ADWARE

# The Hidden Money Trail


**Those programs that pelt you with ads and bog down your PC are financed by some of America's largest companies.**

BY DAN TYNAN AND TOM SPRING

ALLISON SMITH WILL NEVER FORGET the week before Memorial Day 2005.

Roaming the Internet looking for some free clip art, Smith found a site that looked perfect. But before she could download as much as an icon, her PC was infested with adware.

"All of a sudden I was besieged with pop-up ads," says Smith, a CPA who runs an accounting firm in Conway, Arkansas. "Boom boom boom boom boom—I had so many Internet Explorer windows [open] that they completely stalled my computer."

Many of the ads Smith saw on her desktop bore a calling card from their creator: an ▶

ILLUSTRATIONS BY STUART BRADFORD

**31%** of businesses rate spyware as a major threat for the next year. [DELOITTE GLOBAL SECURITY SURVEY, 2005]

adware program called Aurora, made by New York-based Direct Revenue.

Using another computer, Smith googled "Aurora" to learn more. She ineffectively tried using anti-spyware programs to remove it, tried killing the adware using Task Manager, and eventually hired a computer technician, who spent three days (at $50 an hour) trying to fix the problem. Each time he removed the software, she says, it would automatically reinstall itself under a different name.

Between repairs and lost revenue from downtime, Smith says her adware debacle cost her close to $5000. "What really surprised me was that the ads were from reputable companies, names you'd recognize," she says. "I got really angry that legitimate businesses would advertise their products using a program like this."

Smith's experience is not that uncommon. Many companies' products and services are promoted via adware, software that runs on a user's PC and displays ads, often in response to your Web activities. When we installed various adware programs on test PCs, we saw ads from such well-known brands as Chrysler, Expedia, Microsoft, Priceline, and Travelocity.

Direct Revenue's CEO, Jean-Phillipe Maheu, doesn't dispute that Smith had Aurora on her PC. But, he says, Aurora doesn't pop up as many ads as Smith complained about, indicating that she likely had more than one type of adware installed on her PC. Maheu said his company doesn't condone "drive-by installations," in which the software is loaded on PCs without alerting the user. If Direct Revenue finds that a partner is using this tactic, Maheu says, Direct Revenue severs ties with the partner.

**Estimates of the annual revenue of the adware business range from $200 million to $2 billion.**


**NASTYWARE: CoolWebSearch puts links to advertisers on any Web page you visit. Site owners have no control over the links.**

## IS ADWARE SPYWARE?

ARE PROGRAMS LIKE the one that hit Smith's computer *adware* or *spyware*? Depending on who you ask, experts define the word spyware differently.

Some use the word to describe tools that steal passwords and other personal data. Others consider a program spyware if it installs itself without your clear knowledge and permission. So the same program could be considered spyware or adware, depending on the circumstances under which you got it.

It's surprising to find that nobody knows for certain how much money the adware industry takes in annually—estimates range from $200 million to $2 billion a year in revenue—but if investments are any indication, business is booming.

Venture capital firms are bullish on adware companies, including Direct Revenue, WhenU and 180solutions. According to SEC filings, Technology Investment Capital invested $4.4 million in Direct Revenue, after giving them $6.7 million last year. Trident Capital committed $15 million to WhenU this past summer. And, last year, Spectrum Equity invested $40 million in 180solutions.

How do VCs explain giving money to companies who monitor users' Web browsing habits? "Adware is here to stay," says Venetia Kontogouris, a managing director at Trident Capital. "Privacy for the [Internet] consumer is a lost war."

Adware makers and their funders are only one part of this complex new industry; millions of dollars also come from advertisers, and from the ad brokers who work for them. These people in turn pay search engines (on which brokers place ads), software bundlers that distribute adware, and vast networks of affiliates and subaffiliates. (See "Following the Money: How Adware Gets on Your PC," page 74, for an illustration of the process.)

## A LONG, WINDING ROAD

THE PATH ADWARE takes to get on your PC is murky. Many intermediaries help adware do its job, for a cut of the profits.

