August 27, 2015

Alert Number
I-082715b-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

E-MAIL ACCOUNT COMPROMISE

E-mail Account Compromise (EAC) is a sophisticated scam that targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms.

The EAC scam is very similar to the Business E-mail Compromise (BEC) scam, except that it targets individuals rather than businesses.[1]

In EAC scams, criminal actors use social engineering or computer intrusion techniques to compromise the e-mail accounts of unsuspecting victims. In many cases, a criminal actor first gains access to a victim's legitimate e-mail address for reconnaissance purposes. The criminal actor then creates a spoofed e-mail account that closely resembles the legitimate account, but is slightly altered by adding, changing, or deleting a character. The spoofed e-mail address is designed to mimic the legitimate e-mail in a way that is not readily apparent to the targeted individual. The criminal actor then uses either the victim's legitimate e-mail or the spoofed e-mail address to initiate unauthorized wire transfers.

In some cases, the funds from unauthorized wire transfers are directed to money mules[2] located in the United States. In other instances, wire transfers are directed to accounts of financial institutions outside of the United States. Victim reporting indicates criminal actors are starting to follow up on wire transfer requests by calling to confirm the transactions or to comply with wire transfer protocols, thus making the transaction appear more legitimate.

Other schemes seen in complaints filed with the Internet Crime Complaint Center (IC3) and in additional information made known to the IC3 indicates EAC money mules may be victims of employment scams, romance scams, or personal loan scams. It is not known why a specific victim is identified to be targeted.

Between 04/01/2015 and 06/30/2015, 21 complaints related to the EAC scam were filed with the IC3, with reported losses of almost $700,000. The FBI has identified approximately $14 million in attempted losses associated with open FBI EAC investigations.

EXAMPLES OF THE EAC SCAM ARE LISTED BELOW:

Financial/Brokerage Services –

- An individual's e-mail account is compromised by a criminal actor. The criminal actor, who is posing as the victim, sends an e-mail to the victim's financial institution or brokerage firm requesting a wire transfer to a person or account under the control of the criminal actor.

- An accounting firm's e-mail account is compromised and used to request a wire transfer from a client's bank, supposedly on behalf of the client.

Real Estate –

- A seller's or buyer's e-mail account is compromised through an EAC scam. The criminal actor intercepts transactions between the two parties and alters the instructions for the transfer of funds.
- A realtor's e-mail address is used to contact an escrow company to redirect commission proceeds to a bank account associated with the criminal actor.
- A realtor receives a link within an e-mail from an unknown person who is requesting information related to property. When the realtor clicks on the link, the criminal actor is able to access the realtor's e-mail account. The intrusion exposes client information, which the criminal actor then uses to e-mail the clients and attempt to change wire instructions for loan processing proceeds.

Legal -

- A criminal actor compromises an attorney's e-mail account, which results in the exposure of client bank account numbers, e-mail addresses, signatures, and confidential information related to pending legal transactions.
- The attorney's compromised e-mail account is used to send overlaid wire instructions to a client.
- A criminal actor compromises a client's e-mail account and uses it to request wire transfers from trust fund and escrow accounts managed by the firm.

WHAT TO DO IF YOU BELIEVE YOU HAVE BEEN A VICTIM OF THE EAC SCAM:

- Contact your financial institution immediately upon discovering the fraudulent transfer.
- Contact law enforcement.
- Request that your bank reach out to the financial institution where the fraudulent transfer was sent.
- File a complaint at www.IC3.gov, regardless of dollar loss. Provide any relevant information in your complaint and identify that your complaint pertains to the EAC scam.

TIPS TO PROTECT YOURSELF:

- Do not open e-mail messages or attachments from unknown individuals.
- Be cautious of clicking links within e-mails from unknown individuals.
- Be aware of small changes in e-mail addresses that mimic legitimate e-mail addresses.
- Question any changes to wire transfer instructions by contacting the associated parties through a known avenue.
- Have a dual step process in place for wire transfers. This can include verbal communication using a telephone number known by both parties.
- Know your customer. Be aware of your client's typical wire transfer activity and question any variations.

1.To learn more about how the BEC scam affects businesses, see the Public Service Announcement (PSA) dated 01/22/2015 at www.IC3.gov. It is anticipated that an updated BEC PSA will be released in August, 2015.↩

2.Money Mules are people who are used to transfer and launder stolen money. They are typically given a portion of the money transferred as payment. ↩