Article published on March 13th 2012 | Business

Bundled Software: When Is It Not Adware?

If a user wants a piece of software, why can't he or she be allowed to install it separately? If the bundled software were essential to the functioning of the original software (excluding generic functions such as install, un-uninstall, and documentation), why wouldn't the developer build its functions directly into the original software?

Sure, sometimes there's a software application that clearly complements another application. But for users who do not want the complementary software, having it just means a bloated install file and a needlessly long installation process.

Does the chance that users will want the bundled software ever outweigh the risk of the bundled software being installed without the user noticing? In the case of adware, the technology community is increasingly willing to put the burden of proof on the adware bundlers:

* Cnet's download.com website recently removed any and all software that comes bundled with another piece of software that shows advertising, regardless of how well informed the user is of the bundled software.

* Affiliate networks such as Commission Junction and Kolimbo have either cautioned advertisers against accepting adware distributors into their affiliate programs or kicked them out altogether.

* Many technology law experts are saying that the click-wrap license agreements that supposedly legitimate adware are not proof of informed consent. Some experts even say that such agreements amount to unconscionable contracts: the burden imposed by adware is so great and the benefit offered so negligible.

Adware and Bundled Software: A Modest Proposal

If the spam arms race is any indication, we may soon face even more aggressive attempts to get adware on our computers. There will be even more tortured arguments that bundled adware is installed with users' informed consent. Why not head off any of those arguments right now? Let's push for an industry standard that reputable developers do not bundle software (with a few highly specific exceptions such as documentation, installation, and error reporting).

In the end, by getting rid of bundled software, what do we have to lose except adware?

When adware can't trick you into installing it, it often resorts to a secretive invasion. Find out how to defend yourself.

Adware Installation Stealth Tactic 1: Expensive Freebie

â€¢ How it works: adware may get installed with so-called free software without any mention of it being included anywhere in the software's license or documentation. Or any mention of the bundled software is buried deep within a click-wrap licensing agreement.

â€¢ How to protect yourself: It's become an endlessly repeated clichÃ©, but it's true: only install software from developers you trust. That doesn't mean you can never try any software from a new company. Just familiarize yourself with the developer's reputation before opening wide your hard drive. Search the developer's name on search engines. If a dozen anti-spyware advertisements are listed alongside the search results, that's not a good sign.

â€¢ How to fight back: If you've already downloaded the expensive freebie, it's probably too late to simply uninstall it. The bundled adware will likely stick around on your computer long after the software that came with it has been sent to the recycling bin. Instead, you need to use an anti-spyware program, and preferably two to be sure.

Tactic 2. Adware Drive-by

â€¢ How it works: adware may hide in a website's code and download itself automatically onto the site visitor's hard drive. This is often called a "drive-by" installation.

â€¢ How to protect yourself: drive-by installations of software tend to happen on obscure commercial websites, rather than personal homepages, blogs, or the websites of established businesses. If you can avoid surfing in those kinds of rough waters, you'll be a lot safer from adware attacks.

â€¢ How to fight back: If you do suspect that a site has downloaded software onto your computer, close it immediately and fire up your anti-spyware and antivirus software. You may also want to delete your browser's cache and also any program downloads folders and temporary internet folders, just in case the adware is a new kind of adware that isn't in your anti-spyware software's database yet.

Tactic 3: The Old-Fashioned Way: Email

â€¢ How it works: you know the drill: just as with viruses, adware may come as an email attachment. The stealth part is that simply not opening attachments may not be enough to protect you. The attachment may not display an attachment icon and is set to auto-install as soon as the message is opened.

â€¢ How to protect yourself: make sure your email software does not open attached files automatically. With most new email software applications the option to block automatic downloads of attached files is set as the default. But to be really safe, you should set your anti-spyware software to automatically monitor all email.

â€¢ How to fight back: delete the offending email without opening it or the attachment (assuming that hasn't happened already). Run a full scan of your hard drive using anti-spyware and antivirus software.

http://www.20buckbackup.com/

Article Source:
http://www.articleside.com/business-articles/the-case-against-bundled-software.htm - Article Side

Seolncr - About Author:
Get a online backup at affordable prices for your window pc or mac and to know more a remote backup agent for more info visit http://www.20buckbackup.com/

Article Keywords:

online backup, remote backup agent