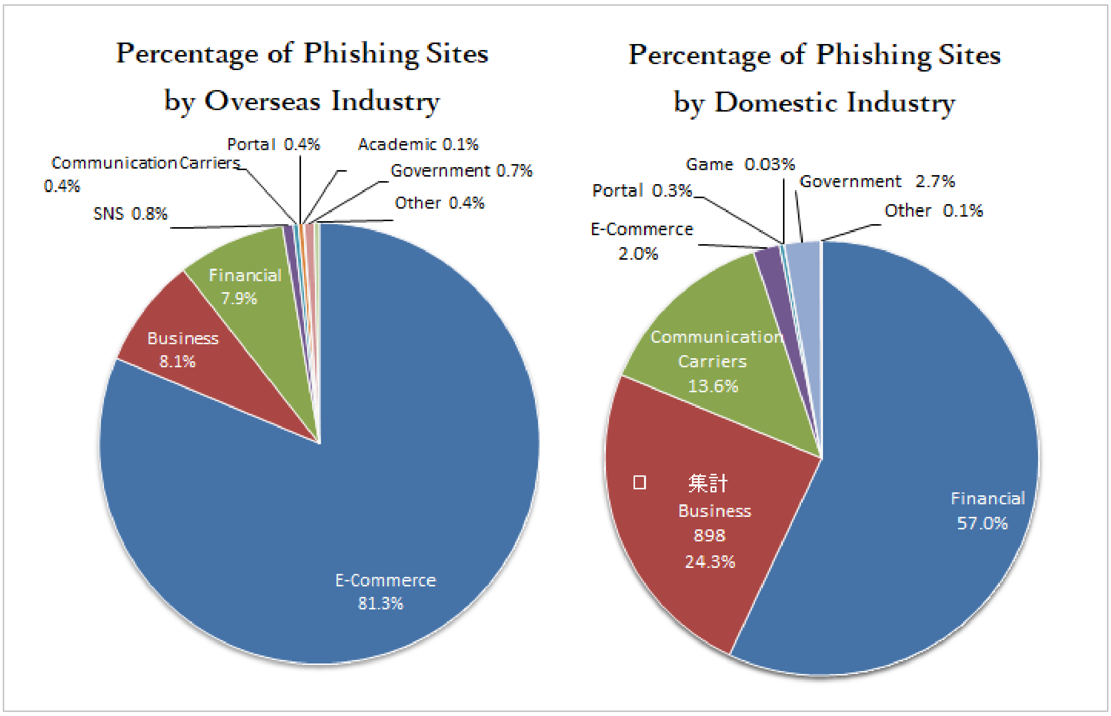
During this quarter, 6,186 reports on phishing sites were received, representing an 11% increase from 5,553 in the previous quarter. This marks a 24% decrease from the same quarter last year (8,088).

During this quarter, there were 3,700 phishing sites that spoofed domestic brands, decreasing 17% from 3,170 in the previous quarter. There were 1,568 phishing sites that spoofed overseas brands, decreasing 9% from 1,730 in the previous quarter. The numbers of brands that the phishing sites spoofed in this quarter are shown by brand type (domestic, overseas) in [Chart 3], and the percentages by industry for domestic and overseas brands are shown in [Figure 9].

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

Phishing Site	April	May	June	Domestic/Overseas Total (%)
Domestic Brand	1,127	1,351	1,222	3,700(60%)
Overseas Brand	587	482	499	1,568(25%)
Unknown Brand (*5)	226	284	408	918(15%)
Monthly Total	1,940	2,117	2,129	6,186

(*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, 81.3% spoofed e-commerce websites for overseas brands, and 57% spoofed financial websites for domestic brands, both representing the largest share respectively.

