Asia Pacific Computer Emergency Response Team

APCERT Secretariat: JPCERT/CC
Japan Computer Emergency Response Team Coordination Center
Contact: apcert-sec@apcert.org

APCERT Media Release

22 February 2011

Embargoed until 3 hours after drill commences
1130 hours(GMT+530 for India, Sri Lanka)
1300 hours (GMT+7 for Indonesia, Thailand, Viet Nam)
1400 hours (GMT+8 for Brunei, China, Chinese Taipei, Hong Kong, Malaysia, Singapore)
1500 hours in (GMT+9 for Japan and Korea)
1600 hours (GMT+10 for Australia)

APCERT protects Critical Infrastructure against Cyber Attacks in Drill Exercise

The Asia Pacific Computer Emergency Response Team (APCERT) today has completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from Asia Pacific economies.

The theme of the drill was "**Critical Infrastructure Protection".** The **objective** of the drill was for participating teams to exercise incident response handling arrangements locally and internationally to mitigate the impact of ongoing Internet based attacks, enabling a better coordination of teams in the region in tackling cyber security incidents.

In this year's **scenario**, critical infrastructure companies of an imaginary economy were targeted. Employees of these companies received scam email and SMS containing hyperlinks to malware hosting websites. The malware, once installed, became part of a botnet, using IRC and a social network service channels to communicate with command and control severs. The botnet aimed to paralyze the targeted economy by commanding the bots to scan and infiltrate the critical infrastructure facilities to cause them malfunction.

Twenty teams from fifteen economies (Australia, Brunei, Bangladesh, China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Singapore, Sri Lanka, Thailand, and Vietnam) participated in the drill. They responded to the simulated incidents and shared information to detect and analyze the malware, to request knocking down systems pertaining to hosting of malware or the botnet, and to inform the critical infrastructure companies and the community of the security threats.

“There were several severe attacks targeting at the critical infrastructure of economies in the past few years,” said Roy Ko, Chair of APCERT. “These attacks usually came from distributed locations that required the coordinated effort of CERT teams and security organizations from different economies to track and close down. It is vital for every CSIRT to build up their capability to detect and defend when the community at-large is under attack and the daily business of the economy is hampered. The coordination network that has been built up within the Asia-Pacific region is a valuable resource to help each other in the event of such incident. The drill exercise will help us verify our points of contacts and procedures, and to respond to active Internet attacks in progress. It is encouraging that more teams have participated in the drill this year, with many other teams and organizations worked as observers to learn from this exercise.”

About APCERT

APCERT was established by leading and national Computer Security Incident Response Teams (CSIRTs) from the economies of the Asia Pacific region to improve cooperation, response and information sharing among CSIRTs in the region. APCERT consists of **26 CSIRTs from 17 economies**.

Further information about APCERT can be found on www.apcert.org.