

WinFixer, WinAntiVirusPro, ErrorSafe, SystemDoctor, WinAntiSpyware, AVSystemCare, WinAntiSpy, Performance Optimizer, StorageProtector, PrivacyProtector, WinReanimator, DriveCleaner, WinspywareProtect, PCTurboPro, FreePCSecure, ErrorProtector, SysProtect, WinSoftware and **ECsecure** are a family of scareware rogue security programs, developed by Winsoftware which claim to repair computer system problems on Microsoft Windows computers if a user purchases the full version of the software. The software is mainly installed without the user's consent. McAfee claims that "the primary function of the free version appears to be to alarm the user into paying for registration, at least partially based on false or erroneous detections. The program prompts the user to purchase a licensed copy of the program. These applications are also known as "Ransomware" or "Extortionware".

The WinFixer web page says it "is a useful utility to scan and fix any system, registry and hard drive errors. It ensures system stability and performance, frees wasted hard-drive space and recovers damaged Word, Excel, music and video files". However, these products are actually virus distribution applications whose sole purpose is to extort a purchase price. It is suspected but not proven that credit card numbers are also harvested in this scam, which become untraceable by the time the information changes hands many, many times before reaching street level.

Methods of Installation

An example of a WinFixer pop-up dialog box within Opera. Even if the user hits Cancel, or X dialogs were clicked to dismiss the box, it would redirect to a WinAntiVirus page anyway, featuring a simulated system scan and a drive-by download of the viruses.

The WinFixer application is known to infect users using the Microsoft Windows Operating system, and is browser independent, One infection method involves the Emcodec.E trojan, a fake codec scam. Another involves the use of the Vundo family of Trojans.

Typical infection

The infection usually occurs during a visit to a distributing web site using a web browser. A message appears in a Dialog Box, or popup asking the user if they want to install WinFixer, or claiming a users machine is infected with malware, and requests the user to run a free scan. Download of the software may be triggered when a user attempts to exit the window by clicking 'Ok' or 'Cancel' or by clicking the corner 'X', it will trigger a pop-up window and WinFixer will download and install itself.

Initial message prior to infection - a user wishing to avoid infection might wish to disconnect from the Internet before closing the dialog box. An easier escape is to use ctrl-alt-del, hold the power button in, or simply unplug the machine.

When the user chooses any of the options or tries to close this dialog (by clicking 'Ok' or 'Cancel' or by clicking the corner 'X'), it will trigger a pop-up window and WinFixer will download and install itself, regardless of the user's wishes.

"Trial" offer of WinFixer

A free, "trial" offer of this program is sometimes found in pop-ups. If the "trial" version is downloaded and installed, it will execute a "scan" of the local machine, and a couple of non existant Trojans and viruses will be located, but does nothing else. To obtain a quarantine or removal, WinFixer requires the purchase of the program.

WinFixer Application

Once installed, WinFixer frequently launches pop-ups and prompts the user to follow its directions. Because of the intricate way in which the program installs itself into the host computer (including making dozens of registry edits), successful removal may take a fairly long time if done manually. When running, it can be found in the Task manager and stopped, but before long it will re-install and start up again, and over time, the user loses access to Task manager and most other admin features. Eventually, the virus assumes all administrative access to the machine, and all information on the hard drive must be destroyed. Once re-formatted, a new OS can be installed, and then the long task of rebuilding begins.

WinFixer is also known to modify the Windows Registry, so that it launches automatically after reboot and scans the users computer.

Firefox popup

The Mozilla Firefox browser is vulnerable to initial infection by WinFixer. Once installed, WinFixer is known to exploit the SessionSaver extension for the Firefox browser. The program causes popups on every startup asking the user to download WinFixer, by adding lines containing the word 'WinFixer' to the prefs.js file.

Avoiding infection

If the initial dialog box is shown, disconnecting from the Internet *before* closing it will stop WinFixer from downloading. Shutting down all browser windows using the Task Manager found in Windows 2000 and above also seems to be effective, or simply unplug the machine. Do not simply close the browser windows using the close button on the window, as WinFixer will still auto-download.

Because this is a java-script dialog box related to the web browser, it does not appear in the Windows Task Manager list.

Blocking its sites such as www.winfixer.com, winantivirus.com or www.systemdoctor.com in your firewall will prevent the typical infecting download. However, there may be other means by which the program installs itself.

If a file download window appears, then simply clicking the "Cancel" or "No" button (depending on your browser) on the file download window that appears can stop the software downloading. You must, however, remember not to click on the Close Window (x) button without first disabling JavaScript, since doing that is usually scripted to start the download instead.

Disconnecting your network connection is effective at stopping the file from downloading.

Removal

There are several respectable programs which may remove the WinFixer application. These include the McAfee VirusScan, Norton Antivirus, and Trend Micro family of products. Additionally, Symantec has published procedures for removing WinFixer manually. This is a manual process involving registry editing. Additionally, Malwarebytes has created a free automated tool that will remove these infections. Spybot - Search & Destroy, SuperAntiSpyware, and AVG may also remove some forms of Winfixer.

Domain Ownership

The company that makes WinFixer, Winsoftware Ltd., claims to be based in Liverpool, England (Stanley Street, postcode: 13088.) However, this address has been proven false.

The domain WINFIXER.COM on the whois database shows it is owned by a void company in Ukraine and another in Warsaw, Poland. According to Alexa Internet, the domain is owned by Innovative Marketing, Inc., 1876 Hutson St, Honduras.

According to the public key certificate provided by GTE CyberTrust Solutions, Inc., the server *secure.errorsafe.com* is operated by ErrorSafe Inc. at 1878 Hutson Street, Belize City, BZ.

Running traceroute on Winfixer domains shows that most of the domains are hosted from servers at <http://www.setupahost.net>, which uses Shaw Business Solutions AKA Bigpipe as their backbone.

Technical Information

WinFixer is closely related to Aurora Network's Nail.exe hijacker/spyware program. In worst-case scenarios, it may embed itself in Internet Explorer and become part of the program, thus being nearly impossible to remove. The program is also closely related to the Smitfraud, Vundo and Virtumonde viruses.

a few examples of drive-by installer popups :

