November 3, 2009

FRAUDULENT AUTOMATED CLEARING HOUSE (ACH) TRANSFERS CONNECTED TO MALWARE AND WORK-AT-HOME SCAMS

Within the last several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts. In a typical scenario, the targeted entity receives a "spear phishing" email which either contains an infected attachment, or directs the recipient to an infected web site. Once the recipient opens the attachment or visits the web site, malware is installed on their computer. The malware contains a key logger which will harvest the recipients business or corporate bank account log-in information. Shortly thereafter, the perpetrator either creates another user account with the stolen log-in information, or directly initiates funds transfers by masquerading as the legitimate user. These transfers have occurred as both traditional wire transfers and as ACH transfers.

Further reporting has shown that the transfers are directed to the bank accounts of willing or unwitting individuals within the United States. Most of these individuals have been recruited via work-at-home advertisements, or have been contacted after placing resumes on well-known job search web sites. These persons are often hired to "process payments", or "transfer funds". They are told they will receive wire transfers into their bank accounts. Shortly after funds are received, they are directed to immediately forward most of the money overseas via wire transfer services such as Western Union and Moneygram.

Customers who use online banking services are advised to contact their financial institution to ensure they are employing all the appropriate security and fraud prevention services their institution offers.

The United States Computer Emergency Readiness Team (US-CERT) has made information on banking securely online available at http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf.

Protecting your computer against malicious software is an ongoing activity and, at minimum, all computer systems need to be regularly patched, have up to date anti-virus software, and a personal firewall installed. Further information is available at http://www.us-cert.gov/nav/nt01/.

If you have experienced unauthorized funds transfers from your bank accounts, or if you have been recruited via a work-at-home opportunity to receive transfers and forward money overseas, please notify the IC3 by filing a complaint at www.IC3.gov.

For a detailed analysis of this scam please visit https://www.ic3.gov/media/2009/091103-1.aspx.