Media Release

22 March 2006

International internet investigation nets arrest

The first successful joint investigation into botnets in Australia by the Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP), the NSW Police and Victoria Police has resulted in the arrest of a suspect believed to have been behind a series of high profile internet attacks.

Following a series of Distributed Denial of Service (DDoS) attacks upon Internet Relay Chat (IRC) servers in Australia in 2005, Australian police using information provided by the Belgian Federal Computer Crime Unit began investigating the attacks which also affected the United States, Singapore and Austria.

The attacks were carried out by means of IRC botnets. Botnets are networks of computers on the Internet which have been compromised of bot programs, which are remotely controlled through Internet Relay Chat servers.

Bots spread by taking advantage of common vulnerabilities on unprotected computers. Home personal computers are often a desirable target for attackers.

The bots, once installed on a host computer connect to an IRC server and silently wait for further commands. By having all the bots connect to an IRC server, an attacker is able to control many (sometimes thousands or tens of thousands) bots at once by issuing commands that all the bots will respond to. In this way botnets can be used to launch DDoS attacks by commanding all the bots to send Internet traffic to a particular IP address at once.

The suspect, a 22-year-old male from Victoria will be charged with using a telecommunications network with intention to commit a serious offence under *Section 474.14 Criminal Code Act 1995.*

DDoS attacks by bot networks are a major issue of concern and threat to Internet Service Providers.

Director of the AHTCC, Federal Agent Kevin Zuccato said Bot networks are also a concern to others involved in the use and management of the Internet and its facilities. They are known to have been utilised by groups to facilitate other unlawful activity.

“Bots and bot networks continue to be of concern, and are linked, not only to DDoS attacks, but to a range of other malicious activity including identity theft and spam,” Federal Agent Zuccato said.

“Home users can help protect their computers from becoming victims of bot activity by having up to date anti-virus software and firewalls, as well as updating their operating systems as soon as security updates are made available,” he said.

People need to be aware of the potential for illegal software to access and corrupt their computer systems and software. The maximum penalty for using a telecommunications network with intention to commit a serious offence is 10 years imprisonment.

Media enquiries: AFP Media (Canberra): (02) 6275 7100