

By: ~~May 2008~~ ~~May 2008~~ Biaga, Technology News Editor

[Rogue Security Solutions Take a Bite out of IE8 Beta 1](#)

ActiveX will continue to come under fire

Simply because of the ubiquity of its predecessors, Internet Explorer 8 will continue to come under fire. With one of the preferred avenues for attacks continuing to serve as a source of malware even in the next iteration of Microsoft's proprietary browser, ActiveX add-ons are a traditional vector of attacks on the Windows platform via IE, and Microsoft has worked to bulletproof [Internet Explorer 8](#) as much as possible with an array of mitigations. But additional security features such as Per-User (Non-Admin) ActiveX, ActiveX Opt-In and Per-Site ActiveX can do nothing to protect against social engineering schemes that rely on tricking the user into infecting the operating system. One illustrative example of ActiveX-based social engineering attacks involves rogue antivirus products. Attackers are counting on the end users' familiarity with the behavior of ActiveX in order to push malware as add-ons, claiming that it is in fact a security solution meant to resolve a plethora of problems on the end user's machine. Security researcher [Sandi Hardmeier](#) recently came across a fraudware website pushing a product dubbed Antivirus Scanner. As soon as a user visits the malicious website, a fake scan is started and performed to the point where the rogue antivirus falsely claims that it has detected malware on the machine. As a direct consequence, it advises users to install an ActiveX add-on, namely the malware itself, and become infected. This threat is tailored specifically to Internet Explorer and the ActiveX technology, and as you can see from the screenshots with [IE8 Beta 1](#), it looks rather convincing. Now, in [Firefox 3.0 RC1](#), the malicious webpage for Antivirus 2008 Online Security Scanner is broken, as the open source browser does not integrate ActiveX add-ons. Still, with the exception of this detail, the attack goes in the same manner, and the end user is, like it or not, offered the malicious payload for download. In general, a rogue antivirus simply blackmails the end user for a moderate sum of money in order to remove the fake threats that it has detected in the first place. But there is no telling what malicious code it will actually install on the computer. Users are advised to run security programs only from trusted vendors, and to steer clear of online scanners that perform unsolicited analysis of their machines.