



# InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

## Phony Ad On Job Sites Leads To 100,000 Stolen Identities

The Trojan stealing the data was hidden in a fraudulent advertisement on online job sites like **Monster.com**.

By Sharon Gaudin, [InformationWeek](#)

Aug. 17, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201800958>

Security researchers have unearthed the single largest cache of stolen identities, thanks in part to a Trojan stealing the data that has been hidden in a fraudulent advertisement on online job sites like **Monster.com**.

Don Jackson, a researcher with security company SecureWorks, told *InformationWeek* that he [found 12 data caches](#) connected to one group using the latest variance of the Prg Trojan, which also is known as Ntos, Tcp Trojan, Zeus, Infostealer.Monstres and Banker.aam. Several of the 12 found caches contain information on about 4,000 to 6,000 identity theft victims, but one contains about 10,000 and the largest one contains 46,000.

He estimates that between the 12 caches, there probably is information on about 100,000 stolen identities.

"That's at least four times as large as the largest ones I've run across before," said Jackson. "That tells me they're using a lot of different methods to do what they do or they've found really reliable methods to do it."

Jackson calls the identity theft organization behind the caches the "car group" because they've named each of the servers storing the information for a different auto manufacturer, like Ford, Mercedes, Chrysler, and French carmaker Bugatti.

The data, which includes bank and credit card account information, Social Security numbers, online payment account usernames and passwords, comes from victims who were all individually infected with the Trojan beginning in early May.

He said the latest variant of the Prg Trojan has been running on fraudulent ads on at least two online job sites. One, he said, is [Monster.com](#). Representatives from Monster did not return a request for an interview.

"The hackers behind this scam are running ads on job sites and are injecting those ads with the Trojan," said Jackson. "When a user views or clicks on one of the malicious ads, their PC is getting infected and all the information they are entering into their browser, including financial information being entered before it reaches the SSL-protected sites, is being captured and sent off to the hacker's server in Asia Pacific."

Jackson said one server is still collecting stolen data and they are seeing 9,000 to 10,000 victims sending information to the server at any one time. When someone clicks on the advertisement, they're taken to a malicious Web page where their computer is infected with the Prg Trojan.

He said they've given information about the caches and the phony ads to the FBI. Jackson also said they tried contacting **Monster.com** but they haven't received a response yet.

"When I first discovered this large cache of data, I couldn't figure out how the hackers were compromising so many Web sites, and as a result, infecting so many victims," added Jackson. "However, when I uncovered the Trojan-injected advertisements, it made total sense. These job sites get tons of traffic so it is no wonder that the hackers are having such success."

The Trojan is designed to exploit several different software flaws, including vulnerabilities -- all of which have been patched by the vendors -- in Microsoft's Internet Explorer browser, WinZip and Apple's QuickTime.

Jackson said they found the caches by writing signatures that detect the Trojan communicating with the hackers' command server, which sends out instructions to the malware and accepts data from it. Researchers followed the traffic back to several servers. He said some are located in the Russian business network, others are in Hong Kong, and they believe the major cache is on a server in Malaysia.

Different hacker groups are selling a kit that helps malware authors compile new versions of the Prg Trojan. The kit, which sells for about \$300 on underground forums and marketplaces, even re-scrambles the code to evade anti-virus detection.

SecureWorks noted that computers infected with the Prg Trojan will have a backdoor proxy server listening for connections on Port 6081. "This port is in not assigned to legitimate services and is not hidden by the rootkit functionality. f port 6081 is open on your computer, you are likely infected with the Prg Trojan," said Jackson. "If anti-virus is not detecting the infection, then you will need to boot the computer into Safe Mode and run another scan. If that fails, manual removal or reinstalling the operating system may be necessary."



Copyright © 2007 [CMP Media LLC](http://www.informationweek.com)