

# Anti-Botnet and Email Security Alert

## PROACTIVE ANTI-BOTNET TECHNOLOGY FOR ENTERPRISES

A Botnet is a network of computers, which have been compromised by malware, tuned to receiving commands from a central command and control computer situated anywhere on the global Internet. This central computer is usually controlled by criminals who use the compromised computers for their criminal activities. These activities can range from organizing denial of service (DoS) attacks, sending spam, phishing scams, and other criminal activities to recruiting other computers to the Botnet. Botnets are very hard to detect because of the fluidity with which they are operated. Botmasters use public services such as the Internet relay chat (IRC) and peer-to-peer (P2P) communication protocols to control their networks. Spam filters based on reputation and real-time black lists (RBL) are being defeated as a result of the spam arriving from Internet Protocol [IP] addresses which are yet to be black listed. The use of images and multimedia content to deceive spam filters contributes to larger loads for bandwidth and e-mail servers.

Reno, Nevada-based Engate Technology Corporation has recently announced a new version of its flagship anti-spam product, the MailSentinel™, which uses a proactive approach to mitigating the challenges faced in detecting and stopping Botnet threats before they reach the enterprise gateway. MailSentinel uses a proprietary database called GlobalRules™, which contains forensic information about known and future sources of spam. Using proprietary profiling and source verification techniques, the database identifies a network associated with an offending IP address or mail transfer agent (MTA) and creates a profile for the entire network containing information like permissible mail servers within the network. This profile is used to evaluate an e-mail for forgeries and tampering as sources of spam do not like to reveal their true identity and hence resort to forging the e-mail headers.

By using this intelligence, the solution creates rule-based filters based on identifying and separating clean hosts from illicit hosts within subnets that are known to be sources of spam. Engate has been profiling spamming networks for the past six years and it has used this experience to create smart rules to profile large networks efficiently. By profiling entire networks beyond infected hosts, Engate has been able to build up a repository of information about potential hosts that may become infected if not already. This helps their filters perform faster and very accurately without a rise in false positives.

The strategy of using a proactive approach to identifying illicit sources and potential sources of spam from compromised hosts helps its solution to scale more efficiently and quickly. The existing method of using reputation and RBLs only offers protection from the known and is not well prepared for the unknown. Botmasters are constantly moving their command and control structures and are always one step ahead of security solutions. Engate's proactive approach effectively minimizes the level of surprise these dynamic threats will offer in the future.

Engate's MailSentinel is currently deployed in mail servers and appliances and also in diskless versions. These diskless versions are suitable for devices such as routers, switches, and firewalls as they fit in 17 MB of read only memory and only require 256 MB of memory for operation. The company is in talks with vendors to embed this solution within network devices to create a layer of defense at the protocol level rather than waiting for a message to get to the mail server for processing. This strategy is significant as mail servers, especially enterprise servers are often inundated with a huge load of messages to process. The company has filed for 10 patents and has recently been granted a patent, which deals with the on-demand and off-line removal of unsolicited messages from a client network. The company's co-founders Wil Cochran, Rich White, Alan Huang, Haw-Minn Lu, and Ira Victor have around 30 patents between them and are responsible for the innovations that are driving Engate. Engate is open to collaboration with Universities and research groups in similar areas.



Vendor Details: Engate Technology Corporation, 4790 Caughlin Parkway, Suite 240, Reno, Nevada 89509 • +1-775-745-7151 • [info@engate.com](mailto:info@engate.com) • [www.engate.com](http://www.engate.com)