CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now
MOSTI Ministry of Science, Technology and Innovation

APCERT Asia Pacific Computer Emergency Response Team

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

MEDIA RELEASE

22 February 2011
CBMR-5-RFI-2-APCERT-V1
FOR IMMEDIATE RELEASE

APCERT PROTECTS CRITICAL INFRASTRUCTURE AGAINST CYBER CRIMINALS IN CYBER SECURITY DRILL

"The involvement of various CERTS in the Asia Pacific region in this annual cyber security drill reflected the strong relationship amongst the economies which could enhance the capability, improve response and creating greater collaborative work that is much needed in the cyberspace for its security and safety." - YB Dato' Seri Dr. Maximus Johnity Ongkili, Minister of Science, Technology and Innovation, Malaysia

(Kuala Lumpur) - 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 is 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 incidents.

In this year's **scenarios**, employees of critical infrastructure companies of an imaginary economy were targeted. They received email and SMS containing hyperlinks to malware hosting websites. Once installed, the malware uses control channels using IRC and a social network service to report to the botnet. The botnet aimed to paralyze the economy by commanding the bots to scan and infiltrate the critical infrastructure elements.

Criminals are capitalizing on the popularization of online business which has become a profitable revenue stream for the underground economy. Criminals use professional 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 are usually compromised and become part of a botnet when users browse websites infected by malware.

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, analyze the malware, and took actions to shut down or block systems

pertaining to hosting of phishing sites that planned to launch DDoS attacks across the region.

"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."

"CyberSecurity Malaysia is once again proud to be involved in the drill by providing an infrastructure to support this year's exercise." said Lt. Col. Husin Jazri, Chief Executive Officer, CyberSecurity Malaysia. The drill does not allow CyberSecurity Malaysia to maintain rapport with other security teams in the region but also it enhances the country's image and reputation. "The relationship with other CERTS is essential in resolving cyber security incidents reported to Cyber999 Help Centre. For the record, CyberSecurity Malaysia also provides technical support to the National Security Council in organizing the annual cyber security exercise for the Critical National Information Infrastructure (CNII) agencies." He added.

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.

~ End ~

CyberSecurity Malaysia is the national specialist centre for cyber security, under the purview of the Ministry of Science, Technology and Innovation (MOSTI). One of the goals of CyberSecurity Malaysia is to achieve **Reliability, Timeliness,** and **Effectiveness** in its services such as the **Cyber999 Help Centre** and the **CyberSAFE.**

For additional information, please visit our website at http://www.cybersecurity.my. For general inquiry, please email to: info@cybersecurity.my. To report cyber incidents such as harassment, fraud or intrusion to our Cyber999™ Help Centre, you may email to cyber999@cybersecurity.my. Follow us on social networks: www.facebook.com ("CyberSecurity Malaysia" fan page) and www.twitter.com/cybersecuritymy

*Jointly issued by **APCERT Secretariat: JPCERT/CC** (Japan Computer Emergency Response Team Coordination Center) and **CyberSecurity Malaysia** (Corporate Branding & Media Relations Department).*

For further enquiries about this document, please feel free to call +603-89460999, Mohd Shamil Mohd Yusoff (ext: 0895) or shamil@cybersecurity.my or Sandra Isnaji (ext: 0867) or sandra@cybersecurity.my or contact: apcert-sec@apcert.org / more information is at www.apcert.org