

# TROJANS

There is a lot of confusion around the whole issue of what the different kinds of security threats are to your PC. What is a virus and is it more dangerous than a trojan? What about a worm? The differences are quite varied, but actually end up being merely technical. What is really important to understand is that they almost universally require user participation to spread. Trojan Horses are a great example of this.

Trojan Horses are impostors--files that claim to be something desirable but, in fact, are malicious. That cool game that a "friend" sent through MSN, or that downloaded song that is only 120 kb in size could very well be a trojan. A very important distinction between trojan horse programs and true viruses is that they do not replicate themselves. Trojans contain malicious code that when triggered cause loss, or even theft, of data. They can also install "zombie" programs that turn your PC into a server for some other malicious purpose, like causing a denial of service attack on an important domain. For a trojan horse to spread, you must invite these programs onto your computers--for example, by opening an email attachment or downloading and running a file from the Internet. Trojan.Vundo is a trojan.

Trojan.Vundo has been cropping up a lot here at the shop lately; we have probably processed 80 PCs in the past few weeks with this particular bug. If your machine fires up, gets to the desktop and then hangs without displaying all the icons or giving you full access to Windows, you may have Vundo. As it turns out, Trojan.Vundo is a trojan that is primarily installed when people click on a web link in a spam email, so it is not file based like other trojans. As you may recall, spam is unsolicited bulk email, generally sent out to advertise to the unwary masses. If you click on a link in a spam email you are asking for all kinds of trouble, not just the trojan kind. When you click on the link you are led to a website that attempts to install the trojan on your PC, which you also have to give permission to. This particular trojan requires user participation TWICE and yet people still install it. Admittedly, up-to-date antivirus software or resident spyware software may be able to stop one from making this terrible mistake. But does it not make more sense to be adequately cautious and just not install these things?

This morning I received three malicious emails, one apparently from Paypal, one apparently from the Bank of America and one apparently from myself. All three were fraudulent about who they were from. The first two were phishing attempts, emails that are meant to lure the unwary user into typing their account information into a website. I am not that stupid, so I deleted them out of hand. The third was more interesting, since it was supposedly from me. There was no message body, but there was an attachment. Again, I didn't bother opening it; I merely deleted the message. SaskTel's Postini service stopped 32 other spam messages for me over the weekend along with 6 virally-infected messages, but nothing is perfect, so these three messages got through.

Nothing works nearly so well as a little education and common sense.

If you have question or comments, I can always be reached via email [sean@intrex.ca](mailto:sean@intrex.ca) or join our forums at <http://intrex.ca> for more in-depth conversations.