

Study: Antivirus Software Not Effective At Stopping Malware

Posted by Wade Burchette on February 8, 2010

A company called Surfright has just released a [study](#) from users who visit their website to remove malicious software, or malware. Even up to date antivirus definitions. One quote from the study from cyveillance.com says that "Even the most popular AV solutions detect less than half of the latest malware threats." VB100, a company that tests antivirus products, says "A few renowned anti virus programs do not pass the VB100 test."

All this confirmed what I already knew: Your antivirus program won't protect you from the biggest threat today, malware. From personal experience, the malware I see the most is fake antivirus programs. I see this a lot because it is profitable. Of course, fake antivirus programs are easy to remove. The idea behind fake antivirus programs is to make as much money as you can as fast you can; burying itself deep is too much work. Also from my experience, malware in Windows Vista is more likely to be confined to a specific user. What this means is that if a computer has more than one sign in name, it is more than likely to be limited to one of those users with the other user unaffected. Windows XP is more likely to have every user affected.

I rarely see viruses or worms anymore. Of course, what is called a virus is not a computer virus. A virus is a program that can spread itself through various means and requires a host program. A worm is like a virus except that it does not require a host program. I saw the Conficker worm recently and last year my brother had a virus in his NVidia video card driver. Viruses and worms still exist and are still rampant, but they aren't as profitable and so the cybercriminals are shifting their focus into something that can make money. Antivirus programs do a fine job at detecting viruses, but even the best antivirus program is weak at detecting malware.

The study just confirms all that. Starting on page 12 of the study, of the 107,435 users from October 10, 2009 to December 4, 2009 who asked SurfRight to scan their computer, 25,308 of the users had antivirus installed and were infected. 78,828 of those 107,435 users had installed an antivirus program, so those 25,308 users represented 32% of all users

with antivirus programs installed were infected. Granted, these numbers will be higher than the real-world results because people visit SurfRight when they think they have a problem.

The most important thing from this study is this: Never assume you are safe. It doesn't matter if you have antivirus software or are using a Mac or are up-to-date with security updates. Never assume you are safe. Complacency can cost you.

References: [Hitman Pro 3 Real-World Malware Statistics, October/November 2009](#)

.....
Last modified: 2010-02-08 16:33:24.0

Permanant Link: <http://www.techs-on-call.biz/blog/post.cfm/study-antivirus-software-not-effective-at-stopping-malware>