

Download.Com Caught Adding Malware to Nmap & Other Software

Written by computathug

Wednesday, 07 December 2011 10:32 - Last Updated Wednesday, 07 December 2011 12:25

CNET's Download.Com is one of the most popular ([currently ranked #174 worldwide by Alexa](#)) and longest-running (been around since 1996) major sites on the Internet. As a download repository, their key value ad was that they screened software to avoid malware, spyware, adware, viruses and other harmful content that certain shady software contains. Even many security experts

[recommended them](#)

as a safe place to download software online. Download.Com is run by CNET, which is part of the 17-billion dollar

[CBS](#)

media empire. Many people assumed that a major site like this wouldn't resort to unethical monetization schemes like adding spyware and other malware to their downloads.

Unfortunately, those people were wrong. In August 2011, Download.com started wrapping legitimate 3rd party software into their own installer which by default installs a wide variety of adware and other questionable software on users machines. It also does things like redirect user search queries and change their Internet home page. At first their installer forced people to accept the malware or close the installer ([see screen shot of infected VLC installer in this article](#)). Later they added a non-default "decline" button hidden way on the left side of the panel. Also, the initial installer shown in the previous screen shot claimed the software was "SAFE, TRUSTED, AND SPYWARE FREE". In an unusual show of honesty, they removed that claim from the rogue installer.

While it is common for internet criminals to infect software installers in this way, we never expected it from a previously-reputable site like Download.Com. Especially given their "[Download.com Adware & Spyware Notice](#)" which currently still says:

"In your letters, user reviews, and polls, you told us bundled adware was unacceptable--no matter how harmless it might be. We want you to know what you're getting when you download from CNET Download.com, and no other download site can promise that. "

and ...

"every time you download software from Download.com, you can trust that we've tested it and found it to be adware-free. "

It is unbelievable and reprehensible that they can make these claims of being adware,

Download.Com Caught Adding Malware to Nmap & Other Software

Written by computathug

Wednesday, 07 December 2011 10:32 - Last Updated Wednesday, 07 December 2011 12:25

malware, and spyware free at the same time at they are actually adding adware and malware to the packages they distribute! Here is an example from an installer screen added by CNET Download.Com which (if the user isn't vigilant enough to catch the small print I've circled below and press the decline button) will infect their machine:



It is bad enough when software authors include toolbars and other unwanted apps bundled with their software. But having Download.Com insert such things into 3rd party installers is even more insidious. When users find their systems hosed (searches redirected, home pages changed, new hard-to-install toolbars taking up space in their browser) after installing software, they are likely to blame the software authors. But in this case it is entirely Download.com's fault for infecting the installers! So while Download.Com takes the payment for exploiting their user's trust and infecting the machines, it is the software authors who wrongly take the blame! Of course it is users who pay the ultimate price of having their systems infected just to make a few bucks for CNET.

They're even using the trojan for children's software such as the [Kea Coloring Book](#) ! Have they no shame?