

### **Safe Transactions with Infected PCs**

A new tool assumes that a PC is loaded with malware--and protects transactions anyway

*Technology Review*

Erica Naone

September 15, 2008

<http://www.technologyreview.com/Biztech/21370/?a=f>

Your computer has been breached by malicious hackers: it's completely loaded with malware and spyware. You're about to get online, connect to a financial institution, and make some transactions. Is there anything, at this point, that can keep your identity off the black market? SiteTrust, a tool released today by Waltham, MA, data-security company Verdasys, aims to protect users from fraud, even when their computers have been compromised.

"Malware is on the rise," says Verdasys chief technology officer Bill Ledingham. Many existing protection technologies don't work against all the malware that's out there, he says, partly because they're built to protect against known attacks. Users, he adds, are often inconsistent about employing antivirus software and keeping it updated, and even when they're not, some malware is sophisticated enough to get through anyway. "Our premise," Ledingham says, "is that, rather than trying to clean up the machines, assume the machine is already infected and focus on protecting the transaction that goes on between the consumer and the enterprise website."

The problem of malware on users' computers is "the number-one problem that the financial institutions are wrestling with today," says Forrester Research senior analyst Geoffrey Turner, an expert on online fraud. Financial institutions can take steps to secure the connections between their servers and their customers' PCs, Turner says; they can even ensure the security of the customer's Web browser. But they're stumped, he says, when it comes to the customer's operating system. Most successful attempts to steal computer users' identities, Turner says, involve using malware to capture their credentials or conduct transactions behind the scenes without their knowledge. "The challenge is, how do you secure the end-user computer?" he says. "Should you even, as a bank, be trying to do that?"

Verdasys thinks that the answer is yes. After licensing SiteTrust from Verdasys, a financial institution would provide it to users as a supplement to their existing antivirus software. Once SiteTrust is downloaded and installed, Ledingham says, it takes up less than a megabyte of disk space. When the user is connected to a protected site, SiteTrust consumes 1 to 2 percent of the computer's processing capacity. While the tool could work with multiple sites, the initial idea is that a customer would receive it for use with a specific website.

SiteTrust bypasses malware because it is essentially a rootkit--a program designed to bury itself deep in a user's operating system, where it can take fundamental control of most of the software running on the machine. The idea, Ledingham says, is that SiteTrust will burrow down to a lower level than any malware on the system. Verdasys has put a lot of research into ensuring that SiteTrust does just that, Ledingham says, but he acknowledges that if the tool becomes successful, online criminals will probably focus on finding ways to go even deeper. He says that Verdasys plans to keep improving the tool, hoping to stay a step ahead of attackers.

When the user types in the URL of a protected site, Ledingham says, SiteTrust steps in. Without changing the appearance of the user's screen, SiteTrust separates the secure transaction from whatever else might be going on in the browser by running a fresh version of the browser code as its own "process." (A process is the series of commands that the computer executes to run a program, and modern computers can run dozens of them at once.) SiteTrust then monitors this process to make sure that no other program tries to interfere with it. As the user interacts with the site, SiteTrust bypasses many of the vulnerabilities of the operating system, instead taking information from the user's keyboard, encrypting it immediately, and sending it to the website. SiteTrust currently runs on Windows machines and works with the Internet Explorer and Firefox browsers, but Ledingham says that the company is working on Linux, Mac, and Safari versions.

SiteTrust is a new application of the technology behind Verdasys's existing product, the Digital Guardian, which is meant to protect businesses against internal theft. The Digital Guardian also uses a rootkit, installed on every computer in an organization, that watches what users do with sensitive information and flags suspicious behavior. Ledingham notes that, although rootkits have caused controversy in the past, particularly when they were installed without users' knowledge, Verdasys has years of experience designing them so that they don't interfere with a computer's normal use. SiteTrust, Ledingham says, includes an uninstall option so that users can completely remove it if they choose, and it doesn't send any background information about the user to the protected site.

Turner says that he appreciates Verdasys's approach with SiteTrust--in particular, the way that the company has planned for the inevitability of online criminals' targeting the tool itself, lining up improvements to make that more difficult. He adds that the company's distribution model is important to getting SiteTrust to consumers. "People aren't aware that they need this level of protection on their own PC," Turner says. Customers aren't likely to look for additional protection unless encouraged to do so by financial institutions that they trust. Turner also notes that receiving the tool from a trusted institution should help counter consumers' general worries about rootkits.

SiteTrust is launching to six million customers of an undisclosed online broker in the near future. The company plans to make additional deals to protect other websites.