

8 May 2008



Google Web Search showing infected sites

By: Traian Teglet, Technology News Editor

[New SQL Injection Worm Found Loose on the Web](#)

4,000 websites have been reported to be infected

Not long after a mass attack JavaScript injection was [reported](#) to have infected hundreds of thousands of websites, a new SQL injection Worm was found loose on the web. According to the ISC(Internet Storm Center) website, a total of 4,000 websites have been found infected, after a quick run at a Google search. The report on the above mentioned site clearly states that is unwise to visit the websites mentioned as being infected. They are to be considered dangerous and harmful for your own computer. The domain name "winzipices.cn" can be found in all of the infected websites HTML source. Searching for the above mentioned domain, on a Google search engine, can get your computer infected, even if you are looking at the "cached" page. It seems that the worm was started somewhere in mid-April, if not earlier. At the moment, the fellows at ISC can provide users with a specific information about how the worm gets into the victims' databases. All they can say is that the worm puts in some scripts and iframes capable of taking visitors to the infected websites. Users who have reached these infected sites have most likely been infected through a general vulnerability found in the Real Player. Users are to keep their computer software up-to-date, in order to ensure that they aren't affected by the new threat. Shadowserver.org has detailed how the new threat is working with specific details. Like ISC, the fellows at Shadowserver.org have specifically informed their users NOT to visit any of the presented websites. If the exploits are successful, the users' PCs will be infected with a file dubbed "test.exe", which downloads from a specific IP address, also found on the above mentioned website. The downloaded malware application seems to react in a manner similar to other Chinese malware applications.