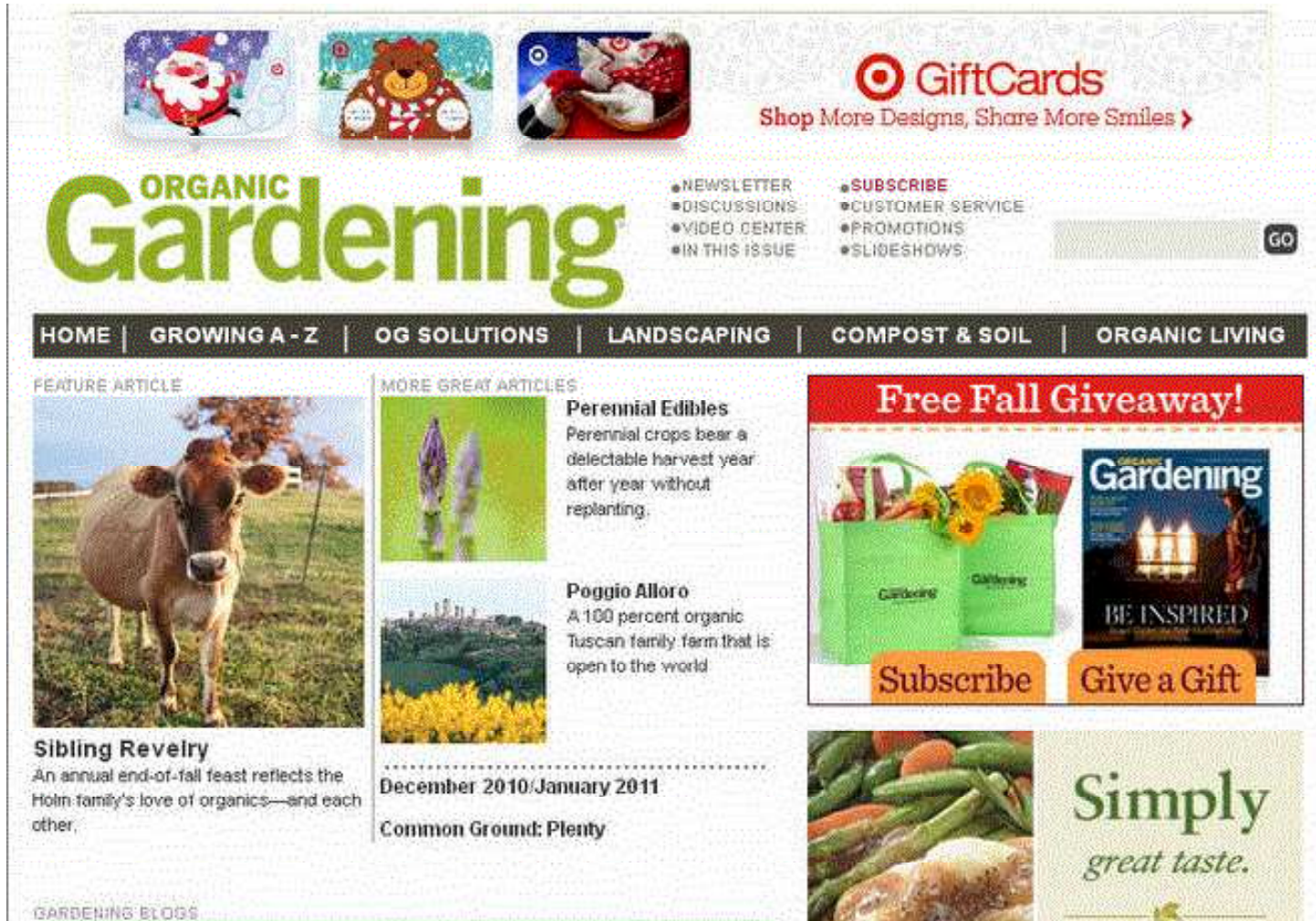


Google DoubleClick Caught Serving Malicious Ad

By [Kim Zetter](#)  December 10, 2010 | 3:09 pm | Categories: [Cybersecurity](#)



