

2 July 2009

By: Lucian Constantin, Web News Editor



Torrentreactor
targeted by
cybercriminals
Wikimedia Commons

[Torrentreactor Website Injected with Malicious Code](#)

File sharers targeted through flurry of exploits

Torrentreactor, one of the largest torrent indexers, has been compromised by unknown attackers who injected a hidden IFrame into its pages. The IFrame loads malicious code from a remote server that attempts to exploit software on visitors' computers and infect them with malware.

The incident has been reported by security researchers from web security company Websense. "Websense Security Labs ThreatSeeker Network has detected that Torrentreactor, one of the oldest and most reliable torrent search engines on the Web, has been compromised," they [announce](#).

The exploits loaded from the external payload server target publicly known vulnerabilities in Internet Explorer, Microsoft Office Snapshot Viewer, Adobe Acrobat Reader and Adobe Shockwave Player. If exploitation is successful, a Trojan downloader will be dropped and executed on the victim's computer.

The Websense researchers note that the executable file has an extremely low detection rate, with only two out of 41 antivirus engines available on Virus Total identifying it as malicious. Once installed on the computer, the trojan connects to a botnet command and control server, from where it downloads yet more malware in the form of a rootkit.

The IP of the command and control server has previously been linked to operations of the Russian Business Network (RBN), an infamous cyber-criminal organization. The Torrentreactor pages have been cleaned by the website's administrators, however it remains unclear how many users were actually affected by the incident.

Following the problems that Mininova has been having and the very recent news of The Pirate Bay being sold, users have already begun to flock to other torrent websites such as Torrentreactor, making them appealing targets for cybercrooks looking to increase their pool of potential victims.

It is worth noting, however, that this is not the first time when Torrentreactor falls victim to attacks associated with the RBN. Back in March 2008, independent Security Consultant Dancho Danchev [documented](#) a similar incident involving injected hidden IFrames. At the time, at least 29,300 of the website's pages advertised scareware applications through rogue redirects.