Story By *David Geer*

BRASH BOTNETS ARE BILKING YOU AND YOUR CUSTOMERS!

Whether you realize it, you and your customers are being mugged and swindled by bands of puppetted Internet computers called botnets.

CASE FILES

According to a November 3rd New Scientist press release, June saw the humbling of Google, Microsoft and Yahoo! as their Web servers were nixed by a Distributed Denial of Service (DDoS) attack levied by botnets, a.k.a. zombie-nets.

Botnets are the most effective means of accomplishing DDoS attacks. "With the explosion in broadband connections an individual with malicious intent can establish a very large network of compromised machines very quickly. Those machines can flood a Web server and make it unresponsive," says Clarence Briggs, chief executive officer, AIT, home to the most secure data centers in the hosting world.

Last summer's DDoS on the three Internet titans is typical of a growing trend toward using botnets to extort Web-based enterprises. Cyber-hoodlums like those responsible will gladly refrain from bringing your site down, for a fee. But extortion isn't the only racket these bully driven bots are into.

From November 2003 to November 2004 Internet crime rose sharply. Organized crime families have discovered that there is money to be made from spamming, scamming, fraud, phishing and other means of duping innocent netizens.

According to a November 16th VeriSign press release, while Spam continues to be the primary vector for all of these Internet crimes, networks of captured machines or "botnets" have become the most common method of spreading spam. Botnets, therefore, are the chief tool of syndicates bent on turning Internet crime into a capitalistic venture.

Botnets can cost you whether the criminals make out or not. According to a New Scientist press release, an executive at a satellite TV firm in Massachusetts has been charged with hiring several botnets to disrupt the websites of three rivals, costing one of their Web hosting firms $1 million. That's what it cost in a case where the perp was caught.

WHAT CAN YOU DO?

What CAN you do? If you're up on your patches, anti-virus, spam protection and other security measures then botnets are probably not infecting you. But that's not your biggest problem. Vulnerable consumer systems are the ones being infected.

These machines become botnets, which attack you and your customers. These DDoS attacks can still bring you down. Spam and Internet swindles are still getting through to your endusers.

HERE ARE SOME ACTION POINTS FOR HOSTS COMBATING BOTNETS:

1. Make generous use of security products such as smart firewalls with intrusion detection and desktop security measures like software firewalls and anti-virus products.
2. Invest in the human touch with a fully manned operation watching your network for suspicious traffic behaviors.
3. Make endusers part of your team in combating botnets.

If we could convince endusers to

Cyber crime is only going to keep growing along with the number of new Internet users and personal computers. Our parents taught us to lock our doors or be wary of strangers; ironically, the internet breeds the opposite as users are constantly tempted to explore new places and stimuli," says Clarence Briggs, Chief Executive Officer of AIT.

Botnets can cost you whether the criminals make out or not. According to a New Scientist press release, an executive at a satellite TV firm in Massachusetts has been charged with hiring several botnets to disrupt the websites of three rivals, costing one of their Web hosting firms $1 million.

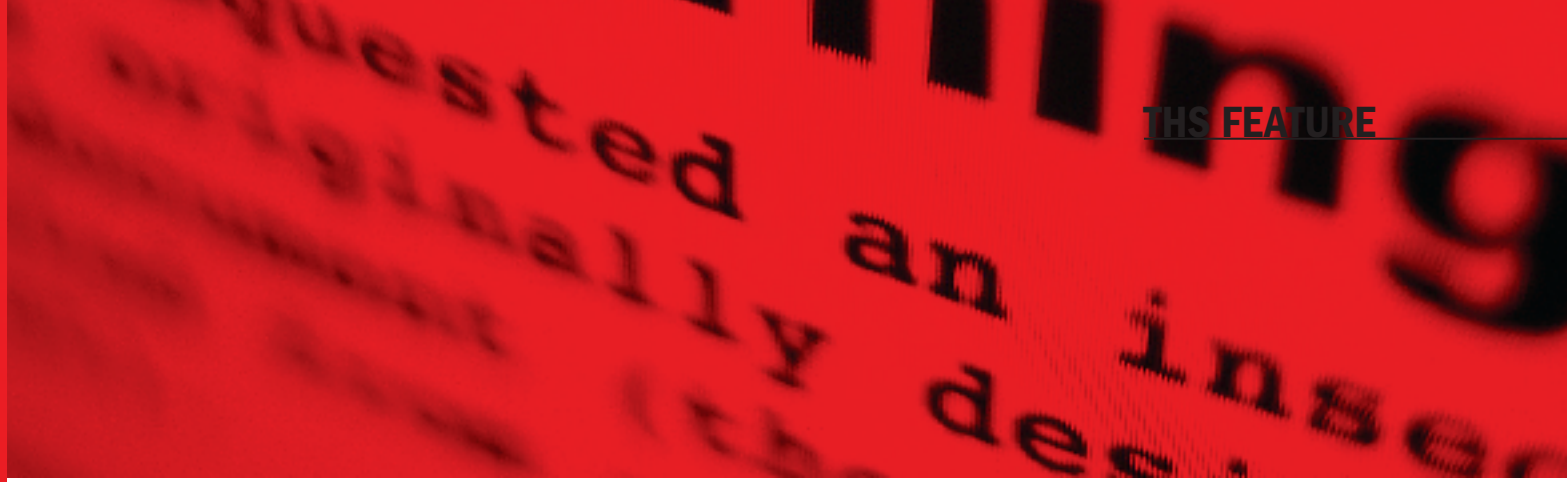
use discretion when clicking on email attachments, if we could get them to keep their system patches up to date, if we could encourage them to make judicious use of common security measures, there would be no vulnerable systems, no zombies, no botnets.

HERE ARE SOME POINTS FOR YOUR ENDUSERS:

1. Never open attachments that aren't expected or scanned by anti-virus protection or other appropriate malware detection products.
2. Never visit unauthorized or suspect websites. Like Spam, some infected websites have been used to open backdoors and turn systems into zombies.
3. Apply security patches religiously.
4. Use quality anti-virus software and firewalls and keep them up to date.
5. Err on the side of exclusion. We recommend the desktop security measures and resources at http://www.mvps.org/winhelp2002/unwanted.htm.

For those who must, or prefer to use Microsoft products, the Hosts file, Restricted Zone and other measures, available at the above site, will go a long way in excluding known bad Internet destinations from your system. Some of the suggested configurations can help secure against hacks, as well. As much as we may someday improve on it, enduser behavior demands that we make ample use of every security measure available to us.

"Cyber crime is only going to keep growing along with the number of new Internet users and personal computers. Our parents taught us to lock our doors or be wary of strangers; ironically, the Internet breeds the opposite as users are constantly tempted to explore new places and stimuli," says Clarence Briggs, CEO of AIT. THS



BEWARE THE CENTRAL SERVER

An attacker's central server takes control of vulnerable computers and uses them as bots. It's easier to find and kill the central server than to locate and eliminate each bot, especially when the central server can make more bots to keep their numbers high.

According to a November 3rd New Scientist press release, once a zombie computer is found, the bot inside it can be dissected to find the address of the controlling IRC chat room so that it can be taken down and the central server can be traced. However, some attackers are now covering their tracks by making the bots corrupt their own program code when extracted.

"In order to combat botnets, it is vital that networks be tightened down from a security standpoint; however, policy and best practices are what it takes to win the war. Never download or even click on a link that you are not sure about, and train your employees and family to do the same. A simple and cute temptation can be all that is needed to setup a "botshop". Prevention means policing behavior and instilling smart habits in users," says Briggs.