# Anti-theft software could create security hole

July 31 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- A piece of anti-theft software built into many laptops at the factory opens a serious security hole, according to research presented Thursday.

The "Computrace" software, made by Vancouver-based Absolute Software Corp., is part of a subscription service that's used to find lost or stolen computers. Many people don't know it's on their machines, but it's included in computers from the biggest PC makers.

The software is built into computers at the factory because that embeds it so deeply that even the extreme act of uninstalling the operating software won't delete it. The software is included in a part of the computer known as the BIOS, which refers to programs used to boot the computer.

The service Absolute sells can be valuable because sensitive data can be purged remotely from a stolen machine. The computer is still able to reach out to a specially designated Web site for instructions even if a criminal is tampering with the machine.

But research by Alfredo Ortega and Anibal Sacco with Boston-based Core Security Technologies, and presented Thursday at the Black Hat security conference here, shows it can cut two ways.

If a criminal has infected a computer that has the Computrace technology, he can take deep control of a machine.

That's because he's able to modify the computer's settings to maintain a connection with that machine even if the operating software is uninstalled then reinstalled - an extreme way, but sometimes the only way, to make sure a computer is cleaned of viruses.

"You have something that's pre-installed, and considered non-malicious, that you can manipulate and turn into a malicious program - that's pretty unique," said Ivan Arce, Core Security's chief technology officer.

Arce said Absolute can fix the problem with an update to the software that is then pushed out to affected computers. He added that users can disable the software's ability to be a problem on their own, too. It takes some technical know-how, though.

"It's not hard to block once you know what to look for," Arce said.

Absolute spokesman Craig Clark said the company would comment after Core's presentation Thursday, but then did not make anyone available. He said Absolute's technical team "needs to understand the concerns Core has raised before they can speak to it accurately."

Roel Schouwenberg, a senior antivirus researcher with Kaspersky Lab, said the vulnerabilities Core Security found could be a "pretty big challenge for the security community" if they're exploited. But he added that the special access a hacker can get is undermined somewhat by the fact malicious programs they try to download still have to come into the computer the same way they always do, and can be protected against.

Any files that download "will not be stealth, they will not be hiding, they will be visible on the system," Schouwenberg said. "Anti-malware (software) will be able to scan them. It could have been a whole lot worse."

---

On the Net:

View Core Security's research paper at:

http://www.coresecurity.com/content/Deactivate-the-Rootkit