Title:
Smitfraud

Word Count:
365

Summary:
SmitFraud is a type of spyware application that is capable of installing itself in your computer through an adware. It has the technical name W32/SmitFraud.A.

Keywords:
Smitfraud

Article Body:
SmitFraud is a type of spyware application that is capable of installing itself in your computer through an adware. It has the technical name W32/SmitFraud.A.

Since SmitFraud is classified as a spyware program, it can intercept and even have direct control over your interaction with your computer. Aside from this, it can also monitor your computing activities without your consent.

You can acquire SmitFraud via the installation of a codec that has been obtained from an unsafe source. You can also get the SmitFraud spyware from certain programs and from files that you have downloaded through torrents and peer-to-peer applications. Once it is installed into your computer, SmitFraud will:

- alter your registry;

- deactivate the Regedit utility;
- and disable your Task Manager.

This type of spyware can infect your Windows DLL files with a virus. The common indication that your computer is infected by SmitFraud is when it shows a fake “Blue Screen of Death” in its desktop background. In addition, SmitFraud is used by its developers in order to create fake alerts from certain software. It then informs the user that the computer is infected and that he or she needs to download and install a particular rogue antispyware application.

In order to remove SmitFraud from your computer, the first thing you can do is to update your antispyware application and perform a thorough scan of all drives. If you do not have an antispyware installed on your PC, you really need to purchase one and install it immediately. Spybot and XoftSpy are examples of antispyware programs that can remove certain variants of SmitFraud. However, if your antispyware application cannot get rid of SmitFraud from your computer, your last resort would be to reformat your PC. Of course, do this once you have ensured that your important data has been transferred to a different partition of your hard drive or an external data storage device.

In order to prevent SmitFraud from entering your computer, always check if the online resources where you download your files and software are credible ones. You should also make it a point to install a good firewall application and keep it running when downloading files from the Internet.