



Don't paddle around!
Summer deals end Sept. 28!

Trojan Hidden on Job Search Sites Steals Personal Data

August 17, 2007


By Brian Prince

SecureWorks researchers have uncovered a cache of stolen data from 46,000 victims of a variant of the Prg Trojan that has been used to swipe personal information from unsuspecting visitors to job sites.

ADVERTISEMENT

STATE GOVERNMENT SAYS LINUX WAS TOO BIG A RISK

"We can't take big risks with our technology," said Paul Campbell, former Director of the Illinois Department of Central Management Services. "State government needs trusted, tested technology that's reliable and predictable."

 Windows Server²⁰⁰³

[STORY CONTINUES >](#)

Experts at the Atlanta-based security company said the information includes bank and credit card account numbers, social security numbers and passwords. The victims were infected—and in numerous cases re-infected—by ads on popular, online job sites, including Monster.com during the past three months.

RELATED LINKS

[Keylogging Trojan Dodges Anti-virus Detection](#)

[SecureWorks Offers Free Security Tools](#)

[MessageLabs Reports Rise in Targeted E-Mail Attacks](#)

[Trojan Piggybacks on Windows Updater](#)

[Super Bowl Site Hacked with Trojan, Keylogger](#)

The hackers behind the attack are running ads on the sites and injecting those ads with the Trojan. When an user views or clicks on one of the malicious ads, their PC is infected and all the information entered into their browser, such as financial information entered before it reaches SSL protected sites, is captured and sent off to the hacker's server, according to SecureWorks researcher Don Jackson.

To read about how a Superbowl Web site was hacked using a Trojan, [click here.](#)

The data cache is run by an organization called the "car group," Jackson said, which is believed to be running a total of 12 servers involved in the attacks. The Car Group got its name because they use car names such as Ford and Mercedes in their attacks. In addition, eight other servers around the world are collecting and storing data stolen by the Trojan.

"What this is an indicator, though, of is [that] this is one of...the top...two Trojans in the world as far as distribution right now, as far as the total number of data caches found by SecureWorks and other organizations that track these things," Jackson said.

Anti-virus vendors say they are writing file-based signatures to address the Trojan, which it is easily able to evade by changing a couple bytes of code.

"This Trojan uses its own packer...it compresses and changes the code around," he said. "This packer is unique to this Trojan. It was written specifically for it, and the construction kit that produces the executables is very, very good at putting instruction substitutions, giving a long string of instructions for a simple task and putting garbage code or null operations in there, so that it is hard for anti-virus. Anti-virus has not been able to pick a stub...that they can identify reliably from file to file."

Prg appears to be a variant of a Trojan known as wns poem that was discovered by SecureScience and analyzed by Michael Ligh late last year.

According to Jackson, many people are getting re-infected five or six times because their computers are unpatched and they are unaware of what sites pose a danger. The ads are pointing to an exploit kit called Icepack, he added, which looks for various old vulnerabilities on PCs.

"I've seen one guy get infected 100 times," he said. "It is not uncommon to see people with the same infection IDs."

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

Copyright (c) 2007 Ziff Davis Media Inc. All Rights Reserved.