David W. Potts Consulting

Personal Computer and Electronics Consulting
4945 SE Casa Del Rey Drive
Milwaukie, Oregon 97222
Telephone or Fax: 503.659.5588

Spybot Resident "Tea Timer" Component

Spyware, scareware and other malicious software can be installed to automatically run when your computer is booted. These items can also be designed with "self-preservation" techniques that will allow them to reinstall themselves, even after they are uninstalled, making eradication difficult.

Spybot Search & Destroy includes a "resident" component called "Tea Timer" that sits in the System Tray (the area of the Windows Task Bar opposite the Start button, where the digital clock resides). The Tea Timer icon looks like this:  .

The Tea Timer component of Spybot "watches" for programs trying to make changes to the System Registry (where many pieces of malicious software install components), warning the user when changes to the System Registry are being requested.

Although there are legitimate changes to the System Registry that can be made by programs (such as changing settings or adding or removing software), you should be suspicious when you are doing something like simply typing in a word processing document and Spybot's Tea Timer detects a request to change the System Registry. If you are not changing settings or adding or removing software, it is likely malicious software is requesting the change to the System Registry. In this event, you can select to "deny the change". If, on the other hand, you are making system changes, you will likely need to "allow the change". If, after denying a change, there are no negative ramification seen, and the same change is continually requested, you also have the option to have Spybot's Tea Timer "remember the decision", so it will deny the change without continually asking your permission.

The Spybot Tea Timer component can also perform some background tasks. When it does, you may see the lock icon (which is usually at the bottom left corner of the icon) moving, clockwise, around the Tea Timer icon. During this activity, you may notice your computer slowing significantly. After a few minutes, the Spybot Tea Timer activity should cease and your computer should return back to normal.

There is a particularly pesky type of malicious software called "scareware", also known as a "rogue antivirus" or "rogue antispyware" application, that can create a pop-up window with a legitimate looking message like "Viruses and spyware have been found on your computer. Click below to load ***the name of the malicious software*** to scan your computer." Once you click to load the software or run the scan, your computer is infected. Scareware sometimes lists items "found" on your computer. These are usually "false positives", meant to scare the user into accepting the installation of the software or initiation of a scan. Once infected, many of these pieces of malicious software employ self-preservation techniques, making them next to impossible to remove. Some offer an uninstaller, if you send money to their author. Some state that, after they run their "scan," you must pay for the "fully licensed product" to remove the items "found".

I have seen malicious software that, even when you select to NOT allow installation, they will install anyway (clicking anywhere in their pop-up box causes their installation). I have also seen malicious software whose pop-up box will not close by using the Close button (the red "X" at the top right corner of the window). If you cannot close the pop-up by using the Close button, you may need to close the task from the Task Manager, accessed by depressing <Ctrl> + <Alt> + <Delete>.