Australian Internet Security Initiative helping address botnet menace

Hardly a day passes without some publicity about the latest internet scam, often about spam emails that entice recipients to reveal personal identity information, which the perpetrators can use for some form of fraud. What is less widely known is how these spam emails are sent.

According to the international e-security company, Sophos, up to 90 per cent of spam is now sent by networks of compromised computers known as 'botnets'. Botnets are made up of individual computers—known as 'zombies' because they are controlled remotely without the owner's knowledge—'infected' by malware (malicious software).

Botnets are involved in other malicious and criminal activities. They can be used to host illegal content, such as a 'phishing' website designed to obtain personal identity information from unsuspecting visitors to the site who think it is legitimate. Botnet malware can be used to harvest and fraudulently use personal identity information that is on the infected computer, such as internet banking data.

Botnets have been used to mount distributed 'denial of service' attacks on websites, effectively taking the websites out of operation while the attack is occurring. Sometimes the threat of a botnet attack is used to blackmail businesses. In 2006, members of a gang in Russia were jailed for extorting more than $4 million from British companies after threatening to attack their websites.

Estimates vary widely on the percentage of worldwide computers that are zombies. The US Georgia Tech Information Security Centre put this figure at 10 per cent in October 2007. The August 2007 Personal Internet Security report from the UK House of Lords suggested a figure of five per cent, but noted that the total number of zombies was unknown. Whatever the actual number is, botnets represent a significant threat to the safety and stability of the internet. Their activities also have the potential to erode consumer and business confidence in internet transactions.

In November 2005, ACMA piloted a program to help address the botnet threat—the Australian Internet Security Initiative (AISI). Six internet service providers (ISPs) participated initially, which was extended to 25 ISPs in October 2006. Participation in the AISI is voluntary. Through the AISI, ACMA provides daily reports to participating ISPs about zombie computers identified on their networks in the previous 24-hour period. The ISPs use this information to liaise with their customers to 'disinfect' or remove the malware from their computer. Customers are usually unaware that their computer is compromised. This activity not only helps address the immediate problem, but alerts users to the need to ensure their computer has anti-malware software—such as anti-virus software—that is regularly used and updated.

Funding of $4.7 million over four years was provided in the May 2007 Budget to further expand and consolidate the AISI. The expansion is part of an integrated suite of e-security activities known as the 'E-Security National Agenda', which involves many agencies. Activities include the e-security website operated by the Department of Broadband, Communications and the Digital Economy, www.staysmartonline.gov.au.

ACMA has expanded its identification of the sources of compromised Australian computers as part of the AISI. This led to a significant increase in the number of compromised computers reported daily to ISPs, which now averages around 3,000 reports per day—up from a few hundred in mid-2007.

Improvements have also been made to the daily reports received by ISPs and communications with them have been streamlined. An example of some of the data received by ISPs is provided below (each line represents information associated with one compromise). All timestamps are relative to Coordinated Universal Time (GMT+0).

IPv4 address	Timestamp	Type (of compromise)
1x1.2x6.22.1x9	2007-11-18 08:37:05	Trojan: Stormworm
1x9.1x8.195.9x	2007-11-18 21:58:57	Trojan: Unknown bot
1x4.1x1.76.1x0	2007-11-18 20:53:59	Spam sender
5x.1x5.96.1x8	2007-11-18 10:51:36	Spam sender

To date, ISPs have strongly supported the AISI and, in 2008, ACMA will actively promote it to Australian ISPs that are currently not part of the initiative. Work will also be done to expand the range of daily data feeds into the AISI. ACMA's experience is that this data needs continual renewal because the utility of sources can change rapidly in line with evolving botnet developments and control mechanisms.

The initiative has attracted international interest and ACMA has worked with the International Telecommunication Union in sharing its AISI experience and expertise.

More information about the AISI, including a list of participating ISPs, is on the ACMA website at www.acma.gov.au (go to For licensees & industry: Content requirements > Internet: Spam & e–Security > Information for ISPs & ESPs).