Typically, an advertiser hires a broker or an ad agency to purchase ad space. The broker or agency buys space from adware firms, like Claria or WhenU.

The adware makers have myriad ways of getting their program on your PC. You can get it directly from the adware company when you download software, like Claria's ScreenScenes screen saver and Gator eWallet software. Or you may have to get adware in order to access Web-based games or other online content, such as that found on Zango.com, a site owned by 180solutions.

Many adware companies also have networks of partners that help distribute and promote their adware. *Bundlers* package adware with other programs—for example, we received WhenU's Save when we installed the BearShare file sharing program. *Affiliates* help market the adware by, for example, buying keyword-based ads on search engines; they may

**27%** of small or medium-size businesses do not use an anti-spyware product. [FORRESTER RESEARCH, 2005]

also purchase banner ads on Web sites.

Reps from several adware companies say they hold their business partners, affiliates included, to a code of conduct that forbids secret, or "drive-by," downloads.

But, because affiliates can be swayed by the potential to earn a lot of money quickly and often operate with little or no oversight, some go "rogue" and use stealth installations or other deceptive tactics to force adware onto PCs. Affiliate programs are "where bad things happen," according to Direct Revenue's Maheu.

PHOTOGRAPH: STEVE JONES

## BATTLING ROGUES

ROGUE AFFLIATES both help and harm adware makers. On one hand, they do a remarkably good job of getting the adware installed on PCs. On the other, rogues can anger consumers, embarrass advertisers, and draw lawmakers' ire.

Adware companies we spoke with say they don't tolerate rogue affiliates. Companies cancel affiliate contracts if someone complains, and some conduct internal investigations to ferret out rogues.

**"I GOT REALLY ANGRY THAT LEGITIMATE COMPANIES WOULD ADVERTISE THEIR PRODUCTS...LIKE THIS."**

**–ALLISON SMITH, TAX ACCOUNTANT WHOSE OFFICE PC WAS INFESTED WITH ADWARE**

Direct Revenue's Maheu, who joined the company in May 2005, says "we give our distributors our guidelines, and if they don't comply, we shut them off." He adds that the company recently cancelled distribution agreements with 8 of the 30 distributors Direct Revenue works with.

"All our distribution will be affiliate-free by the end of the year," Maheu says.

But not all companies are getting rid of affiliates. Affiliates distribute about 80 percent of 180solutions' adware, notes Sean Sundwall, director of corporate communications, adding that he characterizes as "rogues" less than 5 percent (or fewer than 500) of the company's roughly 8000 distribution partners. Last January, 180solutions hired a team to identify and remove deceptive distributors.

In June, 180solutions also took the unusual step of sending pop-ups to 20 million users to notify them that they had its software installed, and to provide removal instructions. In August, the company sued seven former distributors for surreptitiously distributing its software via networks of "zombie" PCs; each zombie was infected with a Trojan horse that let the rogue affiliate control the PC.

## FAIR WARNING?

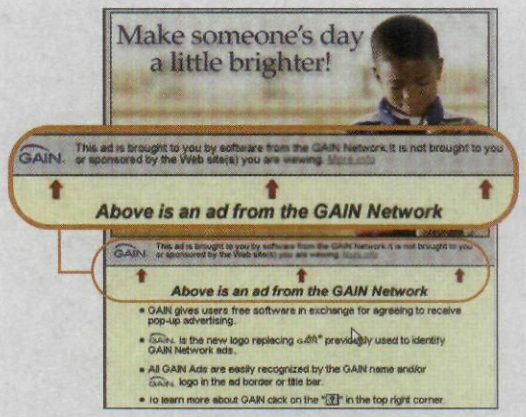
EVEN AS ADWARE companies are going after rogue behavior by affiliates, some of them continue to act in ways that privacy-sensitive consumers consider deceptive.

Not all bundled programs give you a clear warning about the adware you're about to install. In some cases, a disclosure may be buried many paragraphs deep in an End User License Agreement (or EULA) that you may or may not read. Even a careful EULA reader might not realize that a paragraph about "third-party software downloads" is, in fact, a subtle reference to adware.

In contrast, when you install the free BearShare peer-to-peer program, you must agree to EULAs from both BearShare and WhenU. You'll see screens describing this "ads for apps" trade-off before and after the installation.

Many prominent adware firms also label their ads. In our testing, we saw Direct Revenue's labels for Aurora appear on the title bar of its ad windows. 180solutions included an icon in the title bar. And Claria and WhenU put both the ▶

**33%** of scanned enterprise PCs were infected with adware. [WEBROOT STATE OF SPYWARE, Q2 2005]




**GAIN'S NOTICE on the first Claria ad you see explains how the company identifies itself.**

name of the adware application and its logo in one part of the advertising window.

But while some adware companies are trying to make their activities more transparent, other companies do anything they can to obscure their origin. CoolWebSearch (CWS) is a prime example.

All of the more than 40 variants of CWS get on your PC by means of drive-by installations, or by exploiting other security bugs, according to anti-spyware experts. CWS has no EULA, or even a Web site. (The owners of the coolwebsearch.com domain posted a notice disavowing any affiliation to the CWS spyware program, but didn't respond to requests for comment.) And none of the CWS ads we saw in our tests were labeled.

In fact, even the authorities don't know who's behind CWS: The individuals and companies involved shroud themselves in secrecy, using a jumble of servers, located all over the world, to obscure their network, and registering domain names using fake contact information.

In our tests, CWS inserted its own links into Web pages displayed in Internet Explorer. Clicking one of these CWS-inserted links brought us to "search portals"—sites designed to mimic search results pages from Google or MSN Search—featuring ads from well-known companies. The tested version, and other variants of CWS, also add bookmarks to the Internet Explorer Favorites list; put shortcuts to porn and gambling sites on the desktop; change your browser's home page; and/or alter browser security settings. It also actively fights your attempts to remove it from affected PCs, using techniques similar to those viruses use.

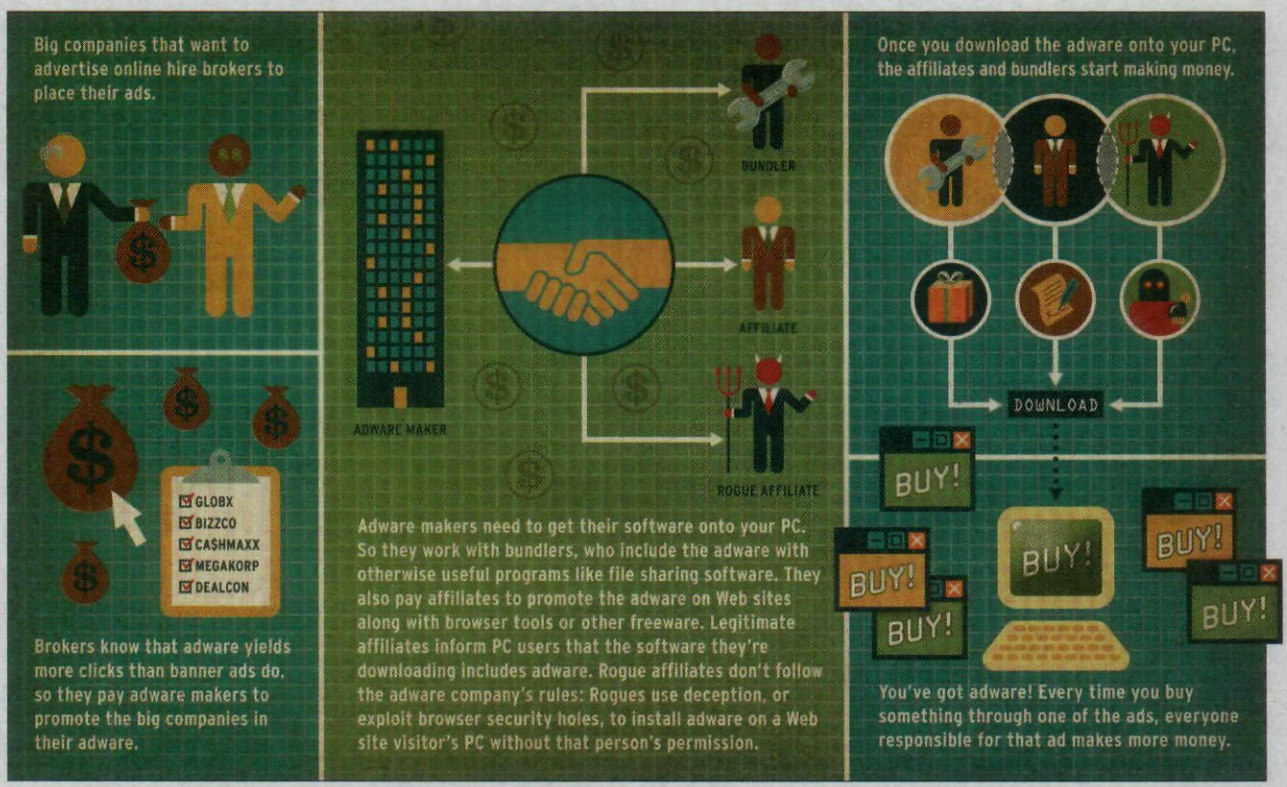
## WHEN ADS GO BAD

COMPANIES THAT say they want no part of adware may end up promoted through adware pop-ups anyway, due to the complex networks of partners and affiliates.

At one time Dell had affiliate relationships with both 180solutions and adware vendor Exact Advertising, but not anymore. "We do not advertise via adware," says spokesperson Jennifer Davis. "And if we learn of a partner of ours doing so, we investigate and deal with it."

However, when we clicked a CoolWebSearch link, it led us to the Dell homepage. But not directly: In the space of a few seconds, our browser loaded a series of Web pages automatically, jumping ▶

## » FOLLOWING THE MONEY: HOW ADWARE GETS ON YOUR PC




INFOGRAPHIC: HEADCASE DESIGN

**80%** of scanned consumer PCs were infected with spyware. [WEBROOT STATE OF SPYWARE, 2Q 2005]

from a CWS search portal, through Abcsearch.com, FindWhat.com, and Resolution Media's site, before ending up on Dell's site. As each new page loaded, a server recorded the affiliate ID. URLs that contain affiliate IDs make it possible for affiliates to get paid for each click.

We interviewed the companies involved to find out how the deal happened. Dell hired Resolution Media, a search-engine marketing firm based in Chicago, to purchase ads on Dell's behalf. Resolution Media placed ads with several small search engines, including Miva's FindWhat.com. FindWhat distributed the ads to its network of search affiliates, including Internext Media's Abcsearch.com. According to Abcsearch vice president David Senet, one of the site's subaffiliates (whom Senet declined to name) placed the Dell ad on the page that our CWS-infected PC brought us to.

