

30 November 2007

By: Bogdan Popa, Security and Search Engines Editor



The message displayed once a user loads a dangerous link
Sunbelt Blog

Oh, Yeah Baby! More Google Spam Goes Live!

Another spam campaign on Google Search

A few days ago, security experts discovered an impressive spam campaign affecting Google Search that places numerous dangerous links displayed for certain keywords appearing on the SERP. Although the Mountain View company removed the malicious links, Alex Eckelberry and Adam Thomas of the Sunbelt Blog wrote that a new spam campaign was started, many links published on Google being hosted in China. As far as I can see, the attackers attempted to create websites to rank well in Google and, once a visitor reaches the page, he may get infected with a dangerous Trojan/malware/spyware. If a user clicks on a malicious website displayed by Google, he gets a message window asking him to install "Spy-shredder", an antispyware technology supposed to protect users' computers and remove potential spyware files detected on the hard drives. "Which, even if 'cancel' is pressed, you still get a fake scanning page", the two experts wrote. It seems like most of the websites are pretty new as they are "freshly registered". However, we're still safe as most of these pages are not yet infected with any sort of malware or virus. Their only goal seems to be obtaining a high Google PageRank, probably to conduct other attacks in the future. "Right now, we're not seeing either site serve exploits, as we saw in the last attack. However, this could change." Moreover, some of the websites are created with advertising purposes as they display ads just after the visitors click on the malicious links. "It simply shows users a site which is trying to generate traffic (for the purposes of getting affiliate commissions)." Although there is no danger at this time, you're still advised to keep your antivirus up-to-date with the latest virus definitions and avoid visiting untrusted websites and spam results published on the Google SERP. However, I believe the Mountain View company will remove the links as soon as possible.