JPCERT-IR-2015-05
Issued: 2016-01-14

JPCERT/CC Incident Handling Report
[October 1, 2015 – December 31, 2015]

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 October 1, 2015 through December 31, 2015.

[*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]

	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports (*2)	1061	1201	1178	3440	4128
Number of Incidents (*3)	1029	1137	1003	3169	3748
Cases Coordinated(*4)	626	684	743	2053	2058

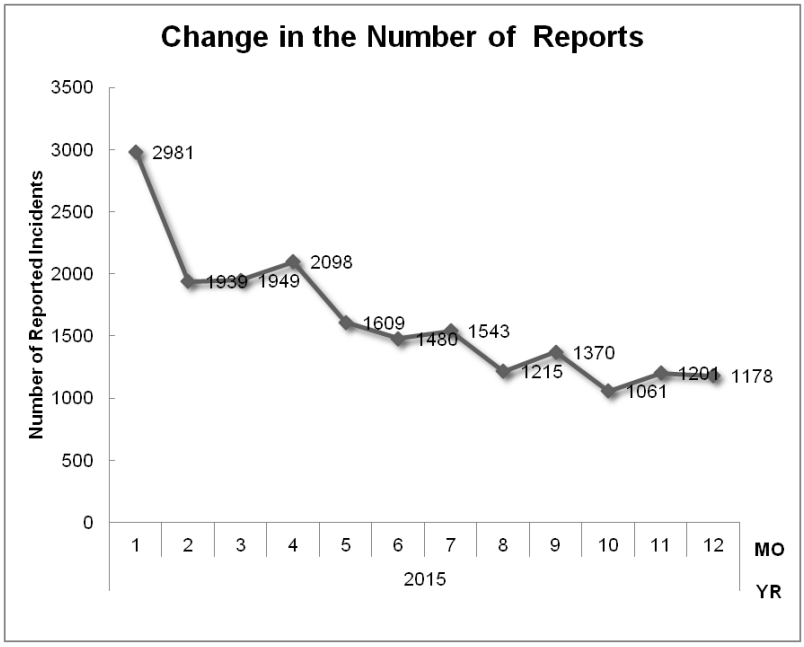
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

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

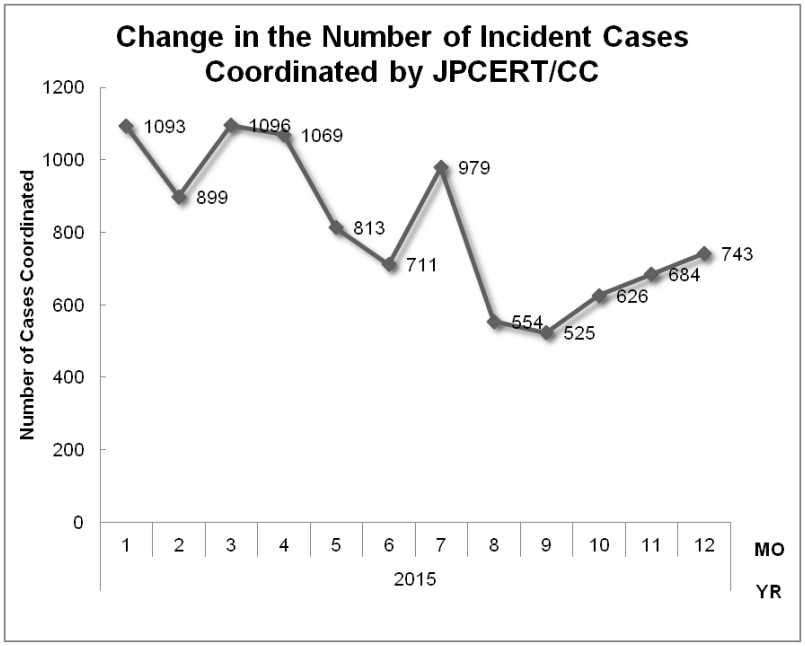
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 3,440. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,053. When compared with the previous quarter, the total number of reports decreased by 17%, and the number of cases coordinated decreased by 0.3%. When compared with the same quarter of the previous year, the total number of reports decreased by 45%, and the number of cases coordinated decreased by 12%.

