



What Is Spyware?

Spyware is software that is covertly installed on a machine without explicit permission for the purpose of collecting information about a user or corporation to be returned to an unauthorized third party, compromising the security of sensitive or proprietary information.

Initially designed to monitor a user's online activity in order for marketers to deliver targeted advertisements, spyware is now being used for more malevolent purposes such as gathering passwords, personal e-mail addresses and contact information, credit card and account numbers, confidential documents and records, etc.

There are thousands of different spyware threats operating on the Internet, each with unique tactics. Many of the most common forms of spyware can be placed into one of the following categories:

- **Adware** Adware is software whose revenues are supported by pop-up ads that are displayed while the program is running. These adware applications are bundled with seemingly legitimate programs, which are often downloaded from the Internet as freeware. The user is often unaware adware is included in these applications. Once installed, adware generates a barrage of pop-up advertisements and can further invade user privacy by installing additional components to track Web surfing habits and collect personal information. Examples of adware applications include: AdBlaster, Ad-Popper, Sandboxer, LoudMarketing, etc.
- **Keystroke Loggers/ System Monitors** A particularly insidious form of spyware, these applications can monitor and record virtually everything a user does on his/her machine. Passwords, keystrokes —everything the user types or clicks— is continually stored in an encrypted log file and then regularly reviewed by the spyware host. Sophisticated new forms of keystroke loggers and system monitors can now install themselves remotely without administrative access to a machine.
- **Trojan Horse** A Trojan horse is a destructive program, deceptively disguised a benign application that is designed to damage operating systems, software, or the hard drive causing loss of information or even the destruction of the user's system. Remote Administration Tools, or RATs, are a type of Trojan horse that allows the attacker unauthorized and unrestricted access to a computer whenever the user is online. Examples of Trojan horses include: Netspy, Winspy, Spyboy, etc.
- **Security Disablers** Security Disablers are a form of spyware designed to modify the security settings specified by a user or administrator in order to alter the efficacy of a firewall or other anti-spyware security measures. This better allows for unauthorized applications to be covertly installed. Examples of security disablers include: StopSign, designed to disable firewalls; AVKillah, designed to disable anti-virus software and firewalls
- **Hijacker** A Browser/ Page Hijacker is an application designed to change the user's browser settings to direct the user to a website specified by the spyware author. Many hijackers use misleading dialog boxes or other deceptive tactics to install on the user's computer. Hijacker programs typically place a reference in the registry so that they reinstall every time the computer is started. A System Hijacker is an application that uses the host computer as a resource for conducting other activities. This strains the performance of the host computer and decreases Internet speed.

To get on the path to protection and learn more about Aluria's flexible pricing, customization and deployment options, please contact an authorized Aluria Reseller or a Aluria Sales Representative at 407-833-8700 or visit Aluria on the web at www.aluriasoftware.com. FREE Evaluation Version available upon request for businesses meeting minimum requirements.