

## ***New Virus Alert - Smitfraud and its variants***

From its first launch, around spring 2008, the SmitFraud group of rogue spyware-scanners has gradually become quite a problem in this virtual world. Using trojans of all kind, these 'scanners' try to install themselves on Windows-computers with the just one reason ...

Trying to trick internet-users into buying these fake spyware-scanners.

### **What is Smitfraud**

SmitFraud is a group of fake spyware-scanners which has become a big problem on the internet. These bogus scanners and their installer-trojans are constantly updated with different names and different fake malware-warnings, to trap internet-users into downloading/installing this fake software (and, of course buying it!).

To accomplice this goal, several trojans are installed automatically thru 'flyby'-installations (on websites) or fake, free downloadable software. After the installation of the hijacking trojans, the desktop will be hijacked to show a fake spyware-warning. Other possible noticeable symptoms are a hijacked browser and pop-ups (warning you, again, for dangerous spyware on your computer). The actual fake scanner can be easily removed, by deinstalling it from the Software-list in the control panel.

The remaining trojans, however, will remain and are not so easily removed!

### **How SmitFraud works**

Usually an installer-trojan installs itself on the victim's computer. It then downloads and installs several trojans.

Among them is the trojan which hijacks the desktop, which displays a fake spyware-warning. Other species of trojans, which are installed, are Spyware, AdWare and Browser-hijackers. All this is done to persuade the user of the infected computer to install a trial-version the bogus scanner.

Usually the desktop-hijack and pop-ups disappear as soon as the user has installed the fake spyware-scanner.

Browser-hijackers and certainly spyware/keyloggers remain on the infected computer.

## ***The most prevalent variant of the Smitfraud malware for this quarter is System Security 2009.***

### **How to manually remove System Security 2009**

To remove System Security 2009 spyware you must block System Security 2009 sites, stop and remove processes, unregister DLL files, search and delete all other System Security 2009 files and registry utility. Follow the System Security 2009 detection and removal instructions below. The most typical software removal method is to remove System Security 2009 by using "Add or Remove Programs" service. However there may be hidden System Security 2009 files, running processes and registries in your computer, so System Security 2009 may recreate all other files after reboot.

### **System Security 2009 manual removal instructions**

Block System Security 2009 sites: bestcleaner.us, ultracleaner.us, ultracleaner.biz, websecurityvoice.com, greatvirusscan.com, securityscanguide.com, getpcguard.com, initialsecurityscan.com, interinetskim.com, wwwmobilereads.com, websecuritymaster.com,

networkstabilityscan.com, fullandtotalsecurity.com, secureserver4.cc, securityscan4you.com, free-web-scanners.info, totalvirusshield.com, justwebsecurity.com, xvirusdescan.com, hypersecurityshield.com, fullvirusprotection.com, freewebmypcscan.com, besthandycap.com, futureinternetsecurity.com, internetsecuritymetrics.com, fullpcvirusscan.com, 0scan.us, thesecuritystandart.com, superiorinternetsecurity.com, free-webscaners.net, webstoresecurity.com, crownsafetytool.com, securityonlinesite.com, loved-online-tube.com, scan-virusremover2009.com, aboutdot.info, ourbestsecurityshield.com, safetyscanguide.com, scantrustsecurity.com, scan-av-express.com, bestscanpc.info, zocleaner.com, gersoft.info, bestscanpc.org, securitysupplycenter.com, best-scanpc.net

### **Stop and remove System Security 2009 processes:**

05643921.exe  
install.exe  
00308937.exe

### **Locate and delete System Security 2009 registry entries:**

Open registry editor (go to the run command and type regedit and be careful not to delete anything but what is on this list, or your system could become unstable)

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\systemsecurity2009

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\systemsecurity2009 displayicon

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\systemsecurity2009 displayname

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\systemsecurity2009 shortcutpath

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\systemsecurity2009 uninstallstring

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "00308937"

HKEY\_LOCAL\_MACHINE\Software\00308937

### **Detect and delete other System Security 2009 files:**

Reboot your system into SAFE MODE by tapping the F8 key before windows begins to boot!!!

Then locate and delete the following files.

%Documents and Settings%\All Users\Application Data\00308937\pc00308937ins

%Documents and Settings%\All Users\Application Data\00308937\00308937.exe

%Documents and Settings%\All Users\Application Data\00308937\config.udb

%UserProfile%\Start Menu\Programs\System Security\System Security 2009 Support.lnk

%UserProfile%\Start Menu\Programs\System Security\System Security 2009.lnk

%UserProfile%\Desktop\System Security 2009.lnk

We strongly recommend you to use a spyware remover to track System Security 2009 and automatically remove System Security 2009 processes, registries and files as well as other spyware threats.

There are many programs out there such as SpyWare doctor, Webroot Spy sweeper Lavasoft ADAWAE Professional.