[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 Reports]



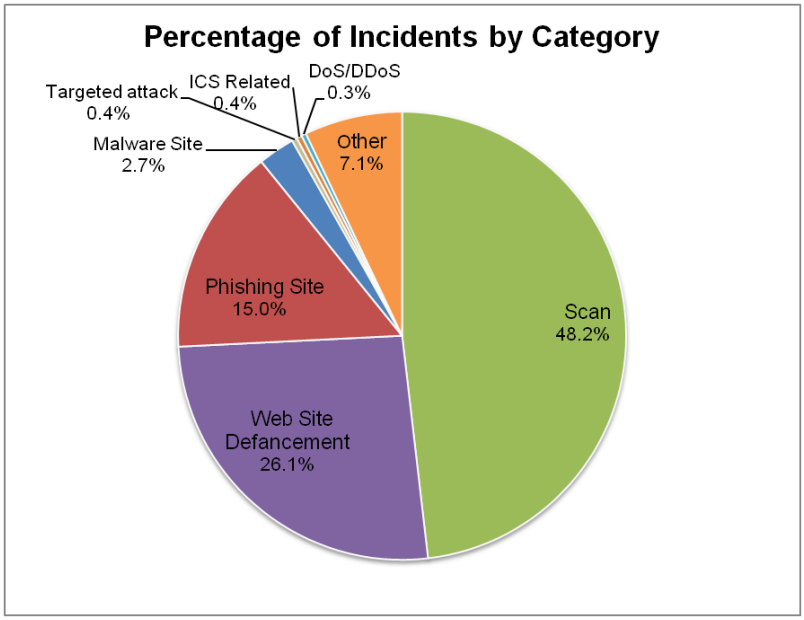
[Figure 2 Change in the Number of Incident Cases Coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on 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 per Category]

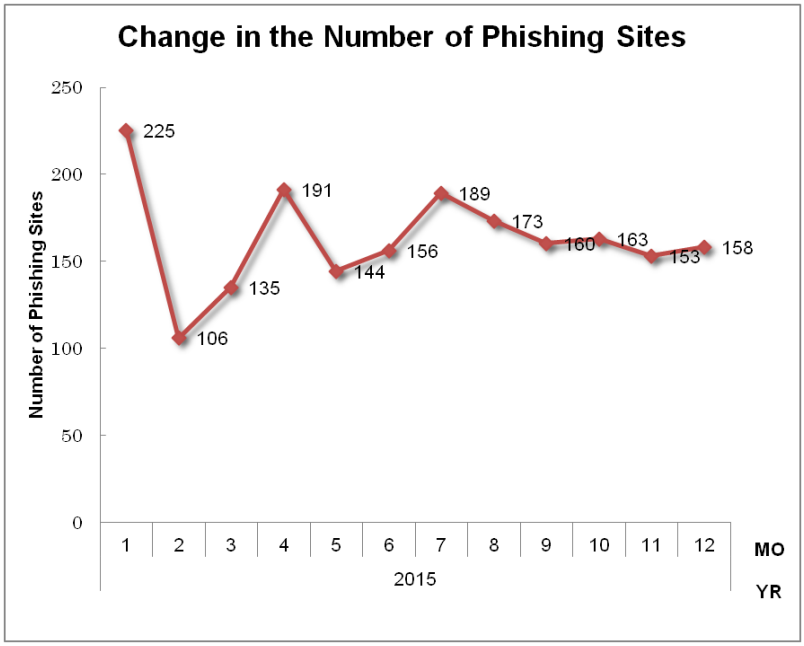
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	163	153	158	474	522
Website Defacement	273	292	261	826	592
Malware Site	25	32	27	84	119
Scan	509	580	437	1526	1985
DoS/DDoS	5	3	3	11	21
ICS Related	0	4	8	12	0
Targeted Attack	4	4	4	12	59
Other	50	69	105	224	450

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 48.2%, and incidents categorized as website defacement made up 26.1%. Also, incidents categorized as phishing sites represented 15.0% of the total.

