Bangkok Post
database
WEDNESDAY, NOVEMBER 28, 2007

THE CRIMS ARE COLLABORATING

Collaboration among authorities is needed if they want to keep up with cyber criminals

Story by SHAWN KELLY AND APINUN TUNPAN

Collaboration among Internet criminals has exceeded that of law enforcement officials, a half-day international seminar at the Asian Institute of Technology (AIT) on understanding the "Underground Economy" of the Internet heard recently.

Experts on a panel advised that to gain an equal foothold, Internet network service providers, law enforcement agencies and national governments needed to collaborate. Information exchange was necessary to take action against cyber crime elements, the experts agreed.

Given the high degree of Internet connectivity, no single country is immune from illicit Internet activity, one expert said, emphasising the fact that any cyber crime occurring in an Internet-connected country immediately becomes a problem for all other countries.

Panel participants included Internet Corporation for Assigned Names and Numbers (ICANN) chief technical officer John Crain, Pakistan Federal Investigative Agency's Ammar Jaffri, Japan Computer Emergency Response Team Coordination Centre's Chris Horsley and Team Cymru's Ryan Connolly.

The event was organised by AIT's Internet Education and Research Lab (intERLab) and the Asia Pacific Network Information Centre (APNIC) and was part of a larger four-day intensive workshop on "Internet Crimes: Prevention, Detection and Investigation" held last month at the intERLab Center.

A presentation on the "Underground Economy" by Connolly revealed the dark of the Internet. Connolly highlighted the different forms of Internet crime, the manner in which the crimes are committed, and the ways in which different governments as well as organisational bodies could help better control and prevent such incidences from occurring.

"Information assets are actively stolen and traded to make real or cyber money. With the vast power and connectivity of the Internet, any corporate organisations, government units or individuals can be victimised," Connolly cautioned.

He added that without a person's consent (and often without their awareness), spyware/virus-infected computers could be a part of the so-called "bot-nets" that someone else has control over. Valuable information items such as bank accounts, credit card numbers, passwords, identification numbers and even Skype or other voice-over IP accounts could easily be stolen and then traded by cyber criminals.

Cyber criminals have openly established their own communities to collaborate, including a market to exchange stolen information assets, and have a rating system in place to identify who has a good or bad reputation regarding underground deals.

Among those attending the event were law enforcement agency officials, security officers from financial institutions targeted by Internet crime, systems and network administrators, as well as technical staff who manage or support networked information systems of ISPs.

Internet security specialists at the workshop said that although enforcement and education were playing an important role in the fight against Internet crime, they still faced an uphill battle.

However, improved communication between administrators and information technology people offers hope for better protection. Corporate administrators and managers needed to understand the value and function of an incident response in order to support the technical people, the intERLab trainers said.

An effective response system requires some level of awareness, cooperation, and support from every employee. Training staff on how to recognise potential incidents and to react appropriately is a vital step in creating a successful incident response program, trainers said.

According to intERLab director Professor Kanchana Kanchanasut, over 20 participants at the intERLab-hosted workshop learned some of the more sophisticated methods used by cyber criminals and specific techniques to thwart them.