

14 March 2008

By: Marius Oiaga, Technology News Editor



## [Mass Web-Based Attacks Prey on Windows](#)

*Video demonstration courtesy of McAfee*

Security company McAfee has warned of a new mass web-based attacks preying on the Windows operating system. The first attack was initially discovered on March 12 and it involved SQL injection. [Craig Schmugar](#), threat research manager, McAfee Avert Labs, revealed that initially McAfee detected in excess of 10,000 compromised pages. Essentially, users are diverted from hacked pages to malformed websites that serve malware via IFRAMES. "This attack involves injection of script into valid web page to include a reference to a malicious .JS file (sometimes in the BODY, other times in the TITLE section). The .JS file uses script to write an IFRAME, which loads an HTML file that attempts to exploit several vulnerabilities, including: MS06-014; RealPlayer (ActiveX Control); Baofeng Storm (ActiveX Control); Xunlei Thunder'; DapPlayer (ActiveX Control) and Ourgame GLWorld GlobalLink Chat (ActiveX Control)," Schmugar stated. In a single day, the number of webpages compromised by the SQL injection attack doubled to over 20,000. Additionally, McAfee also came across another mass web-based attack via hacked webpages, only that this time the threat is connected with phpBB. Schmugar has even put together a video demonstration of this attack in action, and you will be able to find it embedded at the bottom of this article. "The attack seems to have started more than a week ago, and nearly 200,000 web pages have been found to be compromised, most of which are running phpBB. This contrasts yesterday's attack in that the vast majority of those were active server pages (.ASP). The ASP attacks are different than the phpBB ones in that the payload and method are quite different. Various exploits are used in the ASP attacks, where the phpBB ones rely on social engineering. phpBB mass hacks have occurred in the past, including those done by the Perl/Santy.worm back in 2004," Schmugar added.

[March 2008 - Mass Hack Demo](#) from [Schmoog](#) on [Vimeo](#).