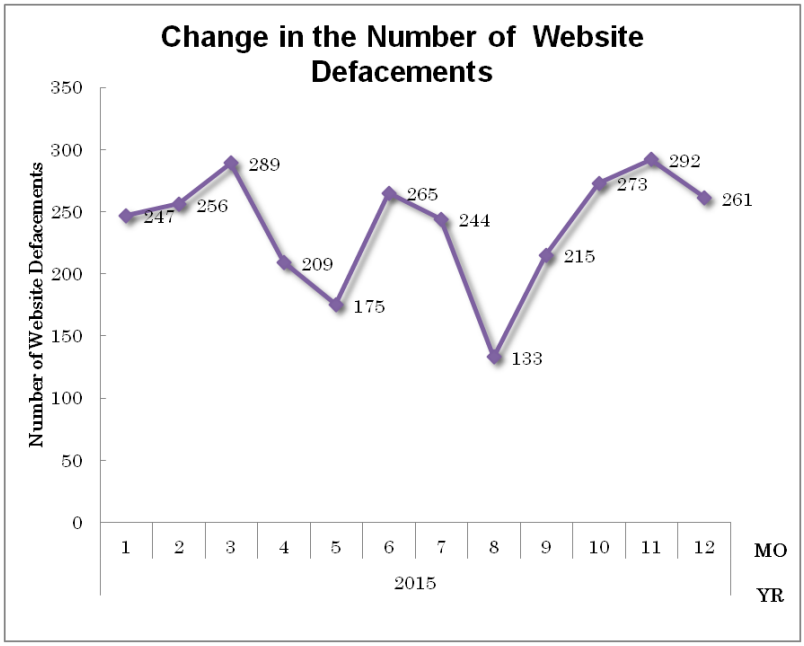


[Figure 3 Percentage of incidents by category]

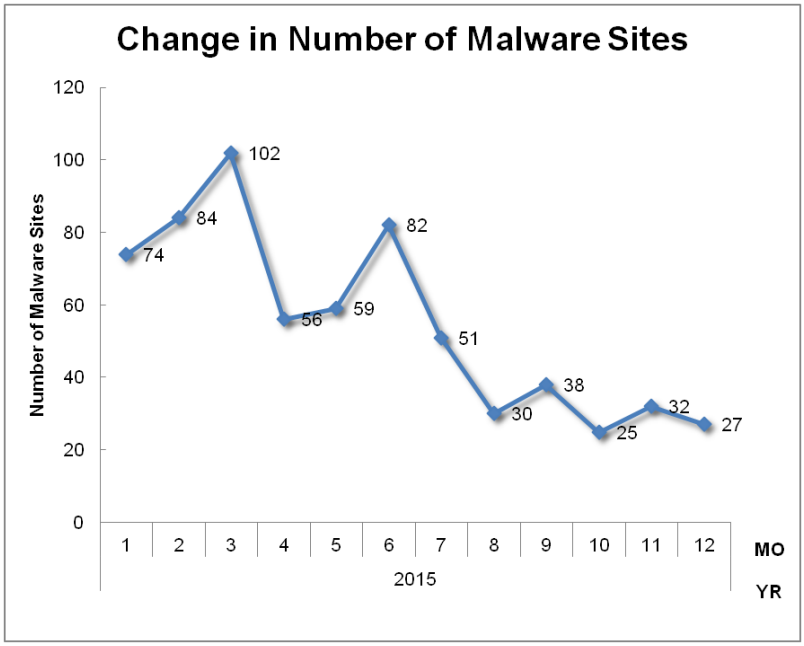
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



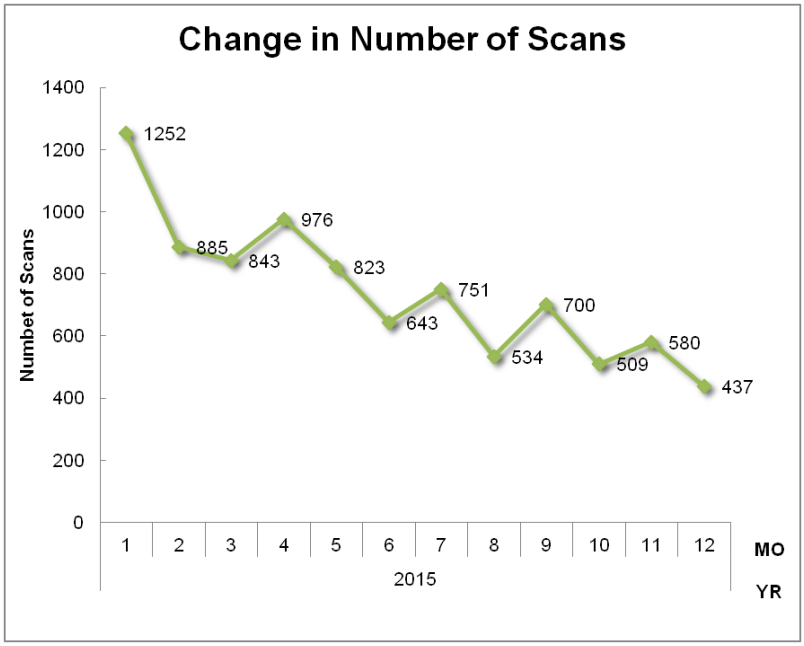
[Figure 4 Change in the number of phishing sites]



