

FDIC: Hackers took more than \$120M in three months

Robert McMillan

March 8, 2010 Ongoing computer scams targeting small businesses cost U.S. companies \$25 million in the third quarter of 2009, according to the U.S. Federal Deposit Insurance Corporation.

Online banking fraud involving the electronic transfer of funds has been on the rise since 2007 and rose to over \$120 million in the third quarter of 2009, according to estimates presented Friday at the RSA Conference in San Francisco, by David Nelson, an examination specialist with the FDIC.

The FDIC receives a variety of confidential reports from financial institutions, which allow it to generate the estimates, Nelson said.

Almost all of the incidents reported to the FDIC "related to malware on online banking customers' PCs," he said. Typically a victim is tricked into visiting a malicious Web site or downloading a Trojan horse program that gives hackers access to their banking passwords. Money is then transferred out of the account using the Automated Clearing House (ACH) system that banks use to process payments between institutions.

Even though banks now force customers to use several forms of authentication, hackers are still stealing money. "Online banking customers are getting too reliant on authentication and on practicing layers of controls," Nelson said.

That's bad news for businesses, which are increasingly on the hook for any losses.

"Commercial deposit accounts do not receive the reimbursement protection that consumer accounts have, so a lot of small businesses and nonprofits have suffered some relatively large losses," Nelson said. "In the third quarter of 2009, small businesses suffered \$25 million in losses due to online ACH and wire transfer fraud."

That's led to some nasty legal disputes, where customers say the banks should have stopped payments, and the banks argue that the customers should have protected their own computers from infection.

Often small businesses do not have the controls in place to prevent unauthorized ACH payments, even when their banks make them available, Nelson said. "Hackers are definitely targeting higher-balance accounts and they're looking for small businesses where controls might not be very good."

The FDIC's estimates are "reasonable," but they illustrate a problem that is becoming too expensive for banks and businesses, said Avivah Litan, an analyst with Gartner. She said that attacks that install a password-stealing botnet program, known as Zeus, have increased so far in 2010, so those losses may be even higher this year.