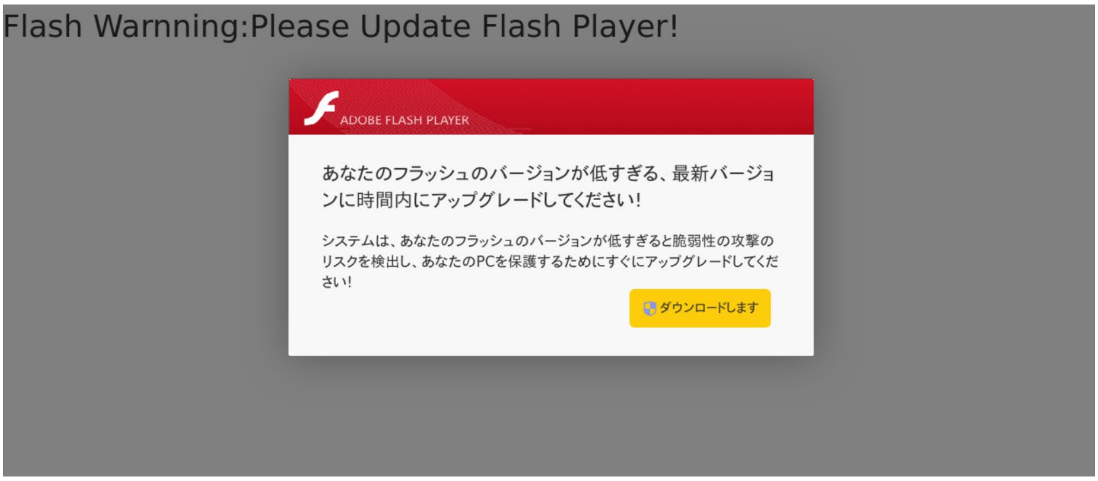
For overseas brands, phishing sites spoofing Amazon accounted for more than half of the phishing sites reported.
For domestic brands, phishing sites spoofing East Japan Railway Company's Eki-Net website and Electronic Toll Collection (ETC) system usage inquiry services were reported in large numbers.
Among domestic financial institutions, phishing sites spoofing EPOS Card, Saison Card, Aeon Card, and Sumitomo Mitsui Card 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 25% domestic and 75% overseas for this quarter, which are roughly the same as the previous quarter (domestic: 24%, overseas: 76%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 311. This was a 14% decrease from 362 in the previous quarter.

During this quarter, JPCERT/CC received reports of a website defacement that attempts to cause malware infection by displaying a fake Adobe Flash Player upgrade message as shown in [Figure 10] when browsing a website. When the user downloads a file by following the instructions on the fake upgrade screen and installs it, an attack tool called Cobalt Strike gets installed on the host.



Flash Warnning:Please Update Flash Player!

あなたのフラッシュのバージョンが低すぎる、最新バージョンに時間内にアップグレードしてください!

システムは、あなたのフラッシュのバージョンが低すぎると脆弱性の攻撃のリスクを検出し、あなたのPCを保護するためにすぐにアップグレードしてください!

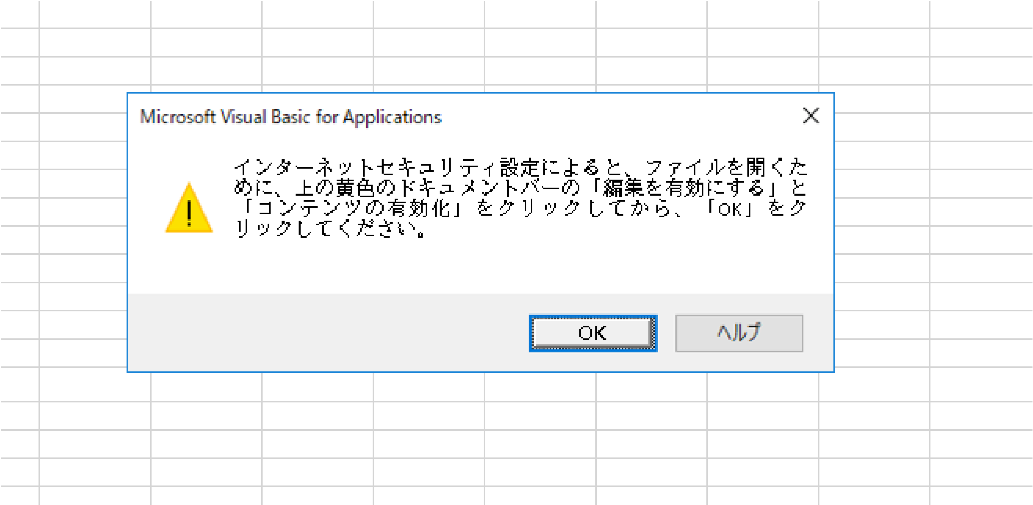
[Figure 10：Screen displayed when accessing the defaced website]

3.3. Targeted Attack Trends

There were 4 incidents categorized as a targeted attack. The incidents identified are described below.

