"Money mules" carry load for global cybercriminals

December 21, 2009

In November, Portals and Rails explored the industry implications of hacking attacks that have resulted in fraudulent funds transfers using online banking interfaces. This week, Portals and Rails revisits this topic, focusing on the tactics these fraudsters use to dupe unsuspecting individuals and organizations.

The FDIC released a special alert on October 29, warning financial institutions of an uptick in schemes to recruit individuals to receive and transmit unauthorized electronic funds transfers (EFTs) from deposit accounts to individuals overseas. These funds transfer agents, also referred to as "money mules," are solicited online by criminals who have gained unauthorized access to the account of a business or consumer. Typically, the criminal will originate unauthorized EFTs from the victim's account to the money mule's deposit account. The money mule is then instructed to quickly withdraw the cash and wire it overseas minus a "commission" of from 8 to 10 percent.

Fraudsters perpetrate work-at-home scams using online job postings and social networking sites
A common hiring tactic for money mules are work-at-home jobs or other seemingly legitimate positions. Fraudsters will use online job search Web sites and social networking sites to persuade individuals to receive and forward stolen funds. According to the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA), victims are often hired to "process payments," "transfer funds," or "reship products." Other victims sign up to be "mystery shoppers" where they receive fraudulent checks with instructions to cash the checks and wire the funds to "test" the performance of a money service business.

The job scams also provide the criminal an opportunity to commit identity theft against the money mule. The personal information provided on the "employment" application (e.g., Social Security number or bank account information) may be used to open credit cards, post online auctions, etc., in the money mule's name and possibly commit additional crimes.

Sophisticated fraudsters use malicious code and money mules to conduct unauthorized funds transfers
An FBI alert issued last month describes how fraudsters are increasingly using malicious code to conduct unauthorized ACH transfers with the help of money mules. Many of these cases involve exploiting the online banking credentials belonging to small and midsized businesses, municipal governments, and school districts.

A typical scenario involves a "spear phishing" e-mail being sent to someone within the company with either an infected attachment or directing the recipient to an infected website. Spear phishing is a phishing attack that targets a specific person and deceptively appears to come from an individual or organization that the potential victim would normally receive e-mails from. The email recipient would usually have authorization to make funds transfers on behalf of the company.

Once the recipient opened the attachment or visited the Web site, malware (malicious software code) containing a key logger would be installed on the recipient's computer. The key logger captures the keystrokes of the recipient's business or corporate bank account login information. Once this information is compromised, the perpetrator either creates another user account with the stolen login or directly initiates funds transfers through either ACH or wire transfer by assuming
the legitimate user's identity. The transactions are typically in increments less than $10,000 to
avoid currency transaction reporting. Money mules play an important role in these schemes by
helping to facilitate the unauthorized transfer of funds.

**Small and midsized businesses lose millions to online banking scams**

Reportedly, small to midsized businesses in the United States have lost $40 million to online
banking fraud since 2004. FBI analysis has found that the main threat from these schemes is not
merely the malware but the vulnerabilities presented by the lack of controls at the financial
institution or third-party provider. In most cases, the victims' accounts were held at local
community banks and credit unions, some of which used third-party service providers to process
ACH transactions.

Many believe that the uptick in these types of fraudulent payment activities directly relate to the
decline in the economy. Consequently, financial institutions, businesses, and consumers have to be
vigilant in looking for signs of this activity. The Federal Financial Institutions Examinations Council
(FFIEC) provides guidance to financial institutions and technology service providers on
authentication in an Internet banking environment. Money mule activity in particular is addressed
by the Bank Secrecy Act and Anti-Money Laundering regulations. There are also resources available
to consumers and businesses on how to protect themselves from these types of online scams.

*By Jennifer Grier, senior payments risk analyst at the Atlanta Fed*

- December 21, 2009 in
  - ACH
  - cybersecurity
  - fintech
  - payments risk
- Permalink
- Comments