

17 May 2007

By: Bogdan Popa, Security and Search Engines Editor

Drive-By Download

Is your PC virus-free?

Get it infected here!

drive-by-download.info

The "malicious" advert

If You Want to Infect Your Computer, Please Click Here!*Interesting test conducted using Google's services*

The security researcher Didier Stevens made an interesting test to see how many users can be lured to an infected website even if they know that the page can harm their computer. The procedure was quite simple: he bought an .info domain because they are often hosting malicious pages and placed a simple message saying "Thank you for your visit!". The website was 100 percent clean with no infected file or ActiveX control. Then, he registered to Google AdWords, the advertising platform that allows the users to advertise on the Internet using Google's index and numerous AdSense pages. He chose only some simple keyword combinations such as "drive by download" and started the 6 months test. The advert was displaying a simple message: "Is your PC virus-free? Get it infected here!". The results were quite amazing. "During this period, my ad was displayed 259,723 times and clicked on 409 times. That's a click-through-rate of 0.16%. My Google Adwords campaign cost me only €17 (\$23). That's €0.04 (\$0.06) per click or per potentially compromised machine. 98% of the machines ran Windows (according to the User Agent string)," Didier Stevens sustained on his blog. This is an obvious sign that the hackers might exploit a computer even with the user's approval. Of course, there is one and important question: how many visitors that clicked on the ads were actually looking to test the security of their computer because they were experienced users? In our times, the online security is definitely a problem because the hackers are targeting almost any online protocol, including HTTP, FTP, instant messaging clients and even the applications installed on our computers. In the recent period, the security advisories revealed that even a simple compression tool such as WinZip or an audio player like Winamp can allow an attacker to connect to our system.