JPCERT/CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-PR-2014-02
Issued: 2014-07-10

JPCERT/CC Activities Overview [April1, 2014 - June30, 2014]

Activity Overview Topics

—Topic 1— Increasingly sophisticated methods used to steal authentication-related information and efforts made to prevent damage

The Council of Anti-Phishing Japan and JPCERT/CC refer to the act of guiding users to a fake website and having them enter personal authentication information with the aim of stealing it as phishing. Both organizations accept information about phishing sites and reports on e-mails, etc., intended to guide users to such sites. For this quarter, phishing sites spoofing financial institutions accounted for 61.2% of the total number of such sites reported, while sites spoofing online gaming services accounted for 15.9%. As these numbers indicate, phishing sites spoofing financial institutions continue to make up the majority of the reports received for such sites.

In addition, recent years have seen an increase in the number of reports on malware targeting users of online services offered by domestic financial institutions. Once infected by this type of malware, authentication-related information stored on the computer is stolen, or is obtained by deceiving users to enter the information on a fake screen that is displayed when they access a legitimate site from the infected computer. Information stolen by such malware can be misused and lead to unauthorized money transfers or other financial damage. There are also reports on malware that steals client certificates issued for corporations, and malware that initiates unauthorized money transfers using the so-called “Man-in-the-Browser (MITB)” attack. Such malware is distributed mainly through e-mail attacks and compromised websites, and as such, a number of events that appear to be separate incidents could actually constitute a large-scale attack. In order to properly assess the threat of an attack, it is vital that detailed information about related incidents is carefully studied.

To protect online service users who are exposed to such sophisticated attacks, related industries are making ongoing efforts to understand the actual situation with regard to attacks, implement measures based on that understanding, and alert users to potential threats. JPCERT/CC also participates in the activities of the related industries and is endeavoring to prevent the spreading of damage in cooperation with related bodies and security service providers.

—Topic 2— Information Security Early Warning Partnership Guidelines and JPCERT/CC Vulnerability Handling Guidelines Revised and Released

The Information Security Early Warning Partnership Guidelines, jointly issued by related industry groups, IPA and JPCERT/CC, stipulate in detail matters concerning the handling of vulnerability-related information based on the notification of the Ministry of Economy, Trade and Industry on "Standards for the Handling of Software and Other Vulnerability Information." The JPCERT/CC Vulnerability Handling Guidelines stipulate the details of coordination between product developers and JPCERT/CC undertaken in accordance with the aforementioned guidelines. Following the revision of the METI's notification on May 14, the two guidelines were updated to specify that for cases in which the product developer cannot be reached after making certain efforts, relevant vulnerability information can be made public following deliberation by an independent committee. The revised guidelines were released on May 30. It is expected that the revised notification and guidelines will contribute to the reduction of risks and damage by allowing for the disclosure of vulnerability information to the product users, even when the developer cannot be reached and no countermeasure is provided. Going forward, detailed rules including those for the operation of committees will be formulated and put into practice at an early point. In addition, guidelines for canceling the public announcement of vulnerability information, and for the notification of vulnerability information to customers and other product users by the developer prior to public announcement, have also been added.

Information Security Early Warning Partnership Guidelines <Japanese Only>
https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
JPCERT/CC Vulnerability Handling Guidelines <Japanese Only>
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

—Topic 3— JPCERT/CC staff member elected to the Board of Directors of FIRST

The Forum of Incident Response and Security Teams (FIRST), an organization that brings together 301 Computer Security Incident Response Teams (CSIRT) active in 65 countries around the world (as of July 10, 2014), held its 26th Annual Conference in Boston, U.S., from June 22 through 27, under the theme of "Back to the 'root' of incident response." JPCERT/CC delivered a lecture titled "Open DNS Resolver Check Site" on June 23 and moderated a panel session titled "Developing Cybersecurity Risk Indicators – Metrics."

The activities of FIRST are planned by the Board of Directors, whose members are chosen by election at the annual conference every two years. For this year's election, Koichiro Komiyama, Senior Analyst of the Global Coordination Division of JPCERT/CC, ran for the board and was elected thanks to the strong support from related organizations. JPCERT/CC takes this success as being underpinned by the expectation for further efforts to promote cooperation among CSIRTs in the Asia Pacific region,

including the Asia Pacific Computer Emergency Response Team (APCERT), as well as in Africa. JPCERT/CC will continue to uphold its commitment to supporting teams wishing to join FIRST and cooperating with other international organizations, thereby contributing to the establishment of more effective international cooperation through FIRST.

FIRST.Org, Inc., Board of Directors
http://www.first.org/about/organization/directors