YAHOO! TECH

FBI Warns of $100M Cyber-threat to Small Business

By Robert McMillan, IDG News Service - Tue Nov 3, 2009

Cyberthieves are hacking into small- and medium-sized organizations every week and stealing millions of dollars in an ongoing scam that has moved about US$100 million out of U.S. bank accounts, the U.S. Federal Bureau of Investigation warned Tuesday.

There has been a "significant increase" in what's known as ACH (automated clearinghouse) fraud over the past few months, much of it targeting small businesses, municipal governments and schools, the FBI said in an alert posted to its Web site.

The criminals can move thousands or even millions of dollars out of their victims' accounts very quickly, using online banking to add new payees to the organization's bank account and then moving the money overnight. Usually the first step is an e-mail to the company's bookkeeper or financial officer that can include malicious attachments designed to look like Microsoft software patches, or simply links to malicious Web sites. The idea is to get the criminal's keylogging software onto a computer with online banking access and then steal login credentials.

Once they have access to the bank account, the hackers set up ACH transfers to money mules -- typically innocent victims who think they're doing payroll processing for international companies -- who then transfer the money overseas via services such as Western Union and Moneygram.

In one case, the criminals even launched a distributed denial-of-service attack against an ACH processor to prevent the bank from recalling transfers before the money mules could move them overseas.

Once the money is out of the country, it is gone for good.

Criminals prefer smaller organizations such as school boards because they tend to work with smaller regional banks that may not have the fraud detection controls in place to stop these fake ACH transfers. These organizations often publish contact information for financial personnel, or even organizational charts posted to their Web sites, making them easy pickings for fraudsters.

There has been a "significant increase" in what's known as ACH (automated clearinghouse) fraud over the past few months, much of it targeting small businesses, municipal governments and schools, the FBI said in an alert posted to its Web site.

The FBI is opening new cases every week on average, the IC3 said. "As of October 2009, there has been approximately $100 million in attempted losses."

The NCFTA is tracking between $1 million and $1.5 million in losses each week to this type of fraud, according to Ron Plesco, the NCFTA's executive director. "That's just from the folks we deal with. We're thinking it's larger than that," he added.

Smaller banks are being hit with this fraud because, unlike the larger national banks, they tend to not have the controls in place to block fraudulent ACH transfers, Plesco said. "It's strategic targeting of what is perceived to be a weakness in controls, whether it's at the small corporation [or at] the small-to-medium bank level."

Banks are covering some ACH losses, but all too often it's the online customer who's left holding the bag.

Article excerpt courtesy of ***Yahoo.com.*** *Article by* ***IDG News Service.***