

## McAfee says Botnets growing problem

by Vanessa Ho

With botnets becoming a growing problem for Internet security, McAfee Inc. released a whitepaper report that looked at the rise of these attacks and what companies and governments can do to prevent them.

The report, entitled "Killing botnets: a view from the trenches," defined a bot as a compromised host connected to the Internet that has been infected with malicious code installed by a hacker or a self-propagating worm. While a botnet, the report said, is a connection of bots that run autonomously.

Botnets allow an unauthorized user to remotely take control of a host computer without the victim's knowledge or permission. Infected computers can be used to launch distributed denial-of-service attacks (DDOS), send spam and spyware or commit cyber extortion.

"Botnets can result in country-wide outages and disruptions," said Eric Winsborrow, vice president of product marketing at McAfee, Inc. in a statement.

In the past, botnet attacks were monitored and detected by intrusion detection systems but were limited in the types of remediation it could take.

The best approach in blocking and preventing botnet attacks, said the report's authors, are network intrusion prevention systems (IPS).

"Intrusion prevention can identify, alert and block attacks against networked devices [in real-time] based on a set of rules established by the system administrator," the report noted.

The report also cited a case study where the network infrastructure of a telecommunications company in Central America was brought down by botnet attacks. One of the company's business units was seeing almost six million botnet attacks a week that caused multiple network outages and many customer complaints.

"[McAfee] deployed a proactive network IPS solution to counter the flood of botnet attacks, which lead to an immediate resolution of symptoms and a subsequent 95 percent decrease in botnet traffic," said Winsborrow.

The report concluded that an IPS approach is the best as it allows botnet attacks to be separated according to source and destination IP address.

"This allows investigators to quantify the number and size of botnets passing through an ISP," wrote the report's authors.

With this added layer of protection, IPS products like McAfee's IntruShield maximize security by not only protecting against the exploit that installs the bots, but also by blocking the bot's communication or activation through the Internet. IntruShield can be deployed deep within the network cloud to identify botnet armies and proactively and accurately block the exploits that bots rely on to take over new machines.

The report noted that national carriers and large ISP's are important to stopping DDOS through botnets by using an IPS-based approach. With ISP's taking the charge in shutting down botnet activity, it can result in such things as better Internet experience for customers, increased availability of the network and enhanced customer security.



## ONE information technology

a division of Integrated Network Inc.

461 Dawson Avenue, Penticton, BC, V2A 8E2

Tel: 250-490-3434 Fax: 250-490-3420

Kelowna Tel: 250-762-6559 Westbank Tel: 250-768-3415 Vernon Tel: 250-542-6225

Toll Free 1-888-NET-ONLY or on the web at [www.oneit.ca](http://www.oneit.ca)

Allysa Myers, a virus research engineer for McAfee, noted in her blog on the company's Avert Labs Web site that ISPs are increasingly becoming involved with security groups that have developed solutions to shut down "command and control" channels used by bots.

While a lot has been done to prevent botnet attacks, Myers also said in her blog that there are other things that can be done to solve the bot problem. She wrote that further cooperation is needed between security companies and ISPs in order to get more "command and control" channels shut down.

In addition, Myers wrote that security companies, ISPs and law enforcement agencies also need to work together to ensure more bot masters face legal action and that there needs to be more accountability for adware vendors who fund these malicious affiliates.

"ISPs should be offering more security services than simply anti-virus software and more security information should be available to novice users," she posted on her blog.

However, the McAfee report warned that despite the overwhelming success of field trials in preventing botnet attacks, it is likely that botnets will evolve to hide from IPS devices. If this occurs, said the report, the technology of the security vendors must evolve as well.



## **ONE information technology**

a division of Integrated Networx Inc.

461 Dawson Avenue, Penticton, BC, V2A 8E2

Tel: 250-490-3434 Fax: 250-490-3420

Kelowna Tel: 250-762-6559 Westbank Tel: 250-768-3415 Vernon Tel: 250-542-6225

Toll Free 1-888-NET-ONLY or on the web at [www.oneit.ca](http://www.oneit.ca)