



FOR IMMEDIATE RELEASE

Contact: John O'Reilly

Phone: (678) 589-7100

Email: [Marketing@telemate.net](mailto:Marketing@telemate.net)

## **TeleMate.Net Software's NetSpective Web Filter protects schools from 'massive' botnet**

*Sudden spike in Tor users creates dangerous cycle that can overwhelm networks with chain of request failures*

**Norcross, GA – September 11, 2013** – TeleMate.Net Software, a leading provider of Internet security solutions, announced availability of Version 4.01 with enhanced signature detection of Tor, originally short for The Onion Router. In recent weeks the number of Tor clients has increase by more than five-fold. Experts agree that the sudden increase in Tor users is caused by a single massive botnet that has global security ramifications.

“Network administrators for school districts across the US have reason to fear since students are often unwilling participants in the spread of malicious content in their search for concealing their identity when accessing social sites and streaming media during school hours”, said Steven Tabaska, CEO of TeleMate.Net Software. “Though Tor conceals Internet traffic by routing content through a global network of relay servers, many technically savvy students fail to realize the hidden vulnerabilities they are inducing into the network.”

The danger of Tor being spread by a botnet is magnified by the sudden rapid spike in clients, their global distribution and Tor's ability to provide anonymous access to websites and other servers. Tor conceals a users' identity and their network activity from surveillance and traffic analysis by separating identification and routing. Security concerns are amplified by Tor's ability to access hidden services. If compromised Tor can route data to and from hidden services, even those hosted behind firewalls or network address translators (NAT), while concealing both parties.

“Policy control standards, as mandated by the Children's Internet Protection Act (CIPA), requires network administrators ensure filtering of obscene and harmful content. This includes detection and blocking of encrypted peer-to-peer technologies like Tor, UltraSurf, Piolet, and Bit Torrent”, Tabaska added. “NetSpective Web Filter's ability to decipher peer-to-peer applications provides a complete solution that protects network users that competitive products fail to address.”

For an online demonstration of TeleMate's NetSpective Web Filter, request a demo at [www.getnetspective.com](http://www.getnetspective.com) or contact us at [info@telemate.net](mailto:info@telemate.net).

### **About TeleMate.Net Software**

TeleMate.Net® Software is a global leader in voice and data network monitoring and security solutions, which provides cost effective, reliable, and feature-rich solutions to service providers, corporations, and federal, state, and local agencies, creating unprecedented visibility within their complex IT networks, and allowing customers to spend less time collecting and monitoring data and more proactive time managing their overall business. Since 1986, TeleMate.Net Software has evolved its core reporting technology, incorporating the latest advances in database, reporting, user-interface, and categorization technologies, to become the dominate force in addressing telecommunications administrators core requirements. For more information about TeleMate.Net, please visit our website at: <http://www.telemate.net>.

###

*If you'd like more information about NetSpective Web Filter™, NetAuditor® for NetSpective, or TeleMate® Unified Call Management, please email [Marketing@telemate.net](mailto:Marketing@telemate.net) or visit the TeleMate.Net website at [www.telemate.net](http://www.telemate.net).*