JPCERT-PR-2015-01
Issued: 2015/01/14

JPCERT/CC Activities Overview [October 1, 2014 - December 31, 2014]

Activity Overview Topics

－Topic 1－ Overseas support for developing security personnel: Lecturers dispatched to a malware analysis competition held for students in Thailand

JPCERT/CC has been continually working to help establish and operate CSIRTs and develop security personnel in the Asia Pacific region, including the ASEAN member states, as well as in Africa. As part of this effort, three lecturers were dispatched to Malware Analysis Competition 2014 held in Thailand during this quarter.

For two days from October 30 to 31, students studying malware analysis techniques gathered in Bangkok to attend the competition, which was sponsored by Thai CERT/ETDA. Approximately 40 students, representing 9 universities and 13 teams, participated from throughout the country, and vied with one another in their skills and ability to analyze malware through competition. According to Thai CERT/ETDA, this event was the first of its kind to be held in Thailand. To help make this event a success, JPCERT/CC first held a "Train the Trainer" workshop in May 2014 to provide Thai CERT/ETDA with know-how needed to train students on malware analysis techniques. During the next half a year, Thai CERT/ETDA offered training for students.

On the first day of the competition, JPCERT/CC gave a lecture on the various methods of malware analysis and a training session which included a hands-on exercise. On Day 2, competition was held in two sections: skills and presentation. In the skills section, participants were evaluated for their analysis skills; in the presentation section, they were evaluated for the method and content of their presentation on the viewpoint and approach in solving a problem. JPCERT/CC served on the panel of judges for the latter and presented a commemorative gift to the winning team of the presentation section.

ThaiCERT/ETDA
https://www.thaicert.or.th/events/2014/ev2014-11-08-1.html

－Topic 2－ TSUBAME training held in Sri Lanka

To make full use of the Internet threat monitoring system TSUBAME, the availability of personnel fully trained to analyze and interpret collected data is as important as the observation sensors and other equipment deployed to collect those data. The deployment of sensors initiated in 2007 has by now covered almost all the countries in the Asia Pacific region. JPCERT/CC is currently looking into the possibility of deploying sensors in the Near and Middle East region, while working to achieve stable operation and more advanced usage by enhancing the skill level of organizations participating in the TSUBAME project.

During this quarter, JPCERT/CC continued its visit to Sri Lanka started in the previous quarter to provide TSUBAME training at Sri Lanka CERT|CC and TechCERT. The training was aimed at familiarizing the staff with the TSUBAME system and the sensor functionality, as well as how to analyze and utilize the information obtained through this system. While TSUBAME's observation results are regularly shared among the project teams through the system, this kind of opportunity to exchange information and opinions in person contributes significantly to the improvement of the technical capabilities of organizations participating in the TSUBAME project. It also helps create an environment for establishing a closer collaborative relationship among CSIRTs.

Some of the past incidents affecting Japan are known to have originated from computers in Sri Lanka. It is expected that the enhanced relationship will lead to a faster response and issuance of alerts in future incidents.

TSUBAME Training and Annual National Conference on Cyber Security in Sri Lanka
http://blog.jpcert.or.jp/2014/10/tsubame-training-and-annual-national.html

TSUBAME (Internet Threat Monitoring System)
https://www.jpcert.or.jp/tsubame

－Topic 3－ Providing information for the international community: JPCERT/CC official English blog enters its 5th year

As part of an effort to create an environment for international cooperation in information security measures, JPCERT/CC has been enhancing its efforts to provide information in English, so that people in the world can have a better understanding of the various initiatives undertaken in Japan. With the English blog, JPCERT/CC has especially focused on making new and relevant information available on a timely basis.

The blog, launched in September 2010, marked its fifth year this quarter. In the beginning, the blog was updated roughly every other month; this year new articles were posted almost every month, providing twice the amount of information posted during the previous year. The articles are all written in English specifically for the English blog, instead of being translations of materials published in Japanese. They cover a wide range of topics, from articles explaining incident trends in Japan for foreign readers to those introducing the activities of JPCERT/CC. The English blog represents the organization's efforts to help foreign readers gain a better understanding of the security situation in Japan and to facilitate international collaboration.

English Blog
http://blog.jpcert.or.jp/

－Topic 4－ Move to establish internal CSIRT spreading among organizations: Security incident readiness among companies and other organizations

In the past, security countermeasures used to be focused on prevention. With attacks becoming increasingly sophisticated, an increasing number of companies and other organizations are looking to establish an internal CSIRT as an effective countermeasure on the assumption that incidents are bound to occur. However, the operation of internal CSIRTs presents various challenges, including developing personnel skills, sustaining their sense of mission and collaborating with other departments within the organization.

In 2007, Nippon CSIRT Association (NCA) was established to provide a place for internal CSIRTs to discuss such challenges and effectively share information about good operating practices and new threats. JPCERT/CC supports NCA by handling its administrative duties. The number of member organizations now total 69, with 22 new organizations added during this quarter. They represent various lines of business, including IT, telecommunication, finance, insurance, logistics, hotel business and retail.

In addition to supporting NCA, JPCERT/CC has continued to provide information and facilitate efforts toward the establishment of internal CSIRTs, such as compiling and publishing CSIRT Materials, which are considered the bible for the management of CSIRTs. JPCERT/CC welcomes the move among organizations to establish internal CSIRTs and views this trend as evidence of increasing understanding of their meaning. As the administrative office of NCA, JPCERT/CC will continue to offer various supports, including advising on the effective management of NCA with its burgeoning membership, enhancing information sharing among existing internal CSIRTs, and providing assistance to organizations planning to establish an internal CSIRT.

Nippon CSIRT Association
http://www.nca.gr.jp/index.html