



[<< Back to Article](#)

Hackers Use Banner Ads on Major Sites to Hijack Your PC

By Betsy Schiffman 11.15.07 | 7:30 PM

The worst-case scenario used to be that online ads are pesky, memory-draining distractions. But a new batch of banner ads is much more sinister: They hijack personal computers and bully users until they agree to buy antivirus software.

And the ads do their dirty work even if you don't click on them.

The malware-spiked ads have been spotted on various legitimate websites, ranging from the British magazine *The Economist* to baseball's MLB.com to the Canada.com news portal. Hackers are using deceptive practices and tricky Flash programming to get their ads onto legitimate sites by way of DoubleClick's DART program. Web publishers use the DoubleClick-hosted platform to manage advertising inventory.

If you've seen any of the ads, you may have experienced something like this: You're on a legitimate site. Your browser window closes down. A new browser window comes up, redirecting you to an antivirus site, while a dialog box comes up telling you that your computer is infected and that your hard drive is being scanned. The malware tries to download software to your computer and scans your hard drive again. (Here's a [video demonstration of the rogue ads.](#))

The malware looks like an ordinary Flash file, with its redirect function encrypted, so that when publishers upload it, the malware is not detectable. Once deployed on a site, the Flash file launches the malicious redirects, which appear to be triggered at preset times or at selected Web domains.

John Mark Schofield, a Los Angeles IT director, encountered the ads on Canada.com. He thinks that because he was on a Mac OS computer, the damage wasn't so severe. "My feeling is that it would have caused me a lot more grief if I had been on a Windows computer: It may have installed the malware. Instead, it took over my browser, which I just fixed by exiting Firefox," Schofield says.

DoubleClick acknowledges the malware is out there, and says it has implemented a new security-monitoring system that has thus far captured and disabled a hundred ads.

"This is an industry-wide challenge. Unfortunately, there are bad actors who

misrepresent themselves and purchase advertising as an avenue to distribute malware. This has the potential to affect all businesses and consumers in the online environment," says Sean Harvey, senior product manager at DoubleClick DART.

Publishers may be somewhat culpable, too. The distributor of the malware-infected ads is believed to be AdTraff, an online-marketing company with reported ties to the Russian Business Network, a secretive internet service provider that, security firms say, hosts some of the internet's most egregious scams. AdTraff is believed to have posed as a legitimate advertiser, using its partners as references. The ads were almost always paid for with credit cards or wire transfers, according to Alex Eckelberry, CEO of Sunbelt Software, a provider of security software.

"The AdTraff guys probably register at a bunch of sites -- maybe more than 300. They say they're advertisers. They get the sales guys at the end of the quarter when they're anxious to take the deal. (AdTraff) wires the cash, and they buy the inventory on the site," Eckelberry says.

AdTraff could not be reached for comment. The company lists a phone number in Germany which leads to a generic voicemail box.