

Rogue software

Contributed by Administrator
 Thursday, 18 September 2008
 Last Updated Thursday, 18 September 2008

Rogue security software is software that uses malware (malicious software) or malicious tools to advertise or install itself or to force computer users to pay for removal of nonexistent spyware. Rogue software will often install a trojan horse to download a trial version, or it will execute other unwanted actions. Effects The main goal of rogue software makers is to sell their product. Many times fake Windows dialog boxes will appear. Most of the time, they will display a message such as "WARNING! Your computer is infected with spyware! Buy [software name] to remove it!" Usually, when the dialog box's OK button is clicked, this will direct the user to a porn website. Sometimes, even clicking the upper right hand X button to close the dialog box will produce the same effect or activate the software's installation. (Pressing Alt+F4 can circumvent that trick). Some software, like SpyAxe will automatically download the trial version without any user action (drive-by installation). False positives A variant of the above technique that rogue security software makers use is that of false positives. A false positive is a fake or false malware detection in a computer scan. This can convince even advanced users that their computer is infected who may not be deceived by the abovementioned similar claims without a scan. This is quite different from an accidental false positive, which can be produced in a scan by security software from honest companies. Detection Almost all reputable antispyware software will detect rogue software if it is installed on the scanned computer. Often, non-reputable rogue antispyware software will install a Trojan horse to download the software from the maker's website, like Titan Shield. Reputable antispyware software can detect the Trojan even before the software is installed. However, often removal of new, aggressive rogue programs requires use of manual removal processes.

Partial list of rogue software There are a large number of number of fake anti-spyware programs active on the Internet. Typically, widely-distributed Web banner ads falsely warn users that their computers have been infected with spyware, enticing them to download the rogue software. Once installed, the software uses human engineering and false positives to manipulate the user into purchasing the software. These programs do not actually remove spyware — or worse, may add more. The following is a partial list of known rogue software. Often the same software is distributed under several names.

* Advanced Cleaner * AlfaCleaner * AntiSpyCheck 2.1 * AntiSpyStorm * AntiSpywareBot
 AntiSpywareMaster * AntiSpywareSuite * AntiSpyware 2008 XP * Antivermins * Antivirgear * Antivirus 2008 *
 Antivirus 2009 * AntiVirus Gold * Antivirus Master * Antivirus XP 2008 * Awola 6.0 * Brave Sentry *
 BestsellerAntivirus * Cleanator * ContraVirus * Doctor Antivirus * DriveCleaner * Disk Knight *
 EasySpywareCleaner * Errorsafe * free-viruscan.com * IE Antivirus * IEDefender * InfeStop * KVMSecure *
 MacSweeper * MalCrush 3.7 * MalwareCore * MalwareAlarm * Malware Bell 3.2 * PCSecureSystem * PC Anti
 [9] * PC Clean Pro * PC SpeedScan Pro * PestTrap * Perfect Cleaner * PAL Spyware Remover * PCPrivacyCyte
 * PC-Antispyware * PSGuard * SecurePCCleaner * Security toolbar 7.1 * SpyAxe * Spy Away * SpyCrush
 Spydawn * SpyGuarder * SpyHeal * Spylocked * SpySheriff * SpySpotter * Spyware Cleaner * Spyware C
 * Spyware Stormer * SpywareStrike * Spy-Rid * SpyWiper * System Live Protect * SystemDoctor *
 TrustedAntivirus * TheSpyBot * UltimateCleaner * VirusHeat * Virus Isolator * VirusProtectPro * VirusRanger
 Vista Antivirus 2008 * WinAntiVirus Pro 2006 * WinFixer * WinSpywareProtect * WorldAntiSpy * XP Antivirus
 XoftSpySE * Zinaps 2008