

Another Tactic of Viruses

Posted by Wade Burchette on February 3, 2010

This is from McAfee labs about a new technique computer viruses are using. This one embeds itself in a help file. I've seen viruses in executable files (.exe) and in library files (.dll). Now viruses have another place to hide: help files.

A computer virus is a bit of code that is embedded into a file and when that file is executed, the virus executes some code and often spreads itself. In this case, once the infected help file is viewed, the virus installs some malicious program. The malicious program is just an encoded file with a file extension of .hlp to make it look like a help file. The purpose of this is to foil anti-malware programs.

All of this just illustrates the point that malicious software will always change tactics to stay two steps ahead of the cleanup programs. Fortunately for you, the motivation behind most malware is profit. This means that most malware is not this complex because that is too much work. These cyber-criminals want as much as they can as fast as they can. Complex malware like this take a long time. Still, never assume you are safe. I've said it before in other blog posts, not even Macs are safe. About 80% of the malware I see is a simple scam, the fake antivirus stuff. And that is relatively easy (for me anyway) to remove. Just always be alert. Being alert can foil most of the cyber attacks.

If you like more information on this new virus tactic, McAfee has a blog entry about it: [Be careful on help file](#).

Last modified: 2010-02-03 19:31:41.0

Permanant Link: <http://www.techs-on-call.biz/blog/post.cfm/another-tactic-of-viruses>