

Fraud Alert Involving E-mail Intrusions to Facilitate Wire Transfers Overseas

20 January 2012

The FBI has observed a trend in which cyber criminals are compromising the e-mail accounts of U.S. individuals and businesses and using variations of the legitimate e-mail addresses associated with the victim accounts to request and authorize overseas transactions. The wire transfers are being sent to the bank accounts of individuals typically located domestically or in Australia and the funds are being sent directly to Malaysia. Investigations indicate that some of the money mules in the U.S. and Australia are victims of a romance scam and are asked to further transfer the funds to Malaysia. As of December 2011, the attempted fraud amounts total approximately \$23 million; the actual victim losses are approximately \$6 million.

This type of fraud has affected banks, broker/dealers, credit unions and other institutions. Therefore, this threat is relevant to any organization that may engage with clients through e-mail channels.

In a typical scenario, the cyber criminal will send an e-mail to a financial institution, brokerage firm employee, or the victim's financial advisor pretending to be the victim and request the balance of the victim's account. When the request for balance information is successful, the cyber criminal then sends another e-mail providing a reason why they can only communicate via e-mail and asks that a wire transfer be initiated on their behalf. The excuse is typically based on an illness or death in the family which prevents the account holder from conducting business as usual.

Victims

Victims of these schemes include both individuals and businesses that typically invest significant amounts of money with their financial advisor(s) or financial institution(s). The individual unauthorized wire transfers range from \$17,500 to \$183,000.

E-mail Addresses

Cyber criminals are using both legitimate compromised e-mail accounts and e-mail addresses that are slightly altered. In cases in which the e-mail addresses were adjusted, they were either modified via the top level domain (eg., from .com to .net) or by adding an additional letter to the user name (eg., abcd@abc.com to abcdd@abc.com). Further investigations have also revealed that the e-mail service provider name has been modified by changing a letter to a number or vice versa (eg., abc@0123.com to abc@.0123.com). The modifications can be very subtle and easily mistaken as the legitimate account holder's official e-mail address on file. In many cases, the e-mails have originated from e-mail service providers including Yahoo, Gmail, and AOL.

Authentication

In some instances wary financial institutions or brokerage firm employees asked for a letter of payment authorization via fax, and the cyber criminals were able to produce a fax with the legitimate customer's signature as further proof that the transaction was being requested by the bank customer. This was most likely done through extensive research of the compromised e-mail accounts in which the cyber criminals were able to obtain copies of official documents signed by the

victim. Some institutions reported that the signatures resembled a “copy and paste” from a previous document.

There have been several reports connected to this scheme where the cyber criminal modified the victim’s e-mail settings to block all legitimate e-mails from the victim’s financial institution. This was accomplished either by implementing a spam rule to dump all communications from the financial institution into a spam folder or automatically deleting the communications. Either method prevents the victim from being alerted that the transaction had taken place and may provide additional time for the money to be transferred out of the account before anyone can identify the transaction as fraudulent.