

DO I NEED ANTIVIRUS AND ANTI-MALWARE SOFTWARE ON LINUX

Many would say, and often do, that there is no need to run antivirus software on Linux. Even I subscribed to the idea for a while. Two of the reasons behind that thinking: 1. Linux doesn't allow software to run as administrator without the user giving explicit permission. 2. The Linux community can, and routinely does, respond more quickly than the developers of proprietary software to identify and patch vulnerabilities. After all, as commenter "Jimmy" responded to an article proclaiming that German antivirus company Avira has scrapped it's Linux offerings, "You can keep a database of malware signatures or you can fix the exploit hole... Mostly Linux folk prefer the latter."

But the more I learn about these nasty pieces of malicious code, the more I see things a little differently. I have come to realize that, although we don't currently see infections on Linux, we should be using anti-malware software on Linux. This is partly as an insurance policy against future Linux-specific malware, and partly because we need to be ensuring that we don't become "carriers" of the infections. After all, we don't want to be passing on Windows viruses through our electronic communications, to our Windows-using friends.

Even though there are no Linux viruses in the wild, there are trojans, worms and other varieties of malware that can get on our Linux computers via security holes in applications or browser-based software. Also, the more our lives move to "the cloud" the more likely there will be malware that runs in cloud applications, gets transmitted from one cloud user to another, and NEVER gets installed on the host machine -- Windows, OS X, Linux, BSD or something else!

How bad is it, really?

According to the 2012 2nd quarter report from Panda Security's Collective Intelligence (<http://press.pandasecurity.com/press-room/reports/>) on average, over 31% of computers world-wide are infected currently infected with some sort of malware. That means that if you and your spouse site down for dinner with two other computer-owning couples, two of the six people at the table have infected computers! Although the report does not mention computers running Linux, it does mention that in 2012 there were an estimated 600,000 "FlashBack" infected Mac OS computers.

Currently 31% of computers world-wide are infected. What you see above may be in our near future. (Which OS would you rather use?)

Combining the Panda Security numbers with the market share numbers from NetMarketShare.com, the worlds's infected Windows computers number over 3.5 times all Mac and Linux computers combined! Does that mean that if you stop any random computer user on the street, they are over 3 times more likely to own an INFECTED Windows computer than to own either a Mac or a Linux computer? Yep!

What Can I Do To Minimize The Threat of Computer Malware?

In order to minimize your computer's likelihood of getting infected, you should be using a Mac or Linux. Choose a Mac if you want to spend more money, have less control, and have fewer choices. Choose Linux if you want to use your existing computer hardware, or if you want to spend less money, have more control, and have more freedom and choice. In fact even on Mac and Linux computers, to truly minimize your risk, you should choose to install only applications that are designed specifically for your operating system. It's simple logic. If you want to avoid getting infections targeted at the Windows OS or Window applications, don't use Windows applications! Don't use Windows, don't run WINE, don't dual boot, and don't run Windows in a virtual environment like Virtual Box, VMWare or Parallels.

In my opinion, do you need to install a piece of bloated, commercial software that checks for things that don't exist onto your fast Linux machine? No. Not yet. Should you ensure that your Linux computer is completely up-to-date and that all of your installed applications have the latest security patches? Absolutely! Also, I'd recommend that you use Gmail to filter malware-carrying spam from your in-box, and ensure that your home computer is behind a router (firewall). You should also install the light-weight ClamAV from your distribution's repositories, and run it occasionally to ensure that you are not spreading Internet germs to your friends running the other, sickly operating system.

Source : http://goinglinux.com/articles/AntivirusonLinux_en.htm