

Distressed client called Thanksgiving evening and asked me to take a look at his computer. He was correct when he said he had a virus. He did have a computer virus that is the worst I have seen so far. Here is what I did to get his PC back into operation:

Main issue: severe virus infection.

Upon booting, virus popups appear and machine will not go past wallpaper display.

Task Manager is prevented from running.

Machine will not boot to Safe Mode.

Booting from a CD containing PE Builder software. Now I can see the file system.

Removing Spybot- Search & Destroy files. Nope, system will not allow file deletion, so just renaming them by prefacing them with "pjs-". Renaming is often better than deleting because the file can be recovered if needed simply by renaming it back.

Renaming Registry Mechanic directory.

Renaming Spyware Blaster.

Renaming AdvancedVirusRemover. This one is really suspicious.

Renaming Symantec

Renaming Uniblue folder that has RegistryBooster2 within.

Attempting to use PE Builder to make backup of Documents and Settings folders to a huge external disk drive. This long processed failed twice because PE Builder balked over some long filenames.

Attempting to use Spotmau to make backups to external disk drive. This 3-hour process succeeded and now I can aggressively attack the virus. You can learn more about Spotmau via Google.

Making DVD copy of the backup files for extra security.

Discussion: The folders under the Documents and Settings folder contain such things as a user's email address book, his email messages, his favorites, photos and any other kind of personal files. If I need to reinstall windows, I will be able to recover this important data from the backup.

The typical path to an Outlook Express address book is
C:\Documents and Settings\UserName\Application Data\Microsoft\Address Book.

The typical path to an Outlook Express message store is
C:\Documents and Settings\UserName\Local Settings\Application Data\Identities\{A47FC4DA-5DAD-4DDF-BF25-76A8CABC0188}\Microsoft\Outlook Express (the {filename} will vary).

Using Spotmau, overwriting the MBR (Master Boot Record) in case the virus has damaged it. Then rebooting for test. Did not work. Virus still displaying its startup window, task manager is still disabled.

I really do not want to reload the whole operating system, so will work awhile to enable the Task Manager. If I can get the TM to work, I may be able to spot the virus files. Was unable to get the

Task Manager to load. The operating system's registry is too badly damaged.

Using the Spotmau tool to replace the current registry files with generic registry files. This should kill the virus, but we will need to reinstall lots of programs. Rebooting.

None of the above worked, restoring file system back to new condition. We will restore the personal files after all else is functioning. I hate to do this.

After two 45-minute attempts using Windows installation disks, have Windows running. Downloading and installing updates to operating system. This will take a few hours and many reboots.

Being quick to install free Microsoft's Security Essentials anti-virus program. If this had been running, the virus problem probably could have been avoided. Nope, it will not install until Service Pack 2 had been installed.

Installing Windows XP Service Pack 2. This is a major operating system upgrade. It installed without problem.

Now installing Microsoft's Security Essentials.

Discussion: I used to push Avira anti-virus and have perhaps 200 installations here in Sun City without any problems. I used it myself. Now, I like Microsoft's Security Essentials. MSFT take a lot of heat about operating system security and got tired of not being adequately protected by third party companies, so it reluctantly developed its own software and made it a free part of the operating system. Stock prices in companies like Norton, Computer Associates, McAfee, etc, dropped 30% within an hour of MSFT's announcement.

Security Essentials is installed and doing a system scan. It shouldn't find anything since this is a new, clean operating system install. The MSE scan finished without problem.

Discussion: When users have a troubled system, they often search the Internet for magic bullets to cure their problems. This is a big mistake. Many of these anti-malware programs are viruses themselves. Even legitimate programs will conflict with one another if more than one is installed. A good anti-virus program will cover all bases.

Back to OS updates. MSFT wants to install SP3, the latest update. This is a major, major update. It is after midnight and I'll let the update cook by itself. I'll have to wait to click on an OK box first. SP3 installed without problem.

Many updates to the operating system are downloading and installing.

Creating Outlook Express email account on laptop. Restoring email messages and address book from backup files.

Restoring personal documents from backup disk.

Reloaded Microsoft Office including Word and Excel.

Reinstalling Google Earth

Reinstalling Kodak EasyShare.

Still to come: Installing printer and cameras.

\$75, Thank You.

Paul J. Shane
705-2178
pjshane@suncitypeople.com

TELL YOUR NEIGHBORS