An agency under MOSTI

Ministry of Science,
Technology & Innovation

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

MEDIA RELEASE

CBMR-3-RFI-03-APCERT10-v1 **Embargoed after drill 1500 hours (GMT+8 Malaysia)**

28 January 2010

CyberSecurity Malaysia and APCERT knock down Cyber Crimes with Financial Incentives in Drill Exercise

Kuala Lumpur – CyberSecurity Malaysia collaborates with the Asia Pacific Computer Emergency Response Team (APCERT) in an annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from Asia Pacific economies. The cyber drill exercise was completed today (Thursday 28 January 2009).

This is the third year in a row CyberSecurity Malaysia assumed the role as exercise coordinator for the APCERT annual cyber drill exercise.

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

CyberSecurity Malaysia
(726630-U)
Level 7, Sapura@Mines
No. 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
T +603 8992 6888
F +603 8945 3205
www.cybersecurity.my

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."

Malaysia CERT (MyCERT), which is part of CyberSecurity Malaysia and the national point of contact for security incident co-ordination, participated both as a player and exercise coordinator. "Our participation and contribution in the cyber exercise is a demonstration of nation's commitment to combating cyber crime. It allows countries to revise security incident handling procedures and capabilities" said Lt. Col Husin Jazri (Retired), Chief Executive Officer of CyberSecurity Malaysia. He further emphasized that the drill is useful particularly in dealing with large- scale security incidents such as the Conficker worm outbreak in 2009 and the recent critical Internet Explorer vulnerability. "One of the lessons that we have learnt since providing the incident response service to the nation since 1997 is that the cyber criminals are organized. Therefore, the good guys have no choice but to work together".

In 2009, MyCERT handled more than 3,500 security incidents involving phishing, online fraud, malware infection and system intrusions. CyberSecurity Malaysia also co-organize the annual national cyber exercise with the National Security Council.

Apart of APCERT members, CyberSecurity Malaysia is currently the Chair of OIC-CERT (Organization of Islamic Conference – Computer Emergency Response Team).

~ end ~

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.

About CyberSecurity Malaysia
CyberSecurity Malaysia is the national cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia. The services include:

- Cyber999™ Help Centre
- Malaysia Computer Emergency Response Team (MyCERT)
- Digital Forensics / CyberCSI™
- Security Management and Best Practices
- Security Assurance
- Vulnerability Assessment Services
- Malaysia Common Criteria Certification Body (MyCB)
- Information Security Professional Development
- Outreach Programmes

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8945 3205

- Cyber Security Policy and Legal Research

Issued on behalf of APCERT by the Corporate Branding & Media Relations Department of CyberSecurity Malaysia.

For more information about CyberSecurity Malaysia, please visit website at www.cybersecurity.my. To report cyber incidents such as harassment, fraud or intrusion to our Cyber999™ service, you may email to cyber999@cybersecurity.my

For more information, kindly contact:

Mohd Shamil Mohd Yusoff
Office: +603 8946 0895
Mobile: +601 2249 6938
E-mail: shamil<at>cybersecurity.my

Sandra Isnaji
Office: +603 8946 0867
Mobile: +601 2324 5867
E-mail: sandra<at>cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8945 3205