JPCERT/CC®

JPCERT-PR-2014-02
Issued : 2014-04-15

JPCERT/CC Activities Overview [January1,2014 –March31,2014]

Activity Overview Topics

—Topic 1—Number of incident reports received in the 2013 fiscal year was 29,191, and the number of cases coordinated was 8,717. - Incident Handling Statistics 2013 Fiscal Year -

The number of incident reports received during the 2013 fiscal year (April 1, 2013 through March 31, 2014) was 29,191 which was a 46% increase from 20,019 of the previous fiscal year.

The number of incidents contained in the reports was 26,687, and this was a 33% increase from 20,083 of the previous fiscal year. Out of the total number of incidents, there were 7,726 cases of website defacement, which was an increase of about 2.7 times from 2,856 of the previous fiscal year. In the 2013 fiscal year, there were numerous reports of website defacement that targeted visitors belonging to a specific group and that embedded malicious programs to lead visitors to malware-hosting sites. The number of phishing websites that were reported was 1,914 which was a 30% increase from 1,474 of the previous fiscal year, and the number of phishing sites that spoofed Japanese service providers targeting Japanese users increased from 311 to 719 (2.31 times of previous fiscal year).

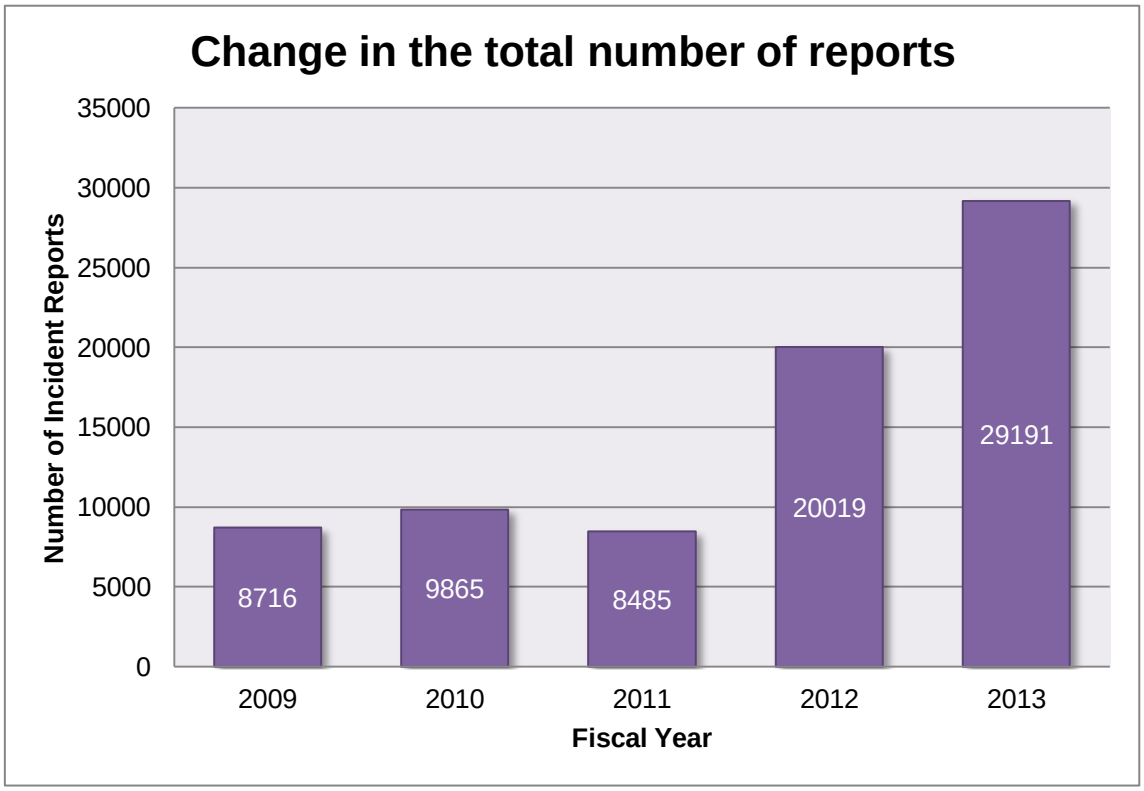
The number of cases coordinated to handle the incidents related to domestic and overseas sites was 8,717.

[*1] The "number of incident reports received" represents the total number of reports received through the web form, e-mail or FAX.

