Forbes / Tech
MAY 6, 2015 @ 08:00 AM 3,361

Busted! Google Names Key Culprits In Scammy Ad Software

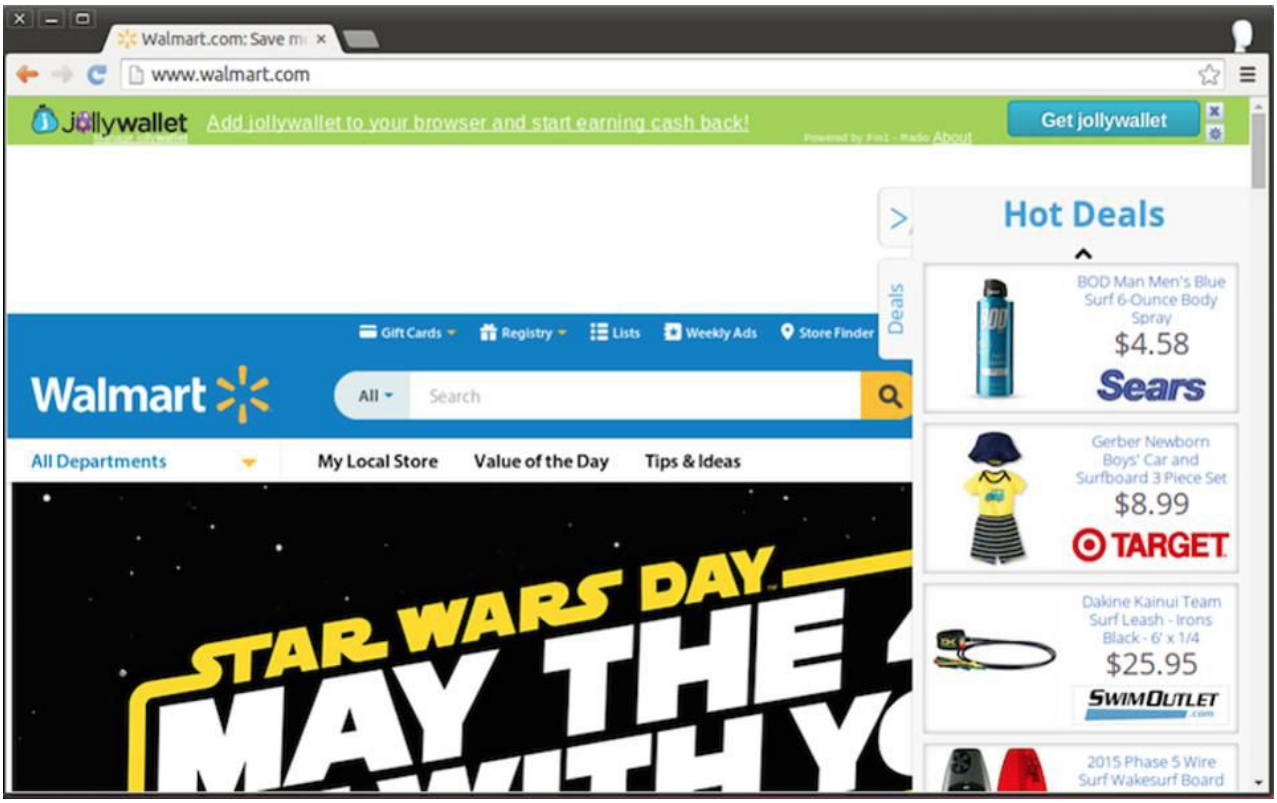
Robert Hof, CONTRIBUTOR
I cover the collision of advertising and the Internet. FULL BIO
Opinions expressed by Forbes Contributors are their own.

If you're the victim of seemingly out-of-place ads that get plastered on websites you're visiting, now you know whom to blame.

Programs called ad injectors can get surreptitiously installed on your computer via browser extensions and insert ads or replace existing ones on pages you visit, from Amazon.com AMZN +1.49% to Walmart.com to Google GOOGL -0.71%.com itself. That's not only annoying, but it can be dangerous because the software can open users' computers to serious security risks. It can steal user information, hijack search queries, and send a user's online activities to other companies for tracking.

Google called out ad injectors in a March 31 blog post, promising to reveal the results of a study of ad injectors it did with University of California researchers. In short, the study found that about 5.5% of IP addresses, meaning millions of unique users accessed Google sites that included injected ads. Some 100,000 people have complained about them so far this year.

Today, it's releasing more results from the full study, and this time Google is naming names. Some of them, such as Palo Alto-based Superfish and JollyWallet from Tel Aviv-based Radyoos Media, are known ad injectors, so they're not much of a surprise. But the study for the first time also implicates several fairly well-known, otherwise legitimate businesses, including shopping ad networks Dealtime.com, PriceGrabber.com, and BizRate.com.



Unwanted ads injected onto Walmart.com

In an interview, Google lead spam and abuse researcher Kurt Thomas explained that it's tough to stop ad injectors because they use the crazily complex system of running ads online to mask the source of the ads and where they ultimately appear. His blog post today names the various players:

> • ***Software:*** *It all starts with software that infects your browser. We discovered more than 50,000 browser extensions and more than 34,000 software applications that took control of users' browsers and injected ads. Upwards of 30% of these packages were outright malicious and simultaneously stole account credentials, hijacked search queries, and reported a user's activity to third parties for tracking. In total, we found 5.1% of page views on Windows and 3.4% of page views on Mac that showed telltale signs of ad injection software.*
>
> • ***Distribution:*** *Next, this software is distributed by a network of affiliates that work to drive as many installs as possible via tactics like: marketing, bundling applications with popular downloads, outright malware distribution, and large social advertising campaigns. Affiliates are paid a commission whenever a user clicks on an injected ad. We found about 1,000 of these businesses, including Crossrider, Shopper Pro, and Netcrawl, that use at least one of these tactics.*

● ***Injection Libraries:*** *Ad injectors source their ads from about 25 businesses that provide "injection libraries." Superfish and Jollywallet are by far the most popular of these, appearing in 3.9% and 2.4% of Google views, respectively. These companies manage advertising relationships with a handful of ad networks and shopping programs and decide which ads to display to users. Whenever a user clicks on an ad or purchases a product, these companies make a profit, a fraction of which they share with affiliates.*