[Figure 5 Change in the number of website defacements]

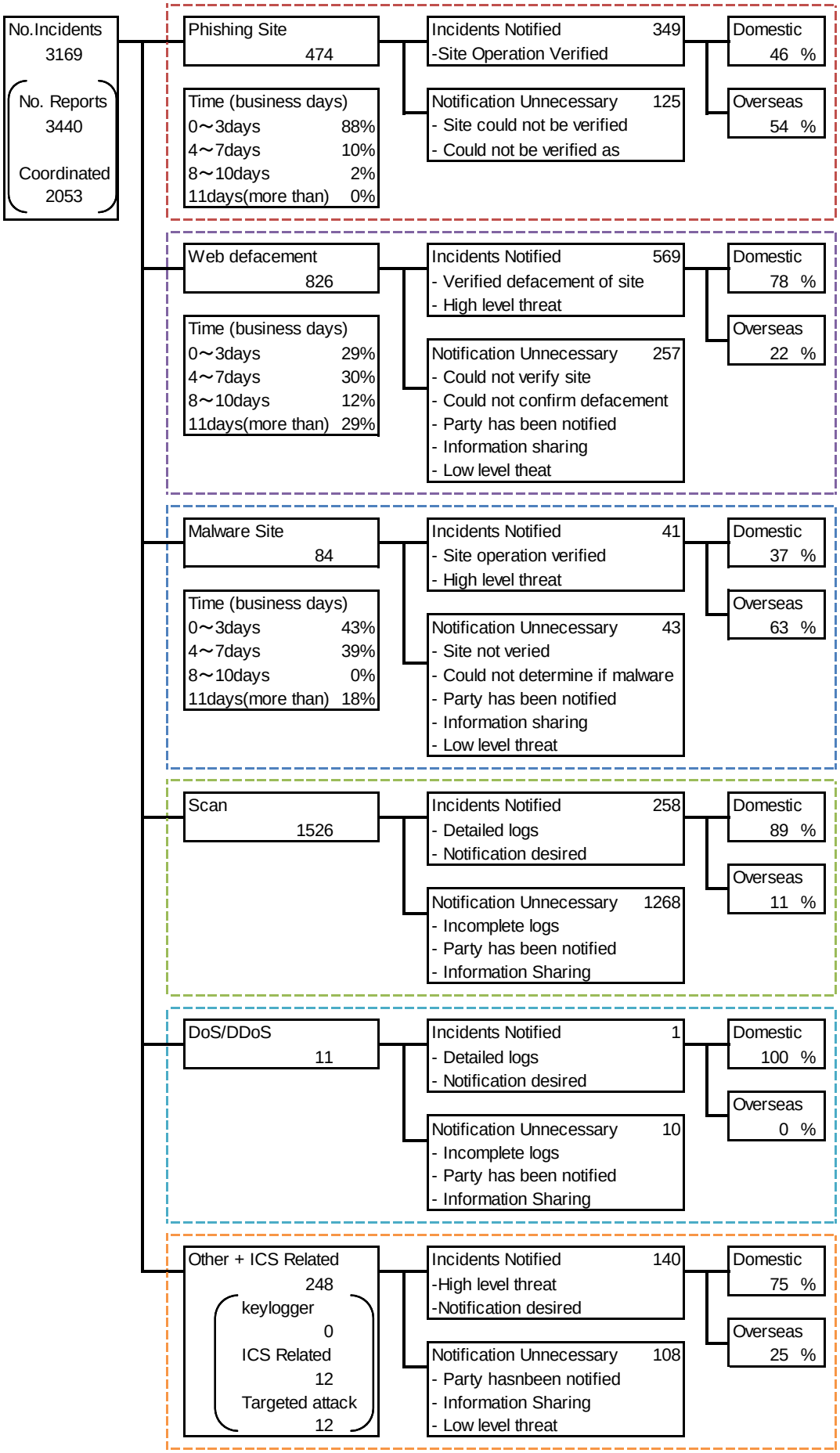


[Figure 6 Change in the number of malware sites]



[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.



