

Misleading Applications – What you need to know

Misleading applications can sneak onto your computer as you surf the Web. Once installed, scammers use them to commit fraud and identity theft. Here's what you need to know to guard against spyware and other misleading applications.

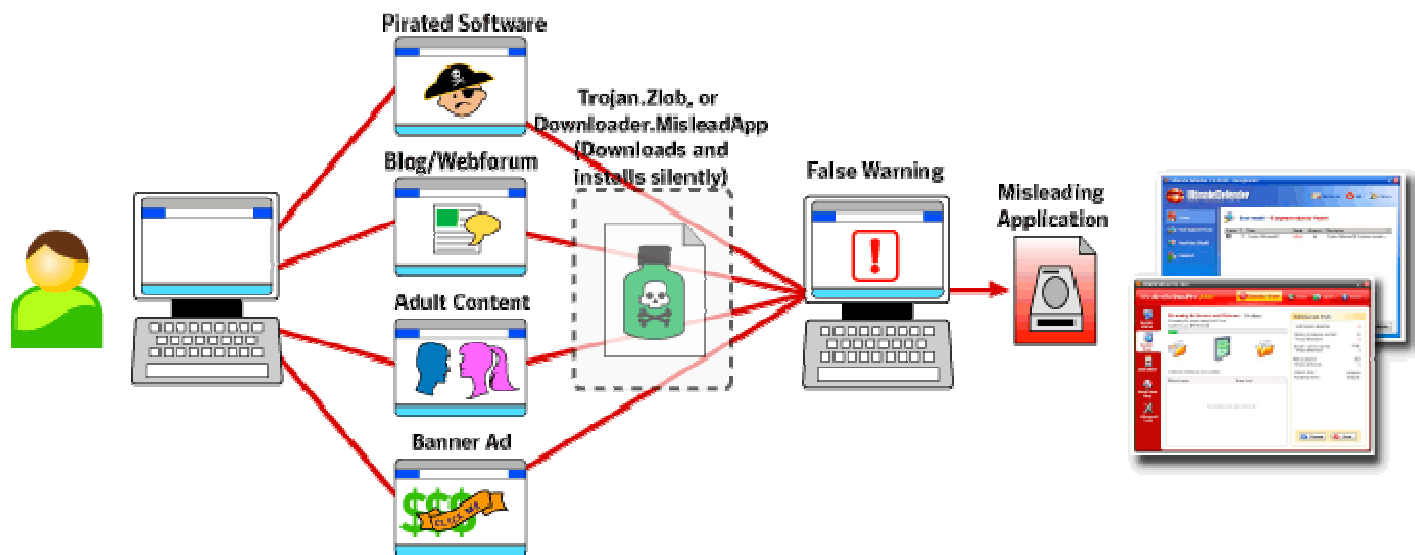
Introduction

Have you ever seen a strange security message pop up like an advertisement while you're surfing the web? Have you seen an unexpected balloon message appear from an unknown program on your system, telling you that you're infected with a new threat? These are common tactics used by a type of program Symantec calls "misleading applications" and other people refer to as "Rogue AntiSpyware" or "SMITFraud". These programs typically sneak onto their victims' systems while they surf the web, masquerade as a normal Microsoft Windows alert, or otherwise trick people into downloading them onto their computer. Once installed, misleading applications exaggerate or make false claims about the security status or performance of your system, then promise to solve these bogus problems if you pay them.

What are misleading applications?

Misleading applications intentionally misrepresent the security status of a computer. Misleading applications attempt to convince the user that he or she must remove potentially unwanted programs or security risks (usually nonexistent or fake) from the computer. The application will hold the user hostage by refusing to allow him or her to remove or fix the phantom problems until the "required" software is purchased and installed. Misleading applications often look convincing—the programs may look like legitimate security programs and often have corresponding websites with user testimonials, lists of features, etc.

How they Attack



Misleading applications typically strike people when they are surfing the web. There is not a single type of website where these applications are found, but they are more common from sites offering pirated goods and adult content, as well as blogs and forums. They can even sneak into advertisements on legitimate sites, usually through banner ads at the top of Web page. In order to get installed onto a system, a person is usually either tricked into downloading the program (thinking it's something else) or a small program called a "Downloader" is installed by the attacker through an un-patched flaw in the person's web browser. This is often known as a "drive-by" install.

Misleading applications often are not the first unwanted program to land on a person's system. A Downloader, such as Trojan.Zlob or Downloader.MisleadApp, infect the system first and then download the misleading application to the computer. Once the downloaded application is installed and ready, the malware that installed it will inform the user that they are infected with a new, previously unknown threat. This can be done through a "balloon message" that appears in the lower right-hand side of the system. The misleading application will then present itself and either pretend to download or run a scan of the system.

The scan results produced by the misleading application may be entirely false or may include some real issues affecting the system, but will always exaggerate the problems on the system and refuse to fix them until the vendor is paid and a registration key is entered into the program.

Why are they dangerous?

Misleading applications, sometimes called rogue anti-spyware or "SMITFraud", trick consumers into believing a problem exists on their system. Consumers who trust the messages are tricked into purchasing bogus applications for resolution of the problems they have been duped into believing exist. Misleading applications scam consumers out of money, faking the existence of problems and failing to deliver the protection they promise. They also create a privacy risk as the victim must provide their credit card information to the scammers in order to register the misleading application and solve the supposed problems.

The victims of misleading applications have paid for software that does not work, handed their personal information to scammers, and are left with a false sense of security that leads them to potentially greater risks from more aggressive threats. Even if a person catches on to the ruse and does not pay the misleading application vendor, the programs can be notoriously difficult to remove without the proper security software.

What to Do

- Use your Internet security suite to proactively protect from spyware and other security risks
- Configure the firewall in your Internet security product to block unsolicited requests for outbound communication
- Be especially cautious when clicking on pop-up advertisements—especially ads promoting system security or performance tools that look like a standard Microsoft Windows alert
- Do not accept or open suspicious error dialogs from within the browser
- Purchase security and system performance software from reputable sources
- Keep software and security patches up to date

List of Misleading applications

- WinFixer
- Ultimate Defender
- SpySheriff
- MalwareWipe
- DriveCleaner
- AVSystemCare
- 1stAntiVirus
- VirusBurst
- SpywareQuake
- AntispywareSoldier

Source: Symantec Corporation