(1) Attacks using LODEINFO malware

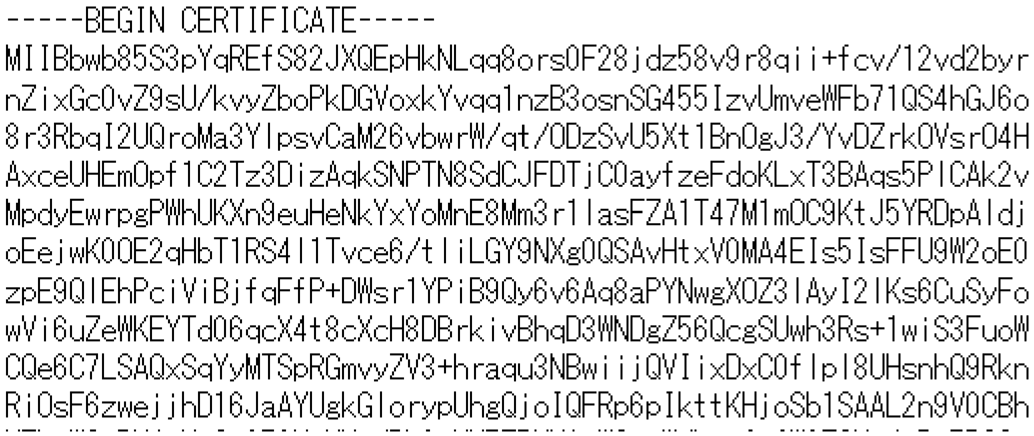
This quarter, JPCERT/CC received reports of targeted attacks attempting to cause infection with the LODEINFO malware. In this attack, the target receives an e-mail message from an attacker impersonating someone they communicated with in the past by e-mail, then after exchanging a few e-mails, receives a malicious Excel file. The malicious Excel file contains a message that urges the target to run a macro as shown in [Figure 11]. When the macro is run, LODEINFO ([Figure 12]) disguised as a PEM file is downloaded and executed.



Microsoft Visual Basic for Applications

インターネットセキュリティ設定によると、ファイルを開くために、上の黄色のドキュメントバーの「編集を有効にする」と「コンテンツの有効化」をクリックしてから、「OK」をクリックしてください。

[Figure 11：Excel file urging the target to run a macro]



```
-----BEGIN CERTIFICATE-----
MIIBbwb85S3pYqREfS82JXQEpHkNLqq8orsOF28jdz58v9r8qii+fcv/12vd2byr
nZixGc0vZ9sU/kvyZboPkDGVoxkYvqq1nzB3osnSG455IzvUmveWFb71QS4hGJ6o
8r3RbqI2UQroMa3YlpsvCaM26vbwrW/qt/ODzSvU5Xt1BnOgJ3/YvDZrkOVsr04H
AxceUHEmOpf1C2Tz3DizAqkSNPTN8SdCJFDTjC0ayfzeFdoKLxT3BAqs5PlCAk2v
MpdyEwrpgPWhUKXn9euHeNkYxYoMnE8Mm3r1lasFZA1T47M1mOC9KtJ5YRDpAldj
oEejwKOOE2qHbT1RS4l1Tvce6/tliLGY9NXg0QSAvHtxV0MA4EIs5IsFFU9W2oE0
zpE9QlEhPciViBjfqFfP+DWsr1YPiB9Qy6v6Aq8aPYNwgXOZ3lAyI2lKs6CuSyFo
wVi6uZeWKEYTd06qcX4t8cXcH8DBrkivBhqD3WNDgZ56QcgSUwh3Rs+1wiS3FuoW
CQe6C7LSAQxSqYyMTSpRGmvyZV3+hraqu3NBwiijQVIixDxC0flpl8UHsnhQ9Rkn
RiOsF6zwejjhD16JaAYUgkGlorypUhgQjoIQFRp6pIkttKHjoSb1SAAL2n9V0CBh
```

[Figure 12：Encrypted LODEINFO disguised as a PEM file]

Currently, LODEINFO v0.6.8 and v0.6.9 have been identified, indicating that development of the malware is still ongoing.

(2) Attacks targeting cryptocurrency exchanges apparently related to the DangerousPassword campaign

This quarter, JPCERT/CC observed attacks on cryptocurrency exchanges seemingly related to the DangerousPassword (also known as CryptoMimic or SnatchCrypto) attack campaign.

JPCERT/CC has identified a malicious Python script that downloads a Windows installer (MSI file) from an external source and executes it on a host of the target organization. It appears that the attacker has somehow run the Python script on the target host. The MSI file downloaded is of the same type that was previously discussed on the JPCERT/CC's blog, and it is capable of sending information about the infected host to an external destination. It is known that DangerousPassword uses various attack methods other than the typical method that uses a shortcut file in an attempt to cause malware infection, indicating the attack campaign is still actively underway.

JPCERT/CC Eyes：Attack Trends Related to DangerousPassword
https://blogs.jpcert.or.jp/en/2023/05/dangerouspassword.html

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 97. This was a 37% decrease from 154 in the previous quarter.

The number of scans reported in this quarter was 998. This was a 52% decrease from 2,059 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), SIP (5060/UDP), Telnet (23/TCP), 37215/TCP and HTTP (80/TCP).

[Chart 4：Top 10 ports by number of scans]

Port	April	May	June	Total
22/tcp	139	179	106	424
5060/udp	0	144	119	263
23/tcp	33	31	42	106
37215/tcp	34	33	11	78
80/tcp	24	12	10	46
25/tcp	11	6	8	25
52869/tcp	1	2	21	24
21/tcp	2	5	2	9
143/tcp	4	2	1	7
445/tcp	1	2	2	5
Monthly totals *	255	423	329	1007

*Monthly totals include those not in top 10.

There were 320 incidents categorized as other. This number was roughly unchanged from 319 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 DDoS attacks using recursive DNS queries

This quarter, JPCERT/CC received reports of DDoS attacks in which a large number of queries requesting FQDNs that contain a nonexistent subdomain were sent to an authoritative DNS server (hereafter "DNS water torture attack"). It was also reported that IP addresses in Japan were exploited in these attacks. JPCERT/CC contacted operators managing the relevant IP addresses and requested them to check the situation and implement countermeasures.

When a DNS water torture attack occurs, the target website and services using name resolution may become unavailable. Moreover, if the authoritative DNS server manages multiple domain names, domain names other than those targeted for attack may be affected as well. Service providers are advised to check their readiness against these attacks (whether appropriate steps are taken, including monitoring of attacks, countermeasures, and preparation of a workaround in the event of an attack) on authoritative DNS servers managing their domain names.

JPRS Topics & Column No. 021
Wide and Shallow Attacks on DNS Servers via Bots—Overview of DNS Water Torture Attack and Countermeasures（Japanese only）
https://jprs.jp/related-info/guide/topics-column/no21.html

Also, if cache DNS servers and routers (which forward traffic to cache DNS servers provided by ISPs, etc.) are configured to accept and respond to requests via the Internet without restriction (in other words, if they are open resolvers), they may be exploited as a springboard for attacks. Therefore, service providers are advised to check their systems to make sure they are not open resolvers, and to make sure they have appropriate countermeasures in place to prevent resolvers from being left open.

Open resolver verification site（Japanese only）
https://www.openresolver.jp/

(2) Coordination involving reports of damage from human-operated ransomware attacks

This quarter, JPCERT/CC received a number of reports of infection to ransomware (e.g., BlackByte, LockBit, BlackCat, Akira). JPCERT/CC has interviewed the victims to obtain information on the scope of damage, status of investigation and status of response at the time of report, then informed them on the characteristics of the relevant ransomware attack and provided advice on how to respond.

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.

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