FIVE STEPS TO GUARD AGAINST BOTNETS

by Texas Attorney General Greg Abbott

ROBOT NETWORKS, ZOMBIE ARMIES these names may sound like science fiction. Unfortunately, they identify actual threats to information systems in Texas and across the globe.

By secretly invading residential Internet connections, hackers and spammers can download harmful software, including spyware and computer viruses, onto home computers. These malicious programs turn ordinary computers into robots that can be remotely controlled by cyber criminals. Once a robot computer network, or botnet, is in place, cyber criminals can use it to spy on Internet users, harvest sensitive personal information and send millions of spam messages.

Last year, the Office of the Attorney General shut down a Texas spammer who "leased" a substantial botnet to others who distributed illegal spam. We also took legal action against two suspects who used botnets to orchestrate spam e-mail campaigns touting near-worthless penny stocks. According to investigators, the defendants sent potential investors millions of unsolicited e-mails with baseless price projections about their stock offers.

Cyber security experts estimate that up to one quarter of all personal computers connected to the Internet may be hijacked by botnets. Signs of an infected computer often include slow operation, frequent "crashing" and outgoing e-mail boxes filled with messages the user did not send. The botnet's viruses and spyware usually do not disable hijacked computers, because computers must be functional and connected to the Internet in order for the botnet to work.

Despite this growing threat, Texans can take five simple steps to prevent their home computers from becoming part of a zombie network.

First, home computer users should install anti-virus and anti-spyware programs. Many Internet service providers and software companies offer programs that protect against malicious software. Most operating systems issue periodic security patches to fix flaws in their software.

Second, home computer users should set up firewalls to block unauthorized access while connected to the Internet. Computers that are unprotected by anti-virus programs and firewalls are extremely vulnerable to harmful software invasions.

Third, consumers should never open e-mail attachments or download files from unknown sources. The links or files could contain hidden programs that could snare the computer in a botnet. Additionally, e-mail users should be aware that spammers often solicit personal information through fraudulent spam e-mails that appear to be from a legitimate source, such as a bank or credit union. To prevent identity theft and unauthorized computer access, Texans should always be cautious when downloading files or opening e-mail attachments.

Computer users also should frequently change their passwords to e-mail accounts, online banking accounts and other secure Web sites. Cyber security experts suggest using passwords that contain a random string of characters that mix uppercase and lowercase letters with numbers and symbols. Consumers should refrain from using birthdays or anniversaries as part of their passwords or using the same password repeatedly.

Finally, home computer users should always disconnect from the Internet when they are away from the computer. Closing the Internet connection prevents hackers and spammers from accessing or abusing private information and resources.

Texans who believe their computers have been hacked or infected by spyware or a virus should immediately disconnect from the Internet and use updated anti-virus and anti-spyware software to fully scan the computer. Users should report unauthorized computer access to their Internet service provider as well as the FBI's Internet Crime Complaint Center at **www.ic3.gov.**

POINTS TO REMEMBER

GUARD AGAINST BOTNETS

- Install fully updated anti-virus and anti-spyware programs.
- Set up a firewall to guard against unauthorized online access.
- Never open e-mail attachments or download files from unknown sources.
- Change passwords frequently.
- Disconnect from the Internet when the computer is not in use.

Report unauthorized computer access to your Internet service provider and the FBI:

FBI Internet Crime Complaint Center
www.ic3.gov

For more information on this and other consumer topics, visit the Office of the Attorney General's Web site at **www.texasattorneygeneral.gov**

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT