

Some Google Ads Found to Spawn Spyware

By [Kate Kaye](#)

April 27, 2007

Online advertising has long been plagued with connections to spyware, and now the seedy spyware underground has moved from pop-up networks to Google's search ad network. Discovered by security software firm Exploit Prevention Labs earlier this month, AdWords ads were used in attempts to install spyware on users' computers. Though Google said it has removed the offending ads and may have terminated the AdWords accounts set up by the culprits, the question remains whether such a response is enough to dissuade future exploitation.

According to Exploit Prevention Labs, an ad that appeared to be promoting The Better Business Bureau was detected by its Web surfing security software as linking to a "dangerous" site. If users clicked through, they'd initially travel through the smartrack.org domain, which attempted to install spyware. If installed, the spyware was intended to alter online banking pages to capture users' personal data. After rapidly passing through the smartrack domain, users were redirected to visit the legitimate Better Business Bureau site, according to Exploit Prevention Labs.

The software firm tracked the early April registration of the smartrack domain by a previously known spyware culprit, and according to its records, believes the offender created Google AdWords sponsored link campaigns by April 10. Exploit Prevention Labs provided a screenshot of the mock Better Business Bureau ad to back up its claim. The company said a search on the phrase, "how to start a business" also resulted in a spyware-driven sponsored link disguised as an AllBusiness.com ad.

"This is a clever way by the bad guys to elevate themselves to the first page," said Roger Thompson, CTO of Exploit Prevention Labs, referring to the Google AdWords buy.

"We cancelled the affected ads as soon as we were made aware of the problem," Google spokesperson Diana Adair told ClickZ News in an e-mail. It is unclear whether the company also terminated the account or accounts associated with the ads, or what other actions the firm has taken in response. Google did not respond to further questions from ClickZ News in time for publication.

Thompson said its system showed Google removed the ads on April 24. His firm detected between 20 and 30 other keyword search phrases that resulted in links connected to the smartrack domain, including "auto show" and "mgm.com original sin." The firm is not sure if those links were included in Google's organic listings or paid search ads.

According to Thompson, the smartrack attempt is the first of its kind his company has come across. "We have not seen other search engines used so far for this," he said. Other search engines, he added, "are probably equally vulnerable" to unwittingly participating in such attacks. In addition to Google, Thompson's firm's software also tracks MSN and Yahoo.

Spyware watchdog Ben Edelman said he has seen a similar spyware-disguised sponsored search link while conducting his own research. What Exploit Prevention Labs found, he said, "Is not unprecedented, but it is important." The Harvard Business School assistant professor and [longtime spyware tracker](#) noted closing the spyware-purveyors' AdWords accounts is only a temporary solution, as the account holder can simply open another account.

Edelman wondered whether Google would sue the culprits since they submitted contact and credit card information when registering for the AdWords account. Even if that information does point to the actual perpetrators, Edelman agreed Google wouldn't necessarily benefit from drawing attention to the problem.

Thompson also recognized Google's dilemma. "Poor old Google is probably doing the best they can," he said. "It's their business model that they make it easy to buy keywords."