[Figure 8 Breakdown of incidents coordinated/handled]

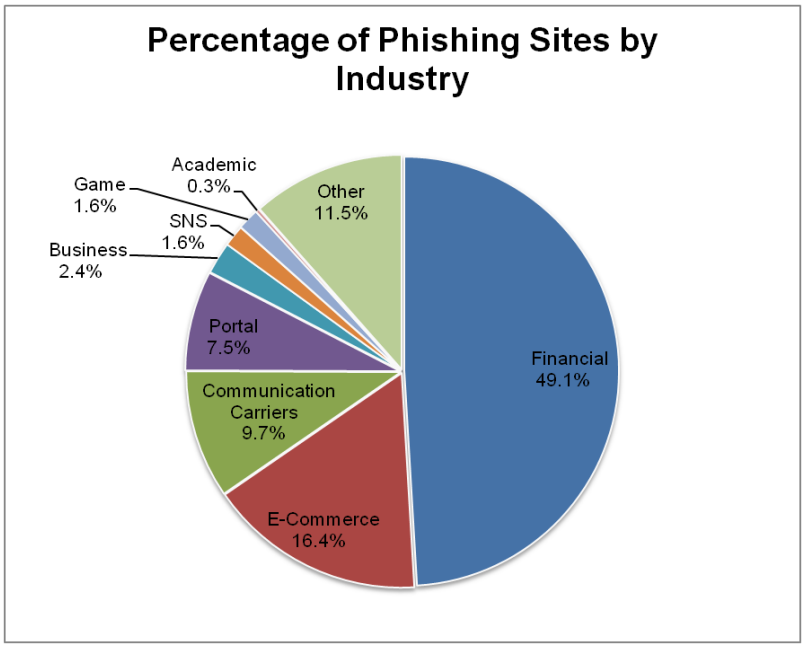
3. Incident Trends Phishing Site Trends

474 reports on phishing sites were received in this quarter, representing a 9% decrease from 522 in the previous quarter. This marks a 17% increase from the same quarter last year (406). 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 is shown in [Chart 9].

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

Phishing Site	Oct	Nov	Dec	Domestic/ Overseas Total (%)
Domestic Brand	30	35	59	124(26%)
Overseas Brand	93	88	69	250(53%)
Unknown Brand(*5)	40	30	30	100(21%)
Monthly Total	163	153	158	474(100%)

[*5] "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[Chart 9 Number of phishing sites by industry]

During this quarter, there were 124 phishing sites that spoofed domestic brands, increasing 10% from 113 in the previous quarter. And there were 250 phishing sites that spoofed overseas brands, which was a 7% decrease from 268 in the previous quarter.

Out of the total number of phishing sites reported to JPCERT/CC, 49.1% spoofed websites of financial institutions, and 16.4% spoofed e-commerce sites. Domestically and overseas, the industry that had the most phishing sites was the financial sector.

Some phishing sites spoofing different brands of domestic financial institutions had common characteristics in their domains and IP addresses, which appears to indicate that a specific group of attackers might be targeting multiple brands. Phishing sites spoofing multiple brands that were continually observed since October had .com as the TLD, and many of them used hosting services in Hong Kong. Phishing sites spoofing a different group of brands that were confirmed after the end of November had gTLDs such as .help, .ren, and .link, as well as subdomains intended to masquerade as a legitimate site. Many of these sites used hosting services in South Korea and the United States.

There were also a number of reports on phishing sites spoofing webmail services of domestic telecommunications operators. Many of these were set up on overseas websites that appeared to have been hacked. On the other hand, phishing sites spoofing domestic online games during this quarter were observed only in late October and in mid-December and amounted to a very small number.

The parties that JPCERT/CC contacted for coordination of phishing sites were 46% domestic and 54% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 48%, overseas: 52%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 826. This was a 40% increase from 592 in the previous quarter.

During this quarter, there were a number of reports that security products detected the download of ransomware when a compromised website was accessed. Website defacements in which an obfuscated code is embedded at the top of the page or immediately after a body tag are especially common. Compromised websites tended to be built using a content management system (CMS) such as WordPress, Joomla, and Drupal. JPCERT/CC has confirmed that when these websites are accessed, a malicious code redirects the visitor to an attack site. This leads to an attack exploiting vulnerabilities in Adobe Flash Player, Internet Explorer, etc., which causes malware to be downloaded and executed.

JPCERT/CC investigated the content of the compromised websites that was provided by their administrators and found that malicious codes containing strings such as //istart and //iend were

embedded in default CMS files. Probable causes of the defacements include attacks that exploit vulnerabilities in CMSs as well as their themes and plugins, and stolen administrator passwords.

