# Secure Computing warns of new security threat

*by Bend_Weekly_News_Sources*

Secure Computing Corporation, a leading enterprise gateway security company, today warned that blogs, bulletin boards and webmail are now being spammed with messages to visit a website to view "fun" videos.

Secure Computing has discovered a website containing a variant of the Storm worm. The worm installs a component on a user's machine that analyzes all network traffic via a layered service provider (LSP) integration and dynamically modifies blog comments, discussion posts and webmail-based emails as they are being posted by the user to include a link to the malicious code, thereby propagating itself to other victims.

"This signifies a new trend in malware that is spread through blogs, message boards and web-based email," said Dmitri Alperovitch, Principal Research Scientist, Secure Computing. "And this threat is particularly insidious in that anti-virus detection doesn't always work. This threat utilizes server polymorphism, which means that it is continuously being repackaged to make the binary appear different to signature-based anti-virus solutions." With the executable file being changed continuously, it easily sneaks below the radar of the leading anti-virus programs, which are largely signature-based.

Viruses, worms, Trojans and other malware have traditionally been distributed through users' email address books, and made to look like messages coming from them.

With this threat, we begin to see the addition of a Web attack component to traditional email based malware," said Alperovitch. "Secure Computing has already seen evidence of the malware propagating through messaging forums, such as Men's Health magazine, as well as thousands of blog sites," he said.