



Hackers Steal \$150,000 from Mich. Insurance Firm

An insurance firm in Michigan lost nearly \$150,000 this month as a result of a single computer virus infection.

Port Austin, Mich. based United Shortline Insurance Service Inc., an insurance provider serving the railroad industry, discovered on Feb. 5 that the computer used by their firm's controller was behaving oddly and would not respond. The company's computer technician scoured the system with multiple security tools, and found it had been invaded by "Zeus," a highly sophisticated banking Trojan that steals passwords and allows criminals to control infected hosts remotely.

The following Monday, Feb. 8, United Shortline received a call from the Tinker Federal Credit Union at Tinker Air Force Base in Oklahoma, inquiring about a suspicious funds transfer one of its customers had received for slightly less than \$10,000.

After that call, United Shortline President Louis M. Schillinger said the firm found 14 other such unauthorized transfers had been made from the company's account to individuals across the United States who had no prior business with Shortline.

"I said, 'Oh my God, someone's just taken all of the money out of our trust account,'" Schillinger said. The hackers moved money from the company's trust account over to its operating account, and then made the illicit transfers from there.

Schillinger said the bank's commercial banking platform requires users to enter a user name and password. The bank's site occasionally asks users to "register" their computers if, for example, the customer is accessing his or her account from an unfamiliar PC. A customer might also receive such a prompt if his or her Internet address had changed. The registration process involves the customer providing the correct answers to a series of "challenge questions."

In any case, the crooks evidently had no problems correctly answering the secret questions when challenged with them, Schillinger said.

"The bank said whoever logged in to make these transfers successfully answered those questions," he said. "They had some very detailed information. [The thieves] knew our patterns, they knew our passwords, my mother's middle name, favorite sports team. And this is all information I don't even have written down anywhere."

Schillinger said his firm has been able to work with its bank, Bay Port State Bank, to recover a little more than half of the money so far. Still, he said, both his company and the bank are still in shock.

“Both my bank and us are looking at each other, asking what could we have done differently to prevent it?”

Bay Port State Bank President Ed Eichler said the bank moved quickly to stop and reverse the transactions as soon as it got the call from United. But Eichler said the bank will be reviewing its processes to figure out how to spot this type of activity more quickly in the future.

“We haven’t had this happen before,” Eichler said. “Before it was a story problem, and now it’s a real life problem. You can do all the training on this you want to, but most of that doesn’t matter until this goes to something that’s actually happened to you that you can put your hands on.”

Eichler said he contacted some colleagues at a much larger bank, and was told that recovering 50 percent of the victim customer’s funds was actually pretty good.

“The big banks told us to go to bed and get over it,” Eichler said. “They told us, ‘We write off more than that every day.’ But we’re not really interested in having this happen to another one of our customers.”

Businesses do not enjoy the same protections afforded to consumers hit by cyber fraud. With credit cards, consumer liability is generally capped at \$50. Consumers who report suspicious or unauthorized transactions on their ATM or debit card, or against their online banking account within two days of receiving their bank statement that reflects the fraud also are limited to \$50 in losses. But waiting longer than that can cost consumers up to \$500 (the liability is unlimited if a consumer waits more than 60 days to report the fraud).

Businesses have no such protection from fraudulent transfers. Generally speaking, banks will work with commercial customers to try and reverse any fraudulent transfers, but the chances of that succeeding diminish rapidly after the first 24 hours following unauthorized activity. What’s more, banks are under no obligation to reimburse commercial customers victimized by cyber fraud.

Unless and until regulators begin insisting that commercial banks assume more responsibility for monitoring customer transactions for anomalies that may indicate fraud, businesses would be wise to take basic precautions when banking online.

As I’ve advised previously, companies can insulate themselves from these attacks by simply using a dedicated machine for online banking. This may take the form of an inexpensive Windows netbook or laptop, for example, that is locked down, and used only for accessing the bank’s Web (and not for e-mail, casual browsing, etc). Alternatively, since 99.9 percent of all malware simply fails to load on non-Microsoft computers, using something other than Windows for online banking — such as a Mac or a Live CD solution — also is a very sound approach.