

Malware – It's Already On Your Computer!

By Gregory S. Michaels

It comes as no surprise that cyber thieves are out to steal our personal information and corporate secrets. What is surprising is that a recent report from the research firm GartnerG2 claims that more than 20 million computers have some sort of malware installed and the report covers only a subset of the many forms of malware on the loose. Personally speaking, I have never sat down at a client's PC and not been able to find some malware. Besides the obvious threat to your privacy and personal information, malware can also cause system instability, performance problems, and even crash your system. So, what exactly is malware? How did it get on your computer? And most importantly, how can you get rid of it?

The least threatening type of malware, also referred to as adware, comes from Internet advertisers. It consists of small files called cookies that are left behind on your system while surfing the net. Adware attempts to track and report back to the advertisers on your Internet surfing habits. The intent is to develop a demographic profile of you so that targeted pop up ads can be delivered during your Internet surfing sessions. Simply visiting a web site can provide a tacit agreement to the sites privacy policies including the acceptance of the adware cookies. Advertisers claim they do not track individualized information. However, by following up with an e-mail that includes a "web bug", advertisers can associate a tracking cookie with an individual. Of course, most advertisers would deny using this technique.

More threatening forms of malware include key loggers, system monitors, and Trojan horses. A key logger can record anything you type including passwords, email messages, real time chats, and credit card numbers. The information can be stored locally or even sent out silently via email. System monitors can literally spy on you through your own webcam. Trojan horses can do just about anything including taking remote control of your computer as well as monitoring your activities. Some other common manifestations of malware include hijacking your Internet browser's home page, changing your default Internet search engine, adding web sites to your browser's favorites list, and even blocking access to some web sites.

It should be obvious by now that a lot of malware gets on your system from surfing the net. However, this isn't the only source. Malware can be installed by anyone with access to your computer. It can be delivered via email disguised as something useful or it may have even been included with your brand new computer. Many times free software (freeware) comes bundled with malware. By downloading or installing the freeware you have agreed to the "terms and conditions" which includes the installation of malware. File sharing freeware popularized by the trading of MP3 music files is perhaps one of the worse perpetrators in the free software arena with some installing over a dozen malware programs along with their freeware. In a sense you are paying, but the currency is privacy, not dollars.

Once malware is on your system it will begin to eat up system resources as it monitors your activities and reports back to its spymasters. Some malware even gets loaded at startup and runs continuously behind the scenes hoping to remain inconspicuous. As your PC accumulates more and more malware the effects on system performance can become noticeable and may even result in complete system crashes or the dreaded "blue screen of death". Many times the system problems that arise are misdiagnosed as a virus.

The best way to protect against malware is to use software programs designed and developed specifically for the task. These programs work much like anti-virus software by searching for known malware files, folders, and system registry keys and allowing you to remove them. However, the process is not always that simple. Just like virus developers, malware developers are continuously trying to stay ahead of the malware removal tools. Some malware is smart enough to reinstall itself after it has been removed. Other malware that comes bundled with freeware may disable the freeware it came with or will prevent removal as long as the freeware is installed. A malware removal program is more likely to be able to eliminate these types of offenders.

Beyond the periodic use of malware removal software, there are some other precautions you can take to prevent malware from infiltrating your system. Turning up your Internet security settings to at least medium or higher will produce warning dialog boxes before any potentially risky programs or cookies are installed. If you didn't ask for it don't allow it. Make sure you read all software and end user licensing agreements carefully to make sure you are not agreeing to install any questionable bundled software. Using a hardware or software based firewall configured to detect any outbound activity will alert you of suspicious outgoing traffic. Get educated on which software applications are known to compromise your privacy. And last but not least, always keep your anti-virus software running and up to date.

By Line:

Gregory Michaels is President of TekTrek Computer Services providing on-site computer services for home and business. For more information email info@tektrekcomputer.com or call 303-438-9365.