Hundreds Click on 'Click Here to Get Infected' Ad

May 19 2007

The fact that 409 people clicked on an ad that offers infection for those with virus-free PCs proves that people will click on just about anything.

People will click on anything. That was evidenced by the 409 people who clicked on an ad that offers infection for those with virus-free PCs. The ad, run by a person who identifies himself as security professional Didier Stevens, reads like this:

Drive-By Download
Is your PC virus-free?
Get it infected here!
drive-by-download.info

Stevens, who says he works for Contraste Europe, a branch of the IT consultancy The Contraste Group, has been running his Google Adwords campaign for six months now and has received 409 hits. Stevens has done similar research in the past, such as finding out how easy it is to land on a drive-by download site when doing a Google search.

In a posting about the drive-by download campaign, Stevens says that he got the idea after picking up a small book on Google Adwords at the library and finding out how easy and cheap it is to set up an ad.

"You can start with a couple of euros per month," he said. "And that gave me an idea: this can be used with malicious [intent]. It's a way to get a drive-by download site on the first page of a search."

First, Stevens bought the drive-by-download.info domain. .info domains are notorious for hosting malware, he points out. Then he set up a server to display the innocuous message "Thank you for your visit" and to log the requests.

No PCs were harmed in this experiment, he emphasizes. The site is benign and has never hosted malware or other scripts or code. Then he started the Google Adwords campaign, using combinations of the words "drive-by download" along with the ad, which links to the drive-by-download.info site.

Next, he sat and waited … for six months.

Over that period, his ad was viewed 259,723 times and clicked on 409 times, for a click-through rate of about .16 percent. The experiment cost him $23, or 6 cents per click/potentially infected machine.

Of the 409 people who clicked, 98 percent were running Windows machines, according to the user agent string, which is a text string that identifies a Web site visitor to a server. The agent string typically includes application name, version, host operating system and language.

This is the breakdown for the browsers that were used in those 409 clicks:

IE 5.5 1
IE 6.0 286
IE 7.0 48
Safari (419.3) 1
Opera 9.01 1
Opera 9.10 1
Firefox 1.0 7
Firefox 1.5.0.7 9

Firefox 1.5.0.8 2
Firefox 1.5.0.9 3
Firefox 2.0 3
Firefox 2.0.0.1 6
Firefox 2.0.0.2 1
Firefox 2.0.0.3 21
SeaMonkey 1.1 2
AdsBot-Google 24

Total 416

Stevens found a discrepancy of seven hits recorded by his logs but not reported by Google. He believes those seven click-throughs might have come from bots that Google filtered out. Bots often include a URL and/or e-mail address in their user agent string so that a Webmaster can contact the botnet operator.

Stevens says that he designed his ad to make it look fishy, but he had no problem getting Google to accept it and has had no complaints to date. And, although a healthy amount of people clicked on it, he said there's "no way to know what motivated them to click on my ad. I did not submit them to an IQ-test."

The reason for running the experiment and publishing his results now is that this technique of putting up ads for what turns out to be drive-by downloads is being used in the wild. For example, the popular geek hardware store Tomshardware.com discovered a Trojan, hosted out of Argentina, lurking on one of its banner ads earlier in May.

Stevens has posted a video of Google showing his ad here on YouTube.

Stevens said he's sure he could get much more traffic if he invested more in his Google Adwords budget and came up with a better designed

ad.