

By: ~~April 2008~~ Popa, Security and Search Engines Editor

[Hundreds of Thousands of Websites Compromised](#)

Mass attack JavaScript injection compromises a huge number of pages

Security companies around the world launched an alert concerning a new mass SQL infection which, by the first estimations, had already affected hundreds of thousands of websites. And what's worse isn't necessarily the huge number of compromised pages, but the fact that among the affected ones, we can easily find UN and UK government websites. Most compromised pages can be found using web's search engines and searching for a certain term which I'm not going to disclose especially for security purposes. According to security company [Websense](#), when a visitor loads one of the compromised websites, it attempts to open a malicious JavaScript file called 1.js which is hosted on the main website. Although similar activities were spotted a few weeks ago, the attacks seem to be different, first of all due to the domain used. "Once loaded, the file attempts 8 different exploits (the attack last April utilised 12). The exploits target Microsoft applications, specifically browsers not patched against the VML exploit MS07-004 as well as other applications. Ominously files named McAfee.htm and Yahoo.php are also called by 1.htm but are no longer active at the time of writing," Websense informs. As mentioned, there are hundreds of thousands of compromised websites, most of them being searchable on Google or Yahoo. "There's another round of mass SQL injections going on which have infected hundreds of thousands of websites. Doing a Google search shows over 510,000 modified pages," security company [F-Secure](#) reports. Websense confirms the number of affected websites, too. "The number of sites affected is in the hundreds of thousands," it said. Just as usual, users are advised to keep their antiviruses and firewall open, apply the latest patches and virus definitions and try to avoid websites that look suspicious and may attempt to drop malicious files on their computers.