

3 January 2008

By: Bogdan Popa, Security and Search Engines Editor



Windows XP is one of the affected operating systems

[Internet Explorer Involved in JavaScript Infection](#)

JS_PSYME.AZ has been spotted in the wild

The new year has come with an avalanche of threats that may seriously harm our computers if we don't protect them as we should. JS_PSYME.AZ has been spotted in the wild by security company Trend Micro, which wrote that this malicious JavaScript affects most Windows versions including 98, ME, NT, 2000, XP and even Server 2003. Even if it has only a low overall risk rating and a low distribution potential, JS_PSYME.AZ may reach your computer if you visit a dangerous website equipped with it. In addition, the infection may be dropped by other malware, Trend Micro wrote in the notification published today. "This malicious JavaScript may arrive bundled with malware packages as a malware component. It may also be downloaded unknowingly by a user when visiting malicious Web sites", the security company noted. But what's worse is that it has a medium damage potential, a rating which underlines the JavaScript's capability to harm the data stored on your system. According to the same advisory, the infection attempts to open Microsoft's browser Internet Explorer in order to download additional infections on the affected computer. "Once executed it opens Internet Explorer window and connects to a URL to download a possibly malicious file. However, the site is unavailable as of this writing", Trend Micro added. Just like in 2007, you're advised to keep your antivirus up-to-date, to apply the latest virus definitions and to install the newest patches or fixes for your security applications. In addition, you should avoid visiting suspicious websites that may attempt to deploy dangerous files on your computer. In case you don't have an antivirus or a security solution installed on your system but you're looking for one, you can check the special category listed on Softpedia available through the following [link](#).