Malicious Software Guide

Prepared by Asadoorian Consulting

The Internet has become a vital tool for just about everyone. All sorts of information can be found with a few simple clicks. Through the years however, users have had one main concern when surfing the web; computer viruses. Computer viruses have traditionally caused noticeable damage to a computer's software or the documents/files contained within. But in the last few years a new threat has emerged. This threat is not easily seen. Unlike viruses, this threat appears to be more annoying than harmful to the end user and often times it blends in so well that it is undetectable to the average user. This category of threat is referred to as Malicious Software by *Asadoorian Consulting*. Malicious Software can usually be broken down into two sub-categories, Spyware and Adware. This guide explains what Malicious Software is and how one can reduce the risk of exposure to it.

Adware

Generally speaking adware is a form of software that is installed on a user's computer in order to monitor the web sites a user frequents. Based on the user's website usage/preferences, the adware software serves specific advertisements tailored to the user's web-surfing habits. These advertisements can appear in the form of pop-ups or even appear within your browser looking like actual content. For instance, when searching the web through Google or Yahoo, adware software may insert advertisements or "sponsored links" directly into the browser, making it appear as though the links are part of the search results. Furthermore, some adware will present ads when a user is not surfing the Internet and their browser is closed. These types of advertisements appear in the form of pop-ups. The motivation behind adware producing companies is that they get paid each time a user clicks on one of the pop-ups or sponsored search results.

Spyware

Spyware is a more advanced and evolved version of adware and is usually more dangerous. Spyware will generally monitor your Internet surfing habits to deliver targeted advertising (similar to adware). But spyware can also capture your keystrokes and other personal information. In addition, spyware will sometimes "hijack" your browser, directing it to websites the user did not request. The most severe cases of spyware will result in the remote control of your computer by someone else. In other words a person anywhere in the world can control your computer and see its contents. In the end, identity theft can result.

Contracting Adware and Spyware

There are a few ways in which malicious software can be installed on your computer. For adware to be installed on your computer, it is usually bundled with free programs that people want. The adware installation is normally discussed in the End User License Agreement for the free application you are installing, but most people rarely read the fine print. Common free applications that contain adware are file and music sharing programs (peer-to-peer applications) that promise free music and movies or free screensaver/weather programs. Of course these types of software are just an example, there are hundreds of other types of not-so-common free applications that contain adware.

Spyware can also be installed in the same fashion as adware, but often times it is not. Rather spyware will take advantage of security vulnerabilities found in Internet Explorer or Windows and install automatically through those vulnerabilities. Generally speaking, all the end user has to do to is surf to a website that takes advantage of such a vulnerability. Often times, websites promise free pornography, music, movies and applications to entice an end user to visit such sites. Once the end user clicks on to the website, the website will look for a number of vulnerabilities and install automatically without the end users knowledge. The next time your computer is restarted, the spyware application becomes active.

Keep in mind that once malicious software is installed on your computer, it will often times lead to hundreds of other malicious software being installed on your computer. Some installations of such software open up a “back door” to your computer that allows just about anything to be installed on your computer. The end result is that your computer becomes infested with hundreds (if not thousands) of individual malicious software applications.

Visible Common Effects of Malicious Software

- Pop-ups (even when your Internet browser is not open)
- Slow running computer
- New homepage
- Additional toolbars in your browser
- Error messages
- Damage to the operating system

Protecting Your Computer from Malicious Software

Protecting your computer from these threats requires steps to be taken from the first day of your computer’s ownership. Just as there are applications to protect your computer from viruses, there are applications available to protect from malicious software. One such application is available for free from Microsoft (http://www.microsoft.com/athome/security/spyware/software/default.mspx). Unfortunately, no one application will protect your computer from all malicious software but having a good one will significantly reduce your exposure to it. In addition to such software, your operating system (Windows) needs to be kept up-to-date with security patches that Microsoft offers. Your computer can be configured to automatically download and install such patches as soon as they are available. Any delay in installing these patches can lead to malicious software attacks against your computer. Finally, as a computer user you must be very careful about which applications you install on your computer (whether free or not) and which websites you visit. Even with the best protection an end user can still install (knowingly or not) malicious software by visiting unknown websites and installing applications they are not familiar with.

What To Do If You Have Malicious Software Installed

Due to the advanced configuration of malicious software, often times once such software is installed and present on your computer removal becomes very difficult if not impossible for the average computer user. The easy steps to attempt when such an issue occurs are to uninstall all unnecessary applications from Add/Remove Programs in the Control Panel (make certain that you are not uninstalling applications that came with your computer or applications that you normally use). This may remove some of the malicious software. In addition, a full scan can be run through your malicious software protection and removal tools. These scans will normally result in detection of numerous entries of malicious spyware. Once the scan is complete, you will be presented with an option to remove the software in question. Please keep in mind that generally speaking, such tools are incapable of removing all malicious software. In addition, removing certain malicious software may render your computer unstable or unusable (due to how certain malicious software is installed). This is why expert troubleshooting and repair is often necessary to remove such software. At *Asadoorian Consulting*, we often have to manually remove each and every component of malicious software because if not done correctly the malicious software will return. This manual process can take anywhere from two to five hours. Please contact us for more information.

More Information

- Federal Trade Commission's Consumer Alert about spyware: http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm
- Information and resources from Microsoft for spyware: http://www.microsoft.com/athome/security/spyware/default.mspx
- Microsoft Windows Update: http://windowsupdate.microsoft.com/

For any questions, please don't hesitate to contact *Asadoorian Consulting:*

- Phone: 818-636-7360
- Email: info@mike5.com
- Website: www.mike5.com