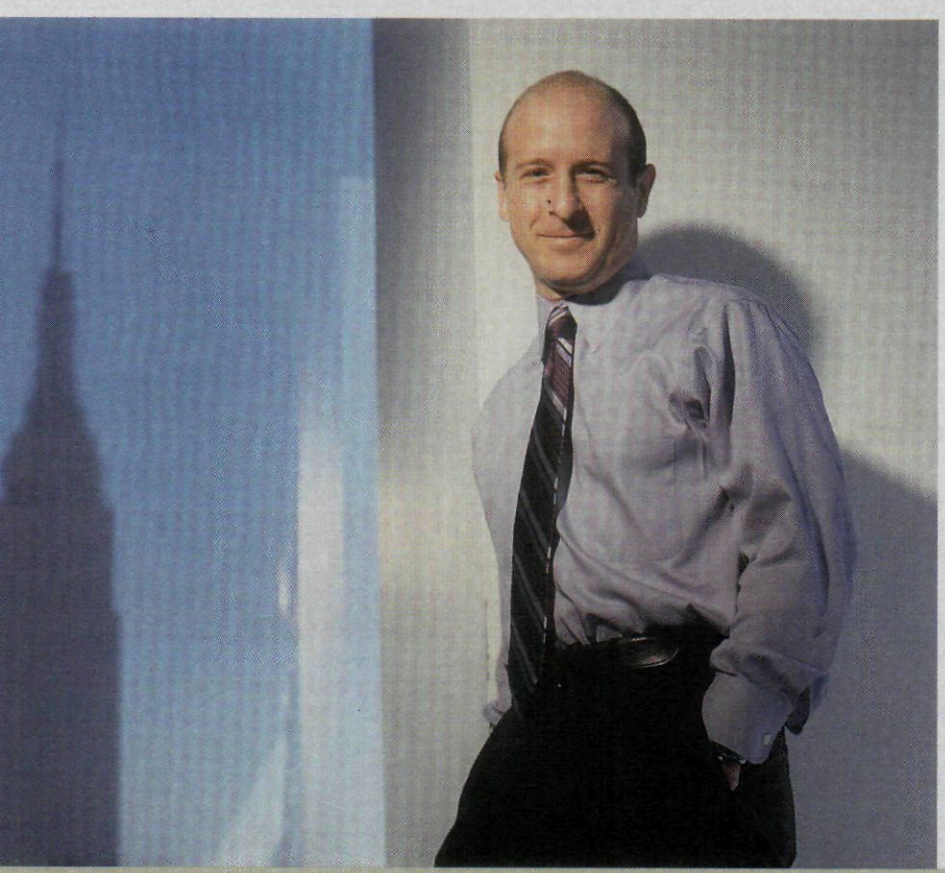
Following our discussion with Dell, the company said it terminated its relationship with FindWhat.com, and Abcsearch said it no longer uses the unnamed affiliate. All of the firms we contacted claim that when they detect fraud, the advertiser isn't charged and the affiliate isn't paid.

We also saw the Netflix logo appear—alongside those from American Express, Citibank, and Toshiba—in ads displayed by Metareward.com on Direct Revenue's ABetterInternet adware (a predecessor to Aurora that, according to Maheu, his company longer distributes).

Netflix director of corporate communications Steve Swasey said the company forbids the use of adware by its affiliate partners; he confirmed that Netflix partnered with Metareward, but not Direct Revenue. Metareward did not respond to requests for comment; the company is a division of Experian (one of the big three credit reporting agencies).

Consumer advocates insist that all parties involved in the ad industry must do a better job of policing their practices.

"The question becomes, 'Can't you think of some way to design a system that's not such an invitation for scams, fraud, cheating, lying, and thievery?'" asks anti-spyware advocate Ben Edelman. "Is this really the best you can do?"



## PAYDAY FROM CLICKS

WHILE SOME ADVERTISERS stumble into adware unawares, others are unapologetic about their use of it.

"We wouldn't do it if it wasn't effective," says Kelly Ford, vice president of marketing for New York–based Travelzoo, a media company specializing in such clients as airlines and online travel sites.

Ford's company works with Claria and Soho Digital, an arm of Direct Revenue. However, he says Travelzoo spends only a small percentage of its total media budget on adware contracts. "We try to do just enough to make an impression in the marketplace without being overly intrusive," Ford explains.

"Advertisers are a notoriously demanding bunch," notes Trevor Hughes, executive director of the Network Advertising Initiative, a trade group for online advertisers. "If adware pop-ups didn't work, they wouldn't buy them."

Still, many advertisers and agencies shy away from using adware. Avenue A/Razorfish, which places ads with 180solutions and Claria, says less than 2 percent of its total billings went toward adware in the first quarter of 2005.

