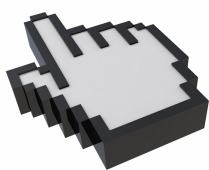


2 July 2009

By: Lucian Constantin, Web News Editor

Highly complex click
fraud trojan discovered
psdGraphics

[Nine-Ball Distributes Complex Click Fraud Trojan](#)

Uses subtle techniques to hijack search results and generate income

Analysts from security company SecureWorks discovered one of the most complex and effective click fraud trojans known to date, while analyzing the malware served by the [Nine-Ball](#) mass injection attack. The trojan, dubbed FFSearcher, leverages on Google's Custom Search widget to generate income for cybercrooks.

The cleverness of this trojan can be observed since the beginning of its installation. "FFSearcher installs itself by attaching to an existing system file as an NTFS alternate data stream," the researchers explain. The Zone.Identifier stream is called when loading the legit netcfgx.dll in order to also load the trojan DLL.

This also means that the trojan does not add any new registry entries. The existent netcfgx.dll one is modified to load netcfgx.dll:Zone.Identifier instead. Upon execution, two kernel drivers are extracted, installed and then deleted. One is used to hide the infection, while the other is employed to inject the payload into the process memory of Internet Explorer and Firefox.

The click fraud is performed by redirecting legit Google search queries through a custom Google search widget created by the attackers. Google Custom Search with AdSense is a legit way for webmasters to generate income by integrating a Google-sponsored search box into their websites. Results to queries performed through these custom search boxes are accompanied by advertisements.

Webmasters receive a fee for every click on the ads displayed along search results, and this is exactly what the cybercriminals want with this attack. "The user never notices any change in their web-surfing experience," Joe Stewart, director of malware analysis, [explains](#), while also noting that Google might also have trouble tracking this sort of fraud.

The trojan's code suggests that Yahoo! Search is also targeted, but researchers note that they haven't been able to trigger a successful attack that redirected search.yahoo.com through a third-party search widget.

"As click-fraud trojans go, this is one of the more clever that we've seen," the Websense analysts conclude. "FFSearcher undoubtedly raises the bar for the fraud detection teams working at the major search engines, and it will be interesting to see how they combat it and other trojans using the same technique in the future," they add.