The screenshot shows the Organic Gardening website interface. At the top, there are three small images of gift cards (Santa Claus, a bear, and a bird) and a Target GiftCards banner with the text "Shop More Designs, Share More Smiles". Below this is the "ORGANIC Gardening" logo and a navigation menu with links for NEWSLETTER, DISCUSSIONS, VIDEO CENTER, IN THIS ISSUE, SUBSCRIBE, CUSTOMER SERVICE, PROMOTIONS, and SLIDESHOWS. A search bar with a "GO" button is also present. The main content area features a "FEATURE ARTICLE" with a photo of a cow and the title "Sibling Revelry", and "MORE GREAT ARTICLES" including "Perennial Edibles" and "Poggio Alloro". A prominent red banner on the right says "Free Fall Giveaway!" and includes images of gift bags and a magazine cover with the text "Subscribe" and "Give a Gift". At the bottom right, there is a "Simply great taste." banner with an image of vegetables.

DoubleClick, the Google-owned ad technology, has been distributing malware in an online ad served through a number of websites, according to the security researcher who says he discovered the attack.

The malware infects users who visit a page where an infected banner ad is displayed. It's installed as a drive-by download, meaning that users don't have to click on the ad to be infected, they just have to visit a website when the ad appears on the page.

Wayne Huang, CTO of Armorize, says his company discovered the problem Dec. 4 and notified DoubleClick.

The malicious advertisement, for gift cards, originates from a bogus advertising agency called AdShuffle, with three f's in the name. The name appears to be playing off legitimate advertiser [AdShuffle](#). The malicious ad has appeared on sites for [Runnersworld.com](#) and [OrganicGardening.com](#), among other sites that are still being determined.

[Runnersworld.com](#) and [OrganicGardening.com](#) are published by the Emmaus,

Pennsylvania-based Rodale Inc. A company spokeswoman said the ads have been taken down.

down.

The banner ad hawks a gift card for retail giant Target.

Huang says it appears the attackers simply copied a legitimate banner ad and inserted Javascript that exploits the user's browser through one of three vulnerabilities. If the user has any of the unpatched vulnerabilities, a piece of software called "hdd plus" is quietly installed on their computer. The Javascript also tries to force browsers' PDF plug-ins to open a PDF to deliver the software through an Adobe exploit.

Once a user is infected, the "hdd plus" program causes a fake Windows warning message to appear on the user's screen indicating that their machine is riddled with malware, and urging the user to purchase a security program.

Huang says a backdoor is also installed on the user's machines, but he says researchers are still examining it to determine what it does.

It's not known how many machines may have been infected by the malicious ad or how many web sites have displayed it. Huang says the infections appear to have begun no earlier than Dec. 4.

Google acknowledged the issue in a statement to Threat Level and said it recently detected malware on its own through its DoubleClick Ad Exchange filter but this malware was stopped and never got served through its system to web sites. It's not clear if the malware Armorize found is the same malware Google detected or a different attack.

"We can confirm that the DoubleClick Ad Exchange, which has automatic malware filters, independently detected several creatives containing malware, and blocked them instantly – within seconds," a Google spokesman wrote in an e-mail. "Our security team is in touch with Armorize to help investigate and help remove any affected creatives from any other ad platforms."

The malicious ads were discovered by an Armorize program called Hack Alert that scans web sites for malicious activity. Huang says that his researchers tested the malware against multiple anti-virus products and only 2 out of 42 vendors detected it.

It's not the first time that DoubleClick has served up a malicious program. In 2007, a legitimate German marketer was caught serving malware through an ad. In that case, the malware caused a flood of pop-up warnings to appear on the user's desktop telling them their machine was infected and urging them to purchase a security program.

DoubleClick said at the time that it had implemented a new security monitoring system to filter ads for malware.

Tags: [malware](#)

[Post Comment](#) | [Permalink](#)

Comments (1)

Posted by: WayneHuang | 12/11/10 | 1:22 am |

Thanks Kim! Details can be found on our blog:

<http://blog.armorize.com/2010/12/hdd-plus-malware-spread-through.html>
