# Spot a bot to stop a botnet

May 1 2012

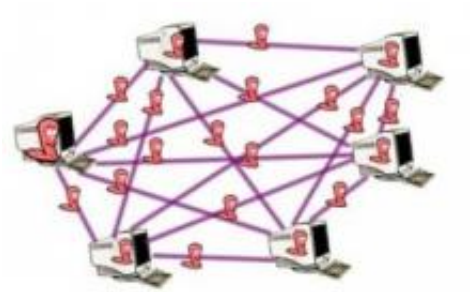

Image credit: Security Networks

Computer scientists in India have developed a two-pronged algorithm that can detect the presence of a botnet on a computer network and block its malicious activities before it causes too much harm. The team describes details of the system in a forthcoming issue of the *International Journal of Wireless and Mobile Computing*.

One of the most significant threats faced by computer networks is from "bots". A bot is simply a program that runs on a computer without the owner's knowledge and carries out any of a number of tasks over the network and the wider internet. It can run the same tasks, such as sending emails or accessing a specific page on the internet, at a much higher rate than would be possible if a person were to carry out the task. A collection of bots in a network, used for malicious purposes, is a botnet and while they are often organized and run by a so-called botmaster there are bots that are available for hire for malicious and criminal activity.

Bots might be illicitly installed on computers in the home, schools, businesses, government buildings and other installations. They are usually carried into a particular computer through a malicious link on the internet, in an email or when a contaminated external storage device, such as a USB drive is attached to a computer that has no malware protection software installed.

Botnets are known to have been used to send mass emails, spam, numbering in the hundreds of millions, if not billions of deliveries. They have also been used in corporate spying, international surveillance and for carrying out attacks known as Distributed Denial of Service (DDoS) attacks, which can decommission whole computer networks by accessing their servers repeatedly and so blocking legitimate users.

Manoj Thakur of the Veermata Jijabai Technological Institute (VJTI), in Mumbai, India, and colleagues have developed a novel approach to detecting and combating bots. Their technique uses a two-pronged strategy involving a standalone and a network algorithm. The standalone algorithm runs independently on each node of the network and monitors active processes on the node. If it detects suspicious activity, it triggers the network algorithm. The network algorithm then analyzes the information being transferred to and from the hosts on the network to deduce whether or not the activity is due to a bot or a legitimate program on the system.

The standalone algorithm is heuristic in nature, the team says, which means it can spot previously unseen bot activity, whereas the network algorithm relies on network traffic analysis to carry out its detection. The two techniques working together can thus spot activity from known and unknown bots. This approach also has the advantage of reducing the number of false positives.

**More information:** *Int. J. Wireless and Mobile Computing*, 2012, 5,

144-153

Provided by Inderscience Publishers