FOR IMMEDIATE RELEASE

Faronics Anti-Executable Successfully Blocks Zotob Worm

SAN RAMON, CA, August 17, 2005 — The new Zotob worm, called one of the fastest spreading infections in history, poses no worry to computer users who have installed Faronics Anti-Executable. In fact, before the Zotob worm was even released, Faronics Anti-Executable had the ability to stop it, thanks to Anti-Executable's unique whitelist concept. The Zotob worm, which exploits a flaw in the plug-and-play feature of Microsoft's Windows 2000 operating system, is wreaking havoc in many corporations around the world.

"Anti-Executable's whitelist technology doesn't rely on definition file updates," said Brent Smithurst, Faronics' Vice President of Technical Operations. "This means that computers protected by Anti-Executable don't need patches to protect against viruses and worms like Zotob; day-zero attacks are not a concern."

Anti-Executable's whitelist provides proactive protection against any past, present, or future executable virus, Trojans, worms, spyware, keyloggers, rootkits, or any other malware, without relying on definition files or heuristic techniques. The concept is simple: during installation, Anti-Executable performs a deep scan of the computer and authorizes all executables on it. From that point on, any other executable is deemed unauthorized and is prevented from installing or running, whether it was downloaded from the Internet or introduced via any removable media. There are no definition files to maintain or update, and any new executable will never run. Period.

The response to the proliferation of malware has traditionally been blacklist concepts or heuristic techniques. The problem with these methods is that they need to be monitored and kept up to date at all times. There is always the possibility of a new virus or Trojan doing its damage before the definition files have been released or updated on the user's computer. For more information about the benefits of whitelist versus blacklist technology, refer to the white paper in the Faronics Content Library.

Faronics' flagship product, Deep Freeze, also would have eradicated the worm with its restart-to-restore technology, which was recently validated by Microsoft Corp. Deep Freeze instantly protects and preserves original computer configurations; regardless of the modifications made to a workstation, a simple restart will eradicate all changes and reset the computer to its original state—right down to the last byte. Viruses, worms, and all other malware, along with the correlating computer downtime caused by them, are effectively eliminated. Deep Freeze in combination with Anti-Executable provides a powerful and impenetrable defense against malware; Anti-Executable will prevent the installation of an unwanted executable, and Deep Freeze will rid the system of the executable.

About Faronics

Faronics develops and markets intelligent utilities for absolute control of multi-user computing environments. Faronics' market-leading solutions ensure 100% workstation availability and have dramatically impacted the day-to-day lives of thousands of information technology professionals and computing lab managers. Our user-driven, powerful technology innovations benefit educational institutions, libraries, government organizations and corporations.

<div align="center"># # #</div>

MEDIA CONTACT

Brent Smithurst (Vice President, Technical Operations)
800-943-6422
bsmithurst@faronics.com