**"WE HAVE TO DO AN OVER-THE-TOP GOOD JOB OF PROTECTING USERS' PRIVACY IF WE'RE TO GAIN THEIR TRUST."**

**–AVI NAIDER, PRESIDENT OF WHENU, AN ADWARE COMPANY**

PHOTOGRAPH: JOHN ABBOTT

**65%** of businesses plan to invest in new or additional anti-spyware tools. [FORRESTER RESEARCH, 2005]


**COOLWEBSEARCH REDIRECTIONS like this one often lead to the Web sites of large, well-known companies.**

## FROM ADWARE TO NOWHERE?

ADWARE VENDORS want to legitimize their business model; to do so they must obtain users' informed consent before they install adware on PCs. But nearly 80 percent of people who get adware end up uninstalling it (according to several adware executives), so it's clear most people don't want the programs.

If adware companies don't clean up their act, Uncle Sam might do it for them. Congress is considering a handful of anti-spyware bills, including the SPY BLOCK Act (S. 687) and the Spy Act (H.R. 29). Both would penalize companies that engage in deceptive practices, secretly install software or secretly collect data about users, or make software difficult to remove. Senate Bill 687 has yet to be voted on, while the Spy Act has passed the House and was in Senate committee at press time.

Consumer advocates aren't optimistic about the proposed regulations. "Laws alone won't do that much to stop spyware," cautions Ari Schwartz, associate director of the Center for Democracy and Technology. Schwartz says spyware legislation will likely make some forms of intrusive behavior lawful.

### » MORE ON THE WEB

FOR THE LATEST reports from Ben Edelman about adware companies, visit benedelman.org. Got spyware yourself? Find help at spywarewarrior.com.

With an eye toward compliance with the potential adware laws, some adware companies are trying to use less-obtrusive, or more-targeted, ads to convince users to keep the apps.

Earlier this year Claria announced its BehaviorLink adware program. Instead of delivering pop-ups, it will embed highly targeted ads into pages on Web sites that have signed up with the company. So if you just had a baby, for example, prepare for a steady diet of diaper and infant-formula ads.

Claria manages this process by collecting a trove of non–personally identifiable data about each user, such as marital status, zip code, age range, and gender. Mainstream applications, such as instant messaging clients and media players, will bundle BehaviorLink.

"We don't want to be on 40 to 50 million desktops, we want to be on 140 million to 250 million desktops," says Scott Eagle, Claria's director of marketing.

WhenU's Save app targets ads based on a user's surfing habits, says president Avi Naider, but Save doesn't send that data to WhenU—it stays on your PC.

Naider says he hopes that cleverly designed, targeted ads and an unusual level of openness about his company's business practices will convince users to keep WhenU installed.

"Given the history of the adware industry, we have to do an over-the-top good job of protecting users' privacy if we're to gain their trust," he says.

Real change in adware practices may be on its way. But until most PC users are convinced that adware makers have truly changed the way they do business, trust in these vendors' promises may remain elusive. And one way or another, the ads will keep on coming. ■

*PC World Contributing Editor Dan Tynan is author of* Computer Privacy Annoyances *(O'Reilly Media, 2005). Tom Spring is a senior reporter for* PC World. *Senior Associate Editor Andrew Brandt also contributed to this story.*


## Spy-Free Computing

THESE STEPS CAN help keep spyware and unwanted adware off your system.

- **Use firewall and antivirus software:** Antivirus tools may be able to prevent an accidental installation. A firewall, such as ZoneAlarm, that watches applications can notify you if an adware program decides to phone home—and can put a stop to it.
- **Use Internet Explorer only when absolutely necessary:** ActiveX makes IE vulnerable to some drive-by installations. Alternative browsers, such as Firefox or Opera, don't use it.
- **Avoid sketchy sites:** Certain kinds of Web sites—particularly some that offer hacking tools, free spyware scans, porn, and the like—tend to attempt drive-by installations.
- **Check the EULA on each download:** Beware of EULA references to "third-party applications" that download advertising or their own updates.
- **Spurn "warning" pop-ups:** Ads that look like a Windows dialog box and warn that you have spyware installed are just slick come-ons designed to lead you to sites that actually install spyware. Instead, use a known spyware remover—like the ones we review in "Best Defenders," on page 85.