



IT Firm Loses \$100,000 to Online Bank Fraud

A New Hampshire-based IT consultancy lost nearly \$100,000 this month after thieves broke into the company's bank accounts with the help of 10 co-conspirators across the United States.

On Feb. 10, Hudson, N.H. based Cynxsure LLC received a voicemail message from its bank, Swift Financial, a Wilmington, Del. institution that focuses on offering financial services to small businesses. The message said to contact the bank to discuss an automated clearing house (ACH) payment batch that had been posted to Cynxsure's account.

The next day, Cynxsure's owner Keith Wolters returned the call and learned from Swift that someone had put through an unauthorized batch of ACH transfers totaling \$96,419.30. The batch payment effectively added 10 new individuals to the company's payroll, sending each slightly less than \$10,000. None of the individuals had any prior business or association with Cynxsure.

Wolters said the bank told him it would try to reverse the transfers, and in the meantime it issued the company a provisional credit, replacing all of the stolen funds. But when he went to draw on that amount, Wolters found he was not able to withdraw money from the account. The next day, Wolters said, the bank reported that it had been unable to reverse the transactions. Shortly thereafter, he said, Swift withdrew the provisional credit.

Cynxsure's attorney is now drawing up papers to sue the bank.

"We have done our best to make sure we've done everything we possibly can to protect our side of the equation," Wolters said. "We've put a lot of time and effort into making sure something like this couldn't have come from our side. We're not going to be one of those companies that goes quietly into the night after something like this."

James Reilly, operations leader at Swift Financial, declined to comment on the incident, saying only that "it is against our corporate policy to discuss this matter further due to customer privacy and possible litigation."

Wolters said his is the only computer used to access the company's accounts online. Since the incident, he has conducted numerous scans with a variety of anti-virus and anti-malware products – which he said turned up no sign of malicious software. Wolters is holding out hope that perhaps the incident is related to a story that he said a Swift Financial executive told him about an incident last summer in which a Swift employee was caught gathering customer online banking credentials without authorization, but that story could not be independently confirmed.

Swift, like all commercial banking institutions serving businesses in the United States, is required under federal guidelines to secure customer transactions using some form of “multi-factor authentication,” or something else in addition to just a user name and password.

Swift and many other commercial banks have chosen to adopt a technology that requires business customers to “register” the computer they use to do online banking, by answering a set of “secret questions.” Customers are generally prompted to answer these questions if they try to access their accounts from a new computer or if the customer tries to log in to his or her account using an Internet address that the bank has never seen associated with that account before.

Wolters said the bank told him that whoever initiated the bogus transaction did so from another Internet address in New Hampshire, and successfully answered two of his secret questions.

The Cynxsure manager said he thought a fingerprint scanner attached to the Windows laptop he uses to access his bank account online would help thwart any attacks from password-stealing malware. The scanner stores passwords as encrypted image files; when his bank or any other site asks for a password, Wolters doesn't enter the password in the site. Instead, he merely presses his thumb onto the scanner, which in turn decrypts the stored password for that site and pastes the information in the password field of the site he's visiting.

Unfortunately, these scanners aren't designed to defeat attacks from malware such as the Zeus Trojan, which is often mislabeled as an invader that records computer keyboard keystrokes. It can do that, but its most useful feature is one that intercepts all data the user enters into user name and password fields. This feature, called a “form grabber,” effectively snatches the credentials before the browser can encrypt the information and send it over the https:// connection.

The fingerprint reader, when presented with the proper finger or thumbprint, will decrypt the appropriate stored credentials for the site currently active in the user's browser, and paste that information into the relevant forms on the site. If a Trojan like Zeus were present on the machine, it would be just as able to rip out that information after the unsuspecting victim hits the “submit” button in their browser.

True, it is still not clear yet whether the attackers in this case used Zeus, or any other malware for that matter. Still, similarities between this attack and others strongly suggest the work of an organized crime gang operating out of Eastern Europe that typically steals banking credentials using the Zeus Trojan, and funnels the stolen funds in the same way as Cynxsure was hit.

Last week, I wrote about criminals using Zeus to siphon roughly \$150,000 from a Michigan insurance company. The attackers in that case sent the money to 15 people across the United States that had no prior business with the company, and the hackers defeated the bank's battery of secret questions in that attack as well.

Alas, Cynxsure may still get some money back, albeit a paltry 1 percent of what was taken. One of the individuals who received a \$9,500 transfer from Cynxsure's account, 26-year-old Merit Moll, from Collowhee, N.C., said he got the payment after signing up for a work-at-home job offered to him by a company calling itself the Element Group. The company's Web site, formerly at element-groupinc.ws, is no longer online. But Moll said he was told to create an account at the site and check his Web-based e-mail at the site once a day for messages that a new task was ready. On Feb. 9, Moll got his first (and last) task, and was asked to wire the money in \$3,000 chunks to three different individuals in Ukraine.

When confronted by his bank that the money he'd received and forwarded on had been stolen, Moll said he told his bank to take the \$750 commission he'd received for his work, as well, as the rest of the money in his account (around \$250), and make sure it was given back to Cynxsure.

"That was every last penny I had," Moll said. "I told them, 'Please take it, I wish I could do more. This is me sending what money back that I can, saying, I am really sorry. They really fooled me.'"

Cynxsure's Wolters said he hasn't seen a dime of the money yet.