

# The constant battle with Malware is frustrating



John Deans

My workday has transitioned lately to battling Malware at a higher rate and on a more destructive level. Over the past couple of months it seems like client calls about new threats and slow computers has doubled.

The war against Malware has really heated up since the spring.

Malware includes all the bad stuff that has a negative effect on your computer. These digital gremlins include viruses, spyware, crimeware, rootkits, phishers, spam and even mobile threats.

Remember the good old days when we only had to worry about viruses coming in through our e-mail? We still do but most anti-virus software now does a very good job blocking them. As long as the virus definitions are kept updated you should be OK. Most antivirus programs now check for new definitions multiple times a day rather than only once a day.

My AVG Antivirus version 8.5 checks every four hours for new virus information and definition updates. The old 7 version only checked once a day and that hurt me at a big client last year. With fast changing

and quick moving viruses, timely definition updates are absolutely critical.

Spyware infections have really exploded this year and they have become more detrimental to Windows-based computer systems. They not only watch your

every move on the computer but they may also be trying to capture and transfer personal information to bad guys on the other side of the world.

It is no longer viable to run your PC without anti-spyware to assist your anti-virus software to keep things clean. When I have a new computer to set up, I immediately install and update the antivirus software which is AVG Antivirus from Grisoft.com. Next I manually run Windows update to get all the latest fixes, patches, and service packs from Microsoft.

Next I download the latest version of Spybot which is at release 1.6.2 from Safer-Networking.org. During the installation I uncheck all the add-ons like skins and additional languages along with disabling the installation of the Tea Timer since that is too intrusive to the system's registry.

After the installation of Spy-

bot is done I update it right away and make sure the program re-starts with those new spyware definitions loaded. From there I go to the immunize button and have Spybot immunize my computer to prevent spyware invasions as a proactive measure.

Phishers and spammers are still trying to send us bogus e-mail messages to fool us into divulging our personal information. Please do not fall for those even though some look very official and may even have your bank's logo on it.

Crimeware has been a problem for years now and is even more prevalent with both the Chinese hackers and the Russian mob trying to steal from us. These digital gangsters utilize key loggers that can watch every keystroke you type on your keyboard.

When logger recognizes a credit card or bank account number it ships that stolen information to overseas servers within seconds.

Once that happens it is sold on the black market and by the end of the day bogus charges are hitting your credit card or bank account from all over the world. Running daily virus and

spyware scans with reliable and updated antivirus/antispyware software is the only way to stay safe if you want to live in today's high tech environment.

Rootkit viruses are the worst. They get deep inside the Windows operation system and become almost impossible to find and extremely difficult to remove.

Computer Helpers and I have spent hours and hours trying to clean a single PC. Since we limit the charges on a single infection event, these harsh computer virus outbreaks are big time money losers.

Recently I spent six hours trying to remove multiple infections from a single computer but I only charged the client a fraction of my time battling the frustrating Malware. Sometimes the infections are so widespread and such damage has already been done to the system registry and software installations that I have to abort the cleanup operation and initialize the whole computer.

This complete reload requires backing up the data, formatting the hard drive, reloading Windows and all drivers, re-installing all applications and finally

importing all the backed up data. This can take one to three hours depending on the number of programs that were installed and how accessible the installation CDROMs are at that time.

At least with a complete reload I know I'm going to be done soon. With Malware cleanups you may be done in 30 minutes by a single scan/repair from ComboFix or you could be there the whole night with things still going wrong.

Some outbreaks are so severe that I cannot even load the anti-virus or anti-spyware programs to fix the problem.

Another good thing about full system reloads is that the computer really runs great after it is all completed. With fresh software newly loaded in a non-fragmented state that is free from Malware of any kind, the rebuilt system is very snappy with no odd behaviors.

One big point I need to make is take care of the problem before it gets bigger — because

it will. I have had clients call me after their system is basically unusable. What really bugs me is when they tell me that threats were showing up for several weeks prior but they decided just to wait. By that point it is quicker just to wipe out the computer and start from scratch.

If they had called me when the first hint of a problem showed up I could have run a single scan/repair process that could have fixed their problem in 15 minutes. Pay me now or pay me more later.

Bottom line: The battle against all forms of Malware continues, so stay vigilant and fight the good fight.

Next week's column: Risky search terms.

*John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.*