

APCERT Media Release

Embargoed until 2 hours after drill commences

on 19 December 2006

1130 hours(GMT+530 for India)
1300 hours (GMT+7 for Thailand, Viet Nam)
1400 hours (GMT+8 for Brunei, China, Hong Kong, Malaysia, Philippines,
Singapore)
1500 hours in (GMT+9 for Japan and Korea)
1600 hours (GMT+10 for Australia)
1900 hours (GMT+12 DST, for New Zealand)

APCERT Shuts Down Malware Embedded Sites During Drill Exercise

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

The drill focused on handling compromised web sites hosting malicious code designed for use in distributed denial of service (DDoS) attacks.

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.

In this year's scenario, a number of global web sites have been compromised and used as a vehicle to spread malicious software which ultimately allows for infected computers to join a massive DDoS attack on e-Commerce web sites.

Fifteen teams from 13 economies, (Australia, Brunei, China, Hong Kong, India, Japan, Korea, New Zealand, Malaysia, Singapore, Thailand, Chinese Taipei, and Vietnam) will share information about incidents that have been detected and take action to shut down or block systems hosting malware or launching DDoS attacks.

This year's drill included extended participation from some APEC economies. Some participating national CERTs have organised local aspects to the drill with key stakeholders, such as major ISPs and law enforcement agencies.

[--- THIS SPACE FOR RECOGNISING LOCAL PARTICIPANTS ---]

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 19 CSIRTs from 14 economies.

“This is the third drill organised by APCERT members”, said Graham Ingram, chair of APCERT. “The drill is important for us to have a chance to share the common experience on cross-border incident handling and helps us refine and test the points of contacts and procedures we have established to share and respond to active Internet attacks in progress. The reality is that APCERT members are already very active in helping each other respond to Internet attacks within our respective economies, hence drills like this help us review and improve our procedures and ensure that we are prepared to help each other as best we can.” Mr Ingram said.

KrCERT/CC, which is part of the Korea Information Security Agency, initiated the idea for the drill and developed the drill scenario. “The drill is basically intended for cross-border incident handling scheme. The practical handling needs close cooperation, seamless communication and effective decision making between CSIRTs and ISPs in each economy. ” said Mr Woo-Han Kim, Head of KrCERT/CC, Korea Information Security Agency.

“The fact that we are now into the third drill and with added participation from other APEC economies serves to reinforce the importance that APCERT places on cross-border collaboration. The speed and diversity of cyber-security attacks demand that front-line CERTs be able to rise up to the challenge. With the fast-evolving and increasingly complex cyber-threats, it is crucial that the front-line CERTs are able to work together to combat cyber-threats through the APCERT drill,” said Mr Martin Khoo, Head of SingCERT, Infocomm Development Authority of Singapore

"MyCERT, a part of the Malaysian Cyber Security Agency (MCSA) finds value in the drill. The exercise illustrates the criticality in having immediate access to an effective contact point beyond physical borders and across time domains. Infrastructure attacks can be mitigated given the speed and competency in dissecting and analysing evidence. Informed decisions can be made in a short time period. We believe the APCERT drill has reinforced the collaboration among the participating economies," said Husin Jazri, Director of MCSA.

Mr Roy Ko, Centre Manager of HKCERT, said, "We have discussed with major ISPs and other related parties, and agreed that a coordinated process to quickly respond to Internet attacks will be beneficial to all parties. Based on the success of today's drill, HKCERT will organize a drill early next year with local parties, including ISPs and law enforcement bodies."

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