

Spyware, Viruses, & Worms - Oh My!

A few weeks ago, an associate (Dorothy) asked me for help with her laptop. Dorothy's laptop (Glinda) was hijacked and no matter what she did - it kept taking her down the yellow brick road to some website in eOz she certainly didn't want to go to.

Glinda was used to help Dorothy run her small business – thus a format and reload of the operating system was an option to be avoided. Given the criticality of Glinda, I agreed to try and repair it for her over the weekend.

Upon entering the infected system, I found myself in a tornado of viruses, spyware, and worms linking to wicked witches' servers all around the globe. One of the worms was a real flying monkey, as it was connecting to a whole bunch of other flying monkeys - causing the entire system to fall into what looked like a state of unconsciousness.

I had little choice but to reboot and run the computer in Munchkin mode – commonly known as SAFE mode. In this special mode, I was finally able to communicate with Glinda and run some trusted ruby red programs to help determine just what kind of lions, tigers, and bears were running loose.

Eventually, after hours of trials and tribulations I was able to conquer the Wicked Witch of the West and send Glinda back to Dorothy with a clean bill of health. Things seem to be going quite well in Kansas for just over a week until Dorothy called to say “they're back”....

After an interesting conversation, I learned that Dorothy's husband Toto also had a computer at home sharing the broadband connection. Toto's computer was clearly infected and eventually the flying monkeys were able to revive the Wicked Witch of the West. Does “I'll get you my pretty” sound familiar about now?

So how does this story end? Dorothy and Toto are saving key documents and will be formatting both systems with the original installation disks. Once they have clean systems, they'll start down the long winding road of updates, re-installing programs, and copying files. Clicking their heels three times - just won't bring their PCs back.

What can I do to keep my system out of the land of eOZ? 1st and foremost, install and keep updated a leading Antivirus program. Even if it “automatically” updates itself – you need to manually check for updates at least once per month – if not per week. 2nd, if you have a newer system with lots of CPU and RAM – install another “free” antivirus program, as no single antivirus program will stop every flying monkey. 3rd, consider not using Outlook or Outlook Express as your primary email applications.

Ok, I think I'm catching 99% of the monkeys – what about Spyware? The simplest answer is to use a non-Explorer browser – thus most of the spyware will not be able to infiltrate the Explorer software. There are really good alternatives and without mentioning any names - one sounds like Gorilla. Also, employ an “active” Anti-Spyware package that let's you know when something is trying to throw a monkey wrench into your system.

Worms & Trojans are just another virus aren't they? Yes and No. Worms and Trojans are another class of nasty programs that try to attack your system through open doors or ports on your computer. Thus, your system really needs either a software or hardware Firewall to close the ports to the outside world. If nothing else - install an inexpensive Router with NAT, to hide your system(s) while the Worm goes down the block to your neighbor's house.

In closing, defending your system in 2005 requires a multi-layered strategy. *Why?* In 2003, any PC connected to the Internet could be attacked in less than an hour. In 2004, three times an hour. In 2005, will nine or twelve attacks per hour scare you? No single program (or device) can protect an “Internet-connected” PC from the imagination of mankind, the diversity of the Internet, and the speed of the electron.