




July 19, 2007

DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: www.djreprints.com.

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)

Hackers Can Now Deliver Viruses via Web Ads

By **EMILY STEEL**

July 19, 2007; Page B1

Web ads are becoming a delivery system of choice for hackers seeking to distribute viruses over the Internet.

In a development that could threaten the explosive growth of online advertising, hackers have started to exploit security holes in the online-advertising chain to slip viruses into ads. Just going to a site that shows such an ad can infect a user's computer.

In May, a virus in a banner ad on tomshardware.com¹ automatically switched visitors to a Web site that downloaded "malware" -- malicious software designed to attack a computer -- onto the visitor's computer. ScanSafe Inc., one of the first security firms to discover the virus, estimates the banner ad was on the site for at least 24 hours and infected 50,000 to 100,000 computers before Tom's Hardware removed it.

After the incident, Tom's Hardware's parent, TG Publishing, was acquired by BestofMedia Group. The company says it won't discuss what may have happened under prior management. But a person familiar with the situation says that Tom's Hardware was unaware of the threat and that ads on the site were supplied by an outside server and likely appeared on a number of other Web sites as well. Users of an online forum hosted on the Tom's site discussed the case, with some people noting that their antivirus software had protected their computers and others lamenting that a virus had been downloaded onto theirs.

Clicking on ads that appear in the sponsored-link results section of Web-search engines can also be very dangerous. Web-security firm McAfee Inc. found in May that 6.9% of sponsored links led to suspicious sites

that might have automatically downloaded malicious software.

"Not being able to offer a safe haven is one of the things that could stand in the way of reputable advertisers and dollars," says Scott Howe, president of Internet-ad network Drive Performance Media, a unit of Seattle-based aQuantive, which Microsoft Corp. recently agreed to buy for \$6 billion. "That's the single biggest fear that many advertisers have....It has taken them a hundred years to build their brand, and it can be destroyed pretty quickly if they are not careful."

The Internet has long been plagued with viruses, spyware and other troublesome software. In the past, though, consumers usually had to open a harmful attachment in an email, download free software that contained malicious code or click on a link to another site. Technology underlying virus-filled ads is more insidious. Simply opening a Web page that includes an ad loaded with a virus can expose a user to harm.

While the number of infected ads has been small compared with the trillions of ads populating the Internet, Web-security experts say the phenomenon is growing, especially on Web sites that accept ads from advertising networks that lack secure safeguards. Eighty percent of malicious computer code on the Internet is found in online ads, according to a recent study by computer-security firm Finjan Inc.

"The online-ad industry's success is going to be dependent on not letting viruses through the walls. They've all got to get better and mobilize," says Zack Rogers, vice president of revenue operations at CNET Networks Inc., which operates a number of Web sites, including CNET.com² and TV.com³.

Top-tier online-ad companies and Web sites say they are refining their security systems to try to prevent harmful material from leaking to the Internet. But security experts say the complex structure of business relationships in the online-ad world makes it difficult for sites to block virus-laden ads. Web sites often work with one group of ad firms to sell ad space and another group to ensure the ads appear when a Web surfer calls up a page. Yet another set of companies saves the digital information that creates an online ad on a computer server and then delivers that data to the Web sites. If just one of these players fails to properly vet their business partner and check each component of an ad for malicious code, an attack can occur.

"This is a multiple-layer problem, and people at all layers need to figure out what they need to do to make it more secure," says Chris Kelly, chief privacy officer at the popular social-networking site Facebook.

The phenomenon has already caught the attention of both the Federal Bureau of Investigation and the Federal Trade Commission. The FTC is encouraging advertisers to be careful about how they place their ads online, and it is warning Web users to safeguard themselves by both updating antivirus software and scanning their systems regularly.

Rooting the harmful code out of the online-ad chain and figuring out its origin is a major challenge. Often, the malicious code has been planted overseas, and it is usually hidden under layers of programming. Last July, more than one million visitors to a variety of Web sites found that their computers had been infected with a virus hidden in a banner ad for the now-defunct DeckOutYourDeck.com, according to VeriSign iDefense Security Intelligence Services, which first identified the threat. VeriSign traced the virus through a series of computer files to a server in Russia. But finding the actual person behind the exploit proved too difficult. Similarly, ScanSafe traced the problems on Tom's Hardware to a site in Argentina but was unable to identify the site's owner.

Ad networks, which distribute ads across the Internet, say they carefully review the companies from which they accept ads and use manual and automatic tools to scan for harmful code. Some companies have developed their own safeguards. Right Media, an online-ad exchange that uses automated systems to match buyers with sellers, last summer designed a system to block ads containing harmful material from entering its network. During its initial test in July 2006, Media Guard scanned more than 50,000 ads, putting each commercial through various tests looking for suspicious code. The scan discovered 17 different types of hidden viruses.

The ad network **ValueClick Inc.** says it uses a combination of automated and manual methods to prevent harmful activity. DoubleClick, an ad firm that **Google Inc.** recently agreed to acquire, says it provides security technology for its clients but doesn't control how they use it. Ad network [Advertising.com](#)⁴, owned by **Time Warner Inc.**'s AOL, says it carefully reviews every company it works with and checks ad content.

Google says it is committed to ensuring the safety and security of its Web sites' users and advertisers. The company says it constantly works to detect and remove sites that serve malicious software in both its advertising network and its search results.

Still, unless ad networks do more to increase security, Web-security experts warn that a major incident could occur. "That is the kind of next step that seems inevitable to me," says Ben Edelman, an assistant professor at Harvard Business School who researches Web-security issues. "Imagine if reading a book could kill you. You might read fewer books. If reading a Web page could kill your computer, might users go to fewer Web pages?"

Write to Emily Steel at emily.steel@wsj.com⁵

URL for this article:

<http://online.wsj.com/article/SB118480608500871051.html>

Hyperlinks in this Article:

- (1) <http://tomshardware.com>
- (2) <http://CNET.com>
- (3) <http://TV.com>
- (4) <http://Advertising.com>
- (5) <mailto:emily.steel@wsj.com>

Copyright 2007 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.