

Verdasys Says it Has A Better Way to Protect Web Transactions Against Malware

Xconomy

Wade Roush

September 15, 2008

<http://www.xconomy.com/boston/2008/09/15/verdasys-says-it-has-a-better-way-to-protect-web-transactions-against-malware/>

It may sound strange, but there's a computer security company just outside Boston where the engineers have declared that the conventional battle against viruses, worms, Trojan horses, and other forms of computer malware is already lost.

Norton, McAfee, and other anti-virus companies may still make millions selling consumers software that promises to keep computers malware-free. But these solutions stop barely half of the malware attacks these days, say the folks at Waltham, MA-based Verdasys. So the only sure way to protect sensitive data—say, when a bank's customers are online, managing their accounts—is to assume that their computers are compromised, and keep the data out of malware's reach.

That's the strategy behind SiteTrust, a new service that Verdasys is launching today for banks, brokerages, and other big companies that serve customers over the Internet—and that are legally liable for losses from online fraud. A privately backed company founded in 2003, Verdasys has served many of these same companies for years with a product called Digital Guardian that keeps sensitive data from slipping outside a company's walls. SiteTrust is its first foray into the consumer world.

“The leading anti-virus products today are only about 50 percent effective against the current crop of malware, let alone against some of the newer techniques that do a much better job of hiding themselves,” says Bill Ledingham, Verdasys' new CTO. “A lot of our online-broker customers, given the losses they are encountering, need a new approach. Given that malware is already resident, how do we insert ourselves and protect just the transaction that is happening between the customer and the corporate website?”

In theory, it's easy to secure the data passing between a user's Web browsers and a corporate server by encrypting it using established standards such as SSL. But this technique doesn't work if the user's PC is infected with malware that's peeking at the data before it gets encrypted—for example, when a user is typing a password. Based on their experience creating Digital Guardian, which monitors and encrypts all proprietary or sensitive information passing through a desktop, laptop, or enterprise server, Verdasys engineers built a small client-side software package—a download less than 1 megabyte in size—that turns on whenever the user visits a website protected by the SiteTrust service.

This software—which is designed for Windows only, though Ledingham says the company is working on Mac and Linux versions—first spawns a new instance of the user’s Web browser, shutting out malware that may be eavesdropping on processes in other Internet Explorer, Firefox, or Safari windows. Then it inserts itself into the innermost operations of the user’s computer, creating a secure space around all communications with the protected site. Says Ledingham, “We immediately encrypt all input from the keyboard, bypassing other points of vulnerability in Windows.”

Ledingham says that since only the originating company’s Web servers have the keys needed to decrypt the data, the SiteTrust technology protects against all sorts of attacks, including keyloggers, unauthorized screen captures, code injection attacks, so-called “man in the browser” and “man in the middle” attacks, and phishing and website spoofing. In studies funded by Verdasys, two independent security consulting firms found that this approach was “100 percent effective against all known malware threats,” in the words of a company statement.

The SiteTrust concept is similar in spirit to an idea developed by Liquid Machines, another Waltham company whose “application injection” technology takes over word-processing programs, e-mail software, and the like, automatically encrypting digital documents and then decrypting them only for authorized users. But Liquid Machines’ system is designed for use within big enterprises and their business partners, whereas SiteTrust extends data protection to all of a company’s Web customers.

One of the top three online brokerage firms—Verdasys can’t yet divulge which one, though it says the firm has 6.3 million customers—has signed up as the first SiteTrust licensee. The firm won’t force its customers to download the SiteTrust software in order to keep accessing their online accounts, but it will probably offer them incentives to drive adoption, Ledingham says.

While SiteTrust marks the first time that the company will be putting software on consumers’ machines, conceiving the service wasn’t a huge leap. “The reality is that a lot of enterprise machines are compromised as well by malware, and a lot of our customers were seeing the anti-virus products decline in efficacy, so we were already having to develop this technology to protect data within the enterprise,” Ledingham says. “It was a logical extension to monetize that by selling it to companies who want to protect their consumer base.”