JPCERT/CC®

JPCERT-PR-2016-01
Issued: 2016-04-14

JPCERT/CC Activities Overview [January 1, 2016 – March 31, 2016]

Activity Overview Topics

－Topic 1－ JPCERT/CC releases "Preparing for Advanced Persistent Threats (APT): A Process Guide for Companies and Organizations"

On March 31, 2016, JPCERT/CC released "Preparing for Advanced Persistent Threats (APT): A Process Guide for Companies and Organizations" (in Japanese), a document that explains how companies and organizations can prevent and minimize damage in the event of an APT. The first edition of this Guide was created by Delta Risk LLC in July 2013 using information provided by Mandiant and Lockheed Martin and based on extensive expertise and experience in addressing APTs. It was provided to organizations that JPCERT/CC supported or partnered with as best practices in addressing APTs. The Guide was updated in March 2015 using the basic countermeasures set out in SANS/CSC's "Top 20 Critical Security Controls" and NIST's Cybersecurity Framework as a reference. The recent release is an online version of this second edition.

This Guide defines an APT attack, gives an overview of the invasion model, and explains the preparations and processes for preventing and mitigating the damage of attack.

A fact-finding survey conducted by JPCERT/CC in 2010 revealed many cases in which an attacker was carrying out an attack from inside the company, but no sign of it was detected for a long time. Even when an abnormality was found, log data was not retained or maintained properly in quite a few cases, preventing the performance of a sufficient investigation. There were also organizations that fell victim to an APT even though they had basic information security countermeasures implemented.

The Guide is meant to provide practical advice on how to effectively counter APTs, which call for a new perspective.

－Topic 2－ JPCERT/CC holds the 8th ICS Security Conference to raise awareness about industrial control system security

On February 17, JPCERT/CC held the Industrial Control System Security Conference 2016 in Tokyo.
At this year's conference, Tsuneo Kitamura, a parliamentary secretary of the Ministry of Economy, Trade and Industry, delivered the opening address, which was followed by lectures given by experts in fields

ranging from university research institutions to critical infrastructure operators. Under the theme of "The Front Line in Industrial Control System Security," speakers shared information about the latest in ICS security and discussed security enhancement measures undertaken in industries and organizations using ICSs. The conference drew a full house of 300. When this conference was first held seven years ago, most of the participants were ICS vendors. However, the participants this year were much more diversified: ICS system asset owners made up about 30%, ICS system vendors 30%, and ICS engineering firms 15%.

－Topic 3－　12th APCERT joint cyber drill

Asia Pacific Computer Emergency Response Team (APCERT) conducted a joint cyber drill to assess the ability to respond promptly to cyber attacks. This drill is held each year with the aim of enhancing cooperation among CSIRTs in responding to incidents that occur in the Asia Pacific region and create a broad impact that goes beyond national borders.

The theme of the 12th joint cyber drill was "An Evolving Cyber Threat and Financial Fraud." Damage caused by malware targeting Internet banking users is reported broadly, not only in Japan but also in other APCERT member economies such as Hong Kong and Singapore. In Sri Lanka, incidents of financial fraud through e-mail spoofing and other means are increasing. This year's theme was set and exercise scenario created in light of these circumstances. By working through the scenario, participating organizations reviewed the steps and technologies used in incident handling, such as notifying relevant organizations and analyzing malware and log files. A total of 26 teams from 20 economies among APCERT member organizations and 6 teams from OIC-CERT (The Organisation of Islamic Cooperation – Computer Emergency Response Teams) participated in the drill. This year's event attracted the greatest number of participating organizations ever, which is an indication of the sense of crisis shared among APCERT member teams toward cyber threats. It also reinforced APCERT’s close cooperation with OIC-CERT seen in recent years.

As APCERT Secretariat and a member of the Drill Organising Committee, JPCERT/CC played a leading role in discussions about the scenario and operation. JPCERT/CC also participated in the drill as a player and served as the Exercise Control (ExCon), whose job is to ensure that the drill proceeds smoothly. See the following webpage for details about the APCERT Drill 2016.

APCERT Drill 2016 - An Emerging Cyber Threat and Financial Fraud
http://www.apcert.org/documents/pdf/APCERTDrill2016PressRelease.pdf