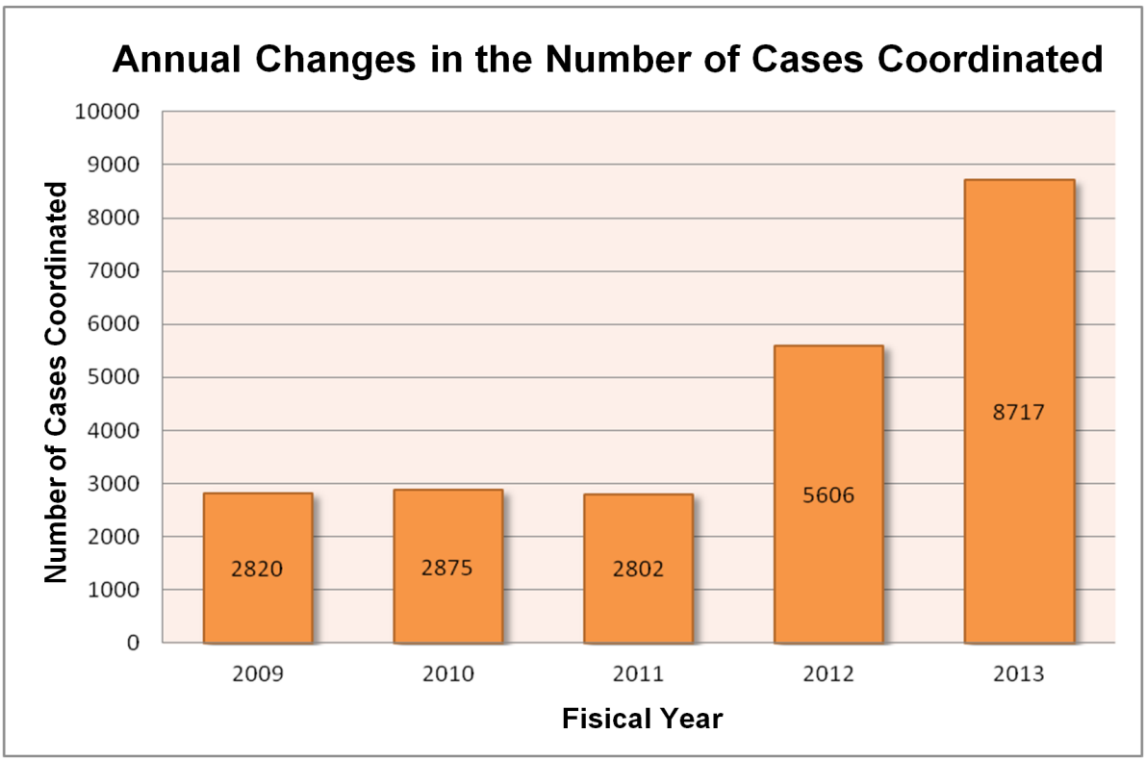
[*2] The "number of incidents" represents the total number of incidents contained in the reports that were received. Multiple reports received for a particular incident are counted as 1 incident.

[*3] The "number of incident cases coordinated" represents the number of cases where the site administrator was contacted with the investigation results and a request to implement countermeasures to prevent the spreading of the incident. Within the incident reports that JPCERT/CC receives, some include information about incidents that has been already handled but can be useful in understanding domestic incident trends. The information also contains those sent by other security companies for reference (which do not require JPCERT/CC's assistance). This is the reason why the number of incident cases coordinated is fewer than the number of incidents.

The change in the number of incident reports received and cases coordinated over the past 5 fiscal years including the 2013 fiscal year is as follows.



[Figure1: Change in the total number of incident reports (by fiscal year)]



[Figure2: Change in the number of incident cases coordinated by JPCERT/CC]

—Topic 2—Publishing technical information on malware that collects internet banking information and providing the decoding tool "Citadel Decryptor"

JPCERT/CC conducted a detailed analysis on the malware "Citadel" which contains a function that steals internet banking information and shared this technical analysis with multiple organizations in this quarter. In order for this information to be utilized by more organizations, JPCERT/CC presented it during a two-day International Information Security Event "CODE BLUE" which was held in Japan on February 17 and 18th.

JPCERT/CC now provides a tool (“Citadel Decryptor”) to organizations that require rapid and efficient incident handling procedures.

Citadel Decryptor, which was developed and used for in-house analysis purposes, is a simple tool that reduces the time required to decrypt data in files and registry. It has been provided to 9 organizations as of the end of this quarter.

JPCERT/CC considers these activities - such as sharing technical information necessary to handle actual incidents – will allow for incident response to be more efficient and eventually result in improving security.

—Topic 3—APCERT Annual General Meeting 2014 and holding the TSUBAME Workshop
- JPCERT/CC continues to serve as the APCERT Chair -

The Annual General Meeting for APCERT, a CSIRT community in the Asia Pacific region, was held in Taipei from March 18th through 21st, and 21 member teams including JPCERT/CC participated in this event. This year's APCERT annual conference was conducted under the theme "Preparing for a Better Future - The role of CSIRT Community".
As the first step towards APCERT’s common objective “a safe, clean and reliable” cyberspace, necessity to construct cross-comparable and robust cyber security metrics was shared among the members.

During the APCERT Annual General Meeting, the election for a part of APCERT Steering Committee was conducted as well as for Chair and Deputy Chair team. JPCERT/CC was re-elected as Chair team (4th term – until 2015) and will continue to lead APCERT activities.

In conjunction with the Annual General Meeting, “TSUBAME Network Monitoring Project” conducted its workshop. (This is one of the working groups in APCERT which implements sensors on the Internet mainly in Asia Pacific region. It aims to encourage collaboration among members in traffic monitoring and data analysis against security threats including worm infection and scanning activities.) As a convener, JPCERT/CC shared its observations gained through the project during the year and provided a hands-on exercise to detect threats from collected data. Additionally, a presentation was given from Hong Kong and Sri Lanka team introducing how they utilize TSUBAME systems.