3.3. Targeted Attack Trends

The number of incidents categorized as Targeted Attack was 12. This was an 80% decrease from 59 in the previous quarter. During this quarter, JPCERT/CC contacted a total of 11 organizations.

While targeted attacks were seen in great numbers during the first half of this fiscal year, only a few of these attacks were seen in this quarter. This may indicate that attackers are not engaging in attacks at the moment, but it is also possible that organizations being attacked have not noticed it. JPCERT/CC advises organizations to remain on the alert and conduct inspections mainly on the following points to confirm whether sufficient measures are in place to counter targeted attacks.

- Are operating systems and applications installed on PCs kept up-to-date to prevent the PCs from getting infected with malware and giving attackers access?
- Are server security updates applied without fail so that Active Directory servers can withstand attacks by a network intruder trying to exploit vulnerabilities?
- Are administrator rights properly operated on PCs participating in Active Directory domains, with no sharing or reuse of passwords, to prevent security from being compromised across the network?
- Are e-mail messages from suspicious senders blocked, with other measures taken such as restricting the types of attachment file that can be received, to counter spoofed e-mail with malware attached disguised as a document file?

It is also recommended that event logs of PCs and servers as well as proxy, firewall, DNS query, and other log data are properly captured to enable early detection and investigation of attacks.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 84. This was a 29% decrease from 119 in the previous quarter.

The number of scans reported in this quarter was 1,526. This was a 23% decrease from 1,985 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were HTTP (80/TCP), SMTP (25/TCP) and SSH (22/TCP).

[Chart 4 Number of scans by port]

Port	Oct	Nov	Dec	Total
80/tcp	247	327	239	813
25/tcp	101	156	111	368
22/tcp	84	56	44	184
445/tcp	22	28	15	65
23/tcp	13	7	9	29
21/tcp	8	7	4	19
3389/tcp	3	4	9	16
1433/tcp	3	9	2	14
53/udp	0	0	9	9
61222/udp	5	3	0	8
8080/tcp	2	1	3	6
16358/udp	2	2	1	5
53/tcp	0	0	4	4
4899/tcp	3	0	1	4
31385/udp	3	1	0	4
2632/udp	2	2	0	4
5900/tcp	2	0	1	3
3306/tcp	2	1	0	3
139/tcp	1	2	0	3
6379/tcp	0	2	0	2
53413/udp	0	1	1	2
5060/udp	1	1	0	2
443/tcp	0	1	1	2
2048/udp	2	0	0	2
110/tcp	1	1	0	2
Other	21	35	9	65
Monthly Total	528	647	463	1638

The number of incidents categorized as Other was 224. This was a 50% decrease from 450 in the previous quarter.

4. Incident Handling Case Examples

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

[Coordination involving domestic DNS servers responding to external zone transfer requests]
Around mid-November, JPCERT/CC received a report from an overseas CSIRT that organizational zone information, which normally should not be made available online, was found in a transferable state on some 1,800 name servers in Japan. The information concerned involved approximately 8,000 domains. The zone transfer function is used to reflect updates to zone information between DNS servers. Without proper access control, organizational domain information that should be hidden could be obtained by a third party unwittingly. This is said to be problematic security-wise, such as by providing a hint for initiating an attack.

JPCERT/CC has been contacting the name server administrators based on the list provided by the reporting body to have them confirm whether the zone transfer setting is intended.

[Coordination involving an overseas AS that illegitimately advertises BGP routes]
JPCERT/CC received a report in early November that BGP route information for a range of global IP addresses managed internally is being advertised by an overseas AS. If advertised BGP route information and hijacked global IP address ranges are left unresolved, they could be exploited by spammers to send spam e-mails, and the IP address ranges could be blacklisted as the source of fraudulent e-mails.

JPCERT/CC investigated the illegitimately advertised BGP route information, confirmed that an overseas ISP was advertising said global IP address range, and requested the advertising ISP and a neighboring ISP to respond appropriately. As a result, the administrator of the neighboring ISP responded that the unauthorized BGP route information had been removed, and this was confirmed by JPCERT/CC. Although it is rare for JPCERT/CC to receive a report on the unauthorized advertising of BGP route information, it is confirmed that similar cases occur with a certain frequency, and that blocks of global IP addresses are often hijacked without BGP route information being advertised.

Request for Cooperation

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

If you would like to encrypt your report, please use JPCERT/CC's PGP public key from the following URL.
Public Key
https://www.jpcert.or.jp/keys/info-0x69ECE048.asc

PGP Fingerprint：

FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

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 2015 Fiscal Year".