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

APCERT Media Release

28 January 2010

Embargoed after drill completion
1230 hours(GMT+530 for India, Sri Lanka)
1400 hours (GMT+7 for Indonesia, Thailand, Viet Nam)
1500 hours (GMT+8 for Brunei, China, Chinese Taipei, Hong Kong, Malaysia, Singapore)
1600 hours in (GMT+9 for Japan and Korea)
1700 hours (GMT+10 for Australia)

APCERT knocks down Cyber Crimes with Financial Incentives in Drill Exercise

The Asia Pacific Computer Emergency Response Team (APCERT) today 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 "**Fighting Cyber Crimes with Financial Incentives".** The **objective** of the drill is for participating teams to exercise incident response handling arrangements locally and internationally to mitigate the impact of ongoing Internet based attacks and enable better coordination of teams in the region in tackling cyber incidents.

In this year's **scenarios**, financial web sites handling online transactions including e-banking, e-auction and stock trading were under different kinds of attack by cyber criminals, with an aim to paralyze online business activities, to compromise user credentials and to transfer money to fuel the underground economy.

Criminals are capitalizing on the popularity of online business which has become a profitable revenue stream for the underground economy. Criminals use professionally developed botnets (network of zombie computers) to obtain login credentials, to host phishing site, and to launch distributed denial of service (DDoS) attacks. Victim computers may be compromised and become part of a botnet when users browse web sites infected by malware.

Sixteen teams from fourteen economies (Australia, Brunei, 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, analyze the malware, and took actions to shut down or block systems hosting phishing sites or involved in DDoS attacks across the region.

"This is the **sixth drill** organized by APCERT members," said Roy Ko, Chair of APCERT. "The drill is important because cyber attacks are borderless. It is vital for every Computer Security Incident Response Team (CSIRT) to share the information and experience on cross-border incident handling, to refine and test the points of contacts and procedures, and to respond to active Internet attacks in progress. The capability to organize an annual drill verifies our competence to protect our own cyber security and our neighbours'. 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 CSIRTs from the economies of the Asia Pacific region to improve cooperation, response and information sharing among CSIRTs in the region. APCERT consists of **23 CSIRTs from 16 economies**.

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