

Extra, Unintended Transactions?

You might be experiencing a ‘man-in-the-browser’ attack

By Lisa Hochgraf

September 2010

Dentists working at Smile Zone, a Springfield, Mo.-based dental practice, were left a bit numb on March 22. That day, organized computer criminals extracted more than \$200,000 from the company’s online bank accounts. The money was sent to nearly a dozen individuals around the country. The office manager said the money was taken in 11 different transfers, including three large wires.

During a recent free CUES Webinar, “The Quarterly Slant,” Ken Proctor cited the Smile Zone incident to illustrate how financial institutions and their customers are particularly susceptible to ZeuS malware—a type of “man-in-the-browser” attack. Proctor is managing director of Cornerstone Advisors Inc., Scottsdale, Ariz., CUES’ partner in *CUES Technology Edge*.

ZeuS malware specializes in mining online banking credentials and taking over (hijacking) sessions your member opens with you, Proctor explained. It often exists in the form of a browser plug-in that gets downloaded as part of a product. The embedded malware detects visits to financial institution Web sites and activates when users sign in to online banking. When the user opens the session with the financial institution, the criminals send their transaction requests on top of what the authentic user is doing. To the bank or credit union, these look like they’re being done by a legitimate user.

During the time the malware has access to the financial institution site, the victim’s computer, IP address and session are used for:

- form grabbing, in which Web form data is collected before it passes over the Internet;
- transaction manipulation and
- session hijacking.

In the case of the Smile Zone attack, both the customer company's employee and the bank had security breakdowns that allowed criminals to steal from them.

Smile Zone had a person responsible for paying some temporary employees, Proctor explained. The person used a home PC to access the bank account. When she opened a personal e-mail about "classmates," the PC was infected. The Smile Zone employee noticed the computer ran slowly for a time and was asking her lots of extra questions as she visited various banking sites, but thought her home virus protection was enough. (It wasn't.)

In turn, the bank from which the money was taken had sophisticated user authentication procedures in place, but didn't look at the transactions themselves to see if they were consistent with past transactions for that company, Proctor said. (They weren't.)

"There were some problems on both sides of that," he added. "Clearly the majority of the problem was the customer because she didn't maintain very good security. But then again, the bank had its own issues."

User authentication (even multi-factor authentication) will not prevent such an attack because the session was opened by a legitimate user, Proctor emphasized. That being the case, how can you protect your credit union and its members?

One-time, single-transaction passwords with a short usable life (instead of session passwords) are pretty much the only way to prevent this type of

attack, Proctor said. A fob that provides a transaction authorization code that's valid for 20 seconds is an example.

“It expires so it cannot be compromised,” he explained, “so the criminal cannot intercept it and have time to try and decrypt it, compromise the calculation of the code, send it back with a file that works. There just isn't enough time to overcome the control.”

An even stronger control is the one-time authentication code that is a “test”...a number that is calculated based in part on the transaction data and in part on information unknown/unknowable through the user's computer, Proctor said.

In addition, transaction alerting doesn't prevent this type of attack, Proctor continued, but it does allow someone to see if something unusual is going on. If you're looking for patterns of transactions and things don't match what you expect, it might be time to dig deeper.

“This malware was directly responsible for helping thieves steal tens of millions of dollars from small to mid-size businesses over the past year,” Proctor said. “It's important to ‘authenticate’ the transactions, not the user.”

Lisa Hochgraf is a CUES editor.

© 2010. CUES. All Rights Reserved.