



5 Steps Every Business Can Take To Guard Against Botnets

Robot networks and zombie armies may sound like names from science fiction. Unfortunately, they identify actual threats to information systems across the globe. By secretly invading business Internet connections, hackers and spammers can download harmful software, including spyware and computer viruses, onto computers and laptops. These malicious programs turn ordinary computers into robots that can be remotely controlled by cybercriminals.

Once a robot computer network, or botnet, is in place, cyber criminals can use it to spy on Internet users, harvest sensitive business and personal information and send millions of spam messages. Last year, the Office of the Attorney General shut down

Texas spammers who “leased” a substantial botnet to others who distributed illegal spam. They also took legal action against two suspects who used botnets to orchestrate spam email campaigns touting near worthless penny stocks. Cyber security experts estimate that up to one quarter of all personal and business computers connected to the Internet may be hijacked by botnets.

Signs of an infected computer may include slow operation and frequent “crashing”. Botnets may present no “symptoms” and may assist in updating your signatures and security settings in order to remain on your PC. 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.

Cyber security experts estimate that up to one quarter of all personal and business computers connected to the Internet may be hijacked by botnets.

Despite this growing threat, businesses and employees can take five simple steps to prevent their computers from becoming part of a robot network.

- 1** Most operating systems issue periodic security patches to fix flaws in their software. **Maintaining operating system and security updates** should protect computer users from known virus, malware and other botnet related threats. The operating system is the interface between the computer and supporting hardware and software. The kernel of any operating system is the most vital area.
- 2** A business 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 invasions.
- 3** A business should **consider using a hosted anti-virus and anti-spam service** that sits in the cloud or Internet. A hosted service can protect a company from known and unknown threats preventing them from ever reaching your network or computer users. This reduces the risks for obtaining a botnet significantly. This software-as-a-service approach is a good alternative to the traditional appliance and can offer a higher level of security for less than an appliance.
- 4** Employees should **never open email attachments, download files from unknown sources, or click on a link from an unknown source**. New attacks may involve social networks or hacked emails where the message appears to be originating from a close friend or other trusted person. The links or files could contain hidden programs that could capture the computer in a botnet. Additionally, email users should be aware that spammers often solicit personal information through fraudulent spam emails that appear to be from a legitimate source, such as a bank, social network site, friend or credit union. To prevent identity theft and unauthorized computer access, employees should always be cautious when downloading files, opening email attachments, and clicking on website links.
- 5** Employees should **always create strong passwords** and update them often to prevent hackers from accessing important information. Strong passwords should include a variety of characters. For best results, employees should combine letters, numbers and symbols for each of their passwords. Equally as important as creating the strong password is keeping this information a secret.

If an employee believes their computer has been hacked or infected by spyware or a virus they should report unauthorized computer access to their Information Systems team immediately. It is also recommended the business contact the FBI’s Internet Crime Complaint Center at www.ic3.gov.

About MessageLabs

MessageLabs services are only one portion of the recommended steps to safe guard against botnets, however, we believe it is an important service every business should consider. MessageLabs anti-virus, anti-spam and anti-spyware services deliver effective protection against email and web based threats. Skeptic™, our proprietary technology represents a unique but essential component in the anti-malware defenses we deploy on our clients' behalf including link following, attachment scanning and more.

Predictive and proactive, Skeptic™ uses heuristics and leading edge techniques to deliver unrivalled zero-hour protection from even the most sophisticated and targeted security threats by monitoring, tracking and blocking them at the Internet level, well away from your business network and computer users. This predictive technology proactively identifies and combats spam and viruses, incorporating thousands of heuristics rules, Bayesian learning, connection-based filtering, smart signatures, fuzzy fingerprinting, dynamic header analysis and more. Deployed across our dynamic global platform, it proactively scans billions of email connections and web requests every day. Because Skeptic scans both email *and* web traffic, it is able to apply what it learns in one medium to the other for more powerful scanning.

Skeptic™ is platform independent; that is independent of any specific technological platform and can work with all operating systems. This means no interoperability issues with your existing infrastructure.

MessageLabs, now a part of Symantec, offers industry leading service level agreements of unequalled protection and accuracy against known and unknown threats inherent in electronic communication. Including, but not limited to,

- 100% service availability
- 100% protection against email borne viruses and malware
- 99% spam capture rate, with a 0.0003% rate of false positives

Our managed services are delivered across a distributed, load balanced infrastructure in 14 data centers in four continents, and supported by security experts 24 hours a day, 7 days a week, 365 days a year. Our managed services offer secure, robust, scalable system architecture designed for optimum performance, improved operating costs and comprehensive administration and reporting via a secure, intuitive web based portal for over 19,000 clients.

We encourage you to try a free trial of our anti-spam and anti-virus service to see if this is an important and necessary step for your business to safeguard against botnets. Please call us at (866) 460-0000 or visit www.MessageLabs.com to download your free trial today.

To speak with a
product specialist call
toll free:

US: +1 866 460 0000
UK: +44 800 917 7733
APAC: +61 2 8208 7100

For specific country offices and contact numbers, visit the MessageLabs website

www.messagelabs.com
info@messagelabs.com