

APCERT Media Release

Embargoed until 2 hours after drill commences

on 21 December 2005

1100 hours (GMT+8 for China, Hong Kong, Malaysia, Philippines, Singapore)

1200 hours in (GMT+9 for Japan and Korea)

1300 hours (GMT+10 for Australia)

APCERT Drill Closes Worldwide Botnet

The Asia Pacific Computer Emergency Response Team (APCERT) today completed its second annual drill to test the timeliness and response capability of many of its member computer security incident response teams (CSIRT) teams.

The drill scenario centred around KrCERT/CC from Korea notifying other APCERT CSIRTs about the detection of a botnet attacking many sites in South Korea and requested intervention and assistance from other APCERT CSIRTs to help stop the attacks, by closing down the attacking bots located in other APCERT economies. A 'botnet' is jargon for a robot network. A botnet comprises hundreds and often thousands of compromised computers (bots) which allow them to be remotely controlled by an attacker to conduct a variety of different types of Internet attacks, including distributed denial of service attacks.

APCERT was established by leading and national CSIRTs from the economies of the Asia Pacific region to improve the level of cooperation, response and information sharing among CSIRTs in the region. APCERT comprises 17 CSIRTs from 13 economies.

“This is the second drill organised by APCERT member CSIRTs in China, Japan and South Korea”, said Graham Ingram, the APCERT Chair.

“This year, the drill has been expanded to include a number of other APCERT teams, including the leading or national CSIRTs of the Philippines, Singapore, Hong Kong, China, Malaysia, Chinese Taipei and Australia, he said. <suggest to place countries in alphabetical order>

“The drill is important 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, but 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. “Though the drill is designed to improve cross-border cooperation to stop Internet attacks, the drill also demonstrates the need for strong relationship between CSIRTs and Internet Service Providers (ISP) in each local economy,” said Mr Arnold Yoon, Coordination Manager for KrCERT/CC, Korea Information Security Agency.

“In reality, most cyber security incidents will be cross-border in nature. For resolution to be effective and timely, it is imperative that national CERTs understand the procedures and importance in working with one another. This drill offers an opportune platform to refine processes and prepare the various national teams to better manage security breaches in today’s borderless world of cyberspace,” said Mr Martin Khoo, Head of SingCERT, Infocomm Development Authority of